applied sciences

MDPI

Article

Implementation of a Blockchain System Using Improved Elliptic Curve Cryptography Algorithm for the Performance Assessment of the Students in the E-Learning Platform

Mohammad Y. Alshahrani

Department of Clinical Laboratory Sciences, College of Applied Medical Sciences, King Khalid University, P.O. Box 61413, Abha 9088, Saudi Arabia; moyahya@kku.edu.sa; Tel.: +966-503-087-507

Abstract: Blockchain technology allows for the decentralized creation of a propagated record of digital events, in which third parties do not control information and associated transactions. This methodology was initially developed for value transmission. Still, it now has a broad array of utilization in various industries, including health, banking, the internet of things, and several others. With its numerous added benefits, a blockchain-based learning management system is a commonly utilized methodology at academic institutes, and more specifically during and after the COVID-19 period. It also presents several potentials for decentralized, interoperable record management in the academic system in education. Integrity, authenticity, and peer-executed smart contracts (SC) are some of the qualities of a blockchain that could introduce a new degree of safety, trustworthiness, and openness to e-learning. This research proposes a unique encryption technique for implementing a blockchain system in an e-learning (EL) environment to promote transparency in assessment procedures. Our methodology may automate evaluations and provide credentials. We built it to be analytical and content-neutral in order to demonstrate the advantages of a blockchain back-end to end-users, including student and faculty members particularly during this COVID-19 era. This article explains the employment of blockchain and SC in e-learning. To improve the trust in the assessment, we propose a novel improved elliptic curve cryptography algorithm (IECCA) for data encryption and decryption. The performance of the suggested method is examined by comparing it with various existing algorithms of encryption. The evaluation of the behaviour of the presented method demonstrates that the technique shall enhance trust in online educational systems, assessment processes, educational history, and credentials.

Keywords: blockchain technology; improved elliptic curve cryptography algorithm (IECCA); blockchain system; e-learning (EL) platform; smart contracts (SC); COVID-19

Citation: Alshahrani, M.Y. Implementation of a Blockchain System Using Improved Elliptic Curve Cryptography Algorithm for the Performance Assessment of the Students in the E-Learning Platform. *Appl. Sci.* **2022**, *12*, 74. https://doi.org/10.3390/app12010074

Academic Editors: Asadullah Shaikh, Uffe Kock Wiil, Yousef Asiri and Gianluca Lax

Received: 27 September 2021
Accepted: 8 December 2021
Published: 22 December 2021

1. Introduction

Thec COVID-19 pandemic has made conventional face-to-face education a perilous procedure, and several nations are changing to an EL way of teaching to prevent the spread of this deadly virus. Several nations' resources are insufficient to support this quick conceptual change from conventional classrooms to EL. As a result, numerous obstacles are posted regularly. Integrating proper end-to-end safety features during the EL procedure is one of the primary difficulties that must be addressed for this EL process to be effective.

Conventional methods of education have come to a standstill as a result of COVID-19's worrisome transmissibility, and EL applications are becoming the only provider of halted teaching programs. Many remedies were suggested on an immediate basis to address the global disruption. EL implementation is completely reliant on the internet, which is home to a slew of criminal activity and security threats. As a consequence, the EL system is vulnerable to several safety risks. Due to the widespread impact of COVID-19, one of the main causes for the current rise in security concerns is a massive dramatic change from the

old education systems to EL. In such a setting, EL technology vendors' primary objective is offering speedy EL services for academic institutions, while ignoring the security issue.

COVID-19 has a massive effect across a broad number of industries. Several countries have enacted lockdowns, compelling academics, professionals, and a diverse variety of other specialists to work remotely to smooth the curves of the disease's transmission. For their everyday productivity, most of these workers rely completely on organizational and institutional assets, which include computer resources, memory, and network availability. Several settings are now set up in such a way that devices outside of the physical environment are unable to access the services and apps that are running. Switching key apps and services to the blockchain environment progressively increases the availability and convenience of access to these services and applications for clients, regardless of their location or device information.

A technology of shared register in the structure of a propagated transferable database is termed a blockchain. Cryptographic techniques and consensus mechanisms secure a blockchain. A blockchain is necessarily a collection of digital incidents. It also comprises smart contracts (SC), which is nothing but the stored programs on the blockchain. The SCs function as executed without having a danger of halts, restrictions, and scams. Blockchain technology is currently viewed mainly as the methodology that facilitates crypto currencies like Bitcoin. However, it is expected that blockchain technology will turn into a more beneficial facilitator of commercial and public contracts. Blockchain technology possesses propagated transaction data and cryptographic techniques that make it remarkably resistant to attacks by intruders [1].

From bureaucratic systems to corporate supply chain management and even the educational sector, blockchain technology has emerged as one of the essential worldwide technologies in the previous decade. The significant manner by which blockchain methodology shall revolutionize the academic business is just beginning to influence learning institutions [2].

Blockchain's implementation in the educational sector is still in its early phases. A restricted count of educational organizations is utilizing blockchain methodology. The majority of these organizations employ it to evaluate and share their academic certifications and learning objectives. On the other hand, researchers in the industry believe that blockchain technology has a lot more to give and can even revolutionize the field [3].

EL is popular interactivity that is not constrained by time or space constraints. It is an excellent way to promote better educational opportunities by utilizing external resources and motivating individuals to learn for themselves. Nevertheless, it confronts other obstacles, including EL evaluation problems, a shortage of assessment criteria, the legitimacy of EL credentials, and, most critically, privacy. Integrating suitable end-to-end safety features during the EL procedure is one of the primary difficulties that must be discussed for this EL process to be effective. Because of the transparency and records authentication features associated with blockchain, it is best suited for the EL system. In EL, security refers to the students' complete access to every educational material. In this case, blockchain can assist in delivering a safe and transparent solution for the EL setting [4].

The purpose of such an encryption key is to conceal secret data in such a manner that an unidentified user cannot decipher its contents. Plain text is the type of data that must be hidden, while enciphering is indeed the process of hiding it. Cipher text refers to the encryption process. The encipherer is one who decodes the communication, whereas the recipient is the entity upon whom he transmits the cryptogram. The algorithm is a list of laws used by the encipherer to decode his plain text [5].

In an e-learning context, assessment is critical. e-learning is a type of remote learning digitized using a digital channel, such as the internet and learning process toolkit. People concerned in the teaching-learning procedure in e-learning settings do not share a physical place of communication, creating a spatial and temporal gap that provides unique issues for assessing students' knowledge and skills acquisition. To accomplish successful and efficient e-learning processes, the education system must suggest methodologies, strategies,

and procedures. Several vital issues exist in the domains of e-learning assessment, like self-assessment, peer-assessment, and automated review, to name a few [6].

The other portion of the article is structured as shown: Section 2 provides the literary works associated with our method and the problem statement. Section 3 explains the flow of the suggested approach. Section 4 analyzes the performance of the presented method, and finally, Section 5 concludes the overall idea of the paper.

2. Related Works

Literature on the recent state of arts in e-learning

Alrikabi et al., (2021) [7] presented the educational process paradigm, with its many cloud inputs and outputs, and how the educational problem in all of its organizations may be addressed by utilizing the digital cloud in distance learning. This research looked at all of the characteristics of that setting, as well as the possibilities of using them in universities and educational institutions.

Shaikh et al., (2019) [8] conducted a thorough study of the literature on cloud-based e-learning critical success factors (CSFs) in the learning and teaching processes. Furthermore, the study uses a combinatorial method to assess the multiple aspects and CSFs of cloud-dependent e-learning, which aids in assessing and evaluating the impact of different aspects and CSFs. In-depth literature analysis revealed four aspects and fourteen criteria, which were then analyzed for prioritizing using a combinatorial methodology. The impact of these aspects and elements would aid multiple parties in devising a strategy and allocating resources to improve the transfer of knowledge via cloud-dependent e-learning.

To explore the diverse elements from different aspects of the web-based e-learning system, Qureshi et al., (2020) [9] used the analytic hierarchy process (AHP) with group decision-making (GDM) and fuzzy AHP (FAHP). The crucial success factors (CSFs) and their parameters were evaluated. The literature study showed 5 distinct characteristics and 25 parameters linked with the web-based e-learning system, which were further investigated. Additionally, the impact of each component was correctly calculated. Understanding the effects of each e-learning element will aid participants in developing educational policies, managing the e-learning system, managing assets, and keeping up with worldwide developments in knowledge acquisition and management.

Nassa et al., (2021) [10] analyzed the effect of e-learning in the context of COVID-19, focusing on aspects like system performance throughout the digital material transfer. Since information is condensed first and subsequently encoded on the transmitter end, the proposed approach is said to be safe and quick. The information is decoded and decompressed at the receive side. Since the quantity of information is smaller during transfer, the problem of network latency is overcome. Furthermore, the packets dropping ratio decreases. As data is encrypted after compressing, the likelihood of deciphering encoded files decreases.

Alam et al., (2021) [11] tried to figure out what factors influence the quality of cloud e-learning services. A comprehensive literature search yielded a mathematical framework for assessing the quality of cloud e-learning services. The suggested theoretical model has been validated by empirical testing, and an online survey was conducted using a self-structured closed-ended questionnaire.

Alruwaili (2020) [12] suggested an e-learning chain (ELC) architecture that supports education accreditation, authentication, surveillance, and verification utilizing distributed ledger technology (DLT) and smart contracts. Smart contracts are used to guarantee that the prototype validation process is supported, allowing for more efficient and safe mechanization and authentication. The ramifications of adopting a blockchain-based e-learning system in other education sectors are examined, as well as future research directions.

2.1. Literature on Blockchain with E-Learning

Zhang et al., (2019) [13] suggested a blockchain technology for e-learning evaluation and certification that incorporates an entirely new network framework built on the aggre-

gation of public and private blockchain systems, and also four principal smart contract strategies for e-learning evaluation and credit interchange, digital certificate allocation and integrity protection, the digital certificate authentication and the e-learning voucher issuance, accordingly. The suggested approach was shown to be a viable contender for creating a more equitable, healthy, and transparent e-learning and online educational atmosphere.

Lam and Dongol (2020) [14] unveiled a proof-of-concept blockchain-dependent e-learning system designed to improve assessment openness and curriculum customization in higher education. This platform may, for example, perform evaluations and provide credentials. They created it to be methodologically and content-neutral to illustrate to end-users, such as learners and lecturers, the advantages of a blockchain back-end. According to the review, the proposed platform might boost trust in online educational institutions, assessment methodologies, educational background, and credentials.

Sastry and Banik (2021) [15] proposed a secured blockchain methodology that builds a flexible and secure data transmission ability, which communicates with present education information. The suggested architecture enhances data protection and removes trust issues amongst users and other institutions that use services and applications.

Cheriguene et al., (2021) [16] introduced a novel online teaching and assessment (NOTA) technique, which uses blockchain technologies to ensure the desired quality of education and assessment integrity while adhering to the course and examination schedules. Furthermore, NOTA use blockchain's incentive systems to encourage both teachers and students to persevere in their objectives, even if they work remotely. The preliminary findings from the Coronavirus era revealed a much higher satisfaction rate of more than 90%. This made them quite hopeful about the proposal's possibilities when implemented on a bigger scale.

Liang and Zhao, (2020) [17] built a blockchain-dependent mechanism for assessing the overall condition of students. The smart contracts, the interplanetary file system (IPFS), and the web service are used to guarantee that information movement is effective, secure, and consistent in this system, which combines "on-chain and off-chain" data. They presented a network infrastructure centered on an education consortium blockchain, in which they developed a blockchain data structure and preservation framework to make learners' quality evaluation data more accessible. Furthermore, a data flow framework is being developed for the secure transfer and authentication of student data, combining the benefits of the RBFT-based hyper chain consortium blockchain with classical data permanence. The system is then built using the microservices framework, and a performance optimization strategy is proposed to assure high availability.

Sun et al., (2021) [18] propose a blockchain-dependent online language learning platform to track learners' daily studies and automatically analyze their performance, freeing educators from laborious and time-consuming assignment assessment and providing trustworthy and reliable feedback on the performance of the students. The present condition of language learning in institutions and existing methods on a blockchain-dependent online language learning platform is reviewed in this article. The framework and smart contracts of the system are then described in depth. Finally, they implemented the system to complete the necessary analysis and reporting.

Ma (2018) [19–22] developed a novel decentralized access control mechanism for securing a collaborative peer-to-peer e-learning system. Using a Blockchain network, the reliability, validity, non-repudiation, and tracking of e-learning materials are guaranteed in this paradigm. This model will also be implemented using RESTful web services and the Go/Java programming language. The suggested approach is evaluated using a crucial metric: average reaction time. Investigations were performed to improve accuracy. The identical experiment is carried out in two vastly different environments: a local area network (LAN) and a cloud web service. The LAN operating atmosphere denotes the ideal condition, whilst the cloud atmosphere describes the actual situation in the real world. Moreover, deploying servers to a cloud system can significantly enhance performance. Increasing the delay, on the other hand, may have a minor influence on system stability.

2.2. Research Gap

Blockchain has recently developed as a completely decentralized and traceable system in which any participating node may contribute reliable information to the blockchain, resulting in a safety framework. Current studies focus mostly on the use of blockchain to secure access control and certifications for e-learning platforms, but the teaching and assessment processes have not yet been considered. As data is huge in e-learning, data loss is a major concern.

2.3. Problem Statement

The huge quantity of e-learning material causes the complication of e-learning evaluations and data loss. Hence, in this article, we suggested implementing a blockchain system using a novel encryption algorithm for the students' performance assessment in the e-learning platform.

Our major contributions to this research include:

- Integration of blockchain technology to the e-learning platform.
- To enhance the trust of the e-learning system by using a novel encryption algorithm.
- To achieve a secure auto-marking process for performance assessment of the students in the e-learning platform with the help of smart contracts.

3. Proposed Work

This section describes the flow of the proposed method. We have used an ethereal blockchain for our research. Ethereum is a blockchain platform that has a currency, Ether (ETH), as well as a programming language, Solidity. Ethereum is a decentralized public ledger for validating and recording transactions as a blockchain network. A proof of work (PoW) consensus protocol is used. The schematic representation of the suggested work is displayed in Figure 1.

The system enables three different sorts of players to be created and they interact with each other with the help of smart contracts:

- Lecturers, teaching assistants, instructors, and other educators.
- Learners that include on-campus pupils, online pupils, and others.
- Readers, members of the public who are engaged in accessing or validating data, such as employers and further education establishments.

A. Input data

A dataset of 1185 students from 27 courses held in 2008–2009 and 2009–2010 was used in this study. Using the criteria of uniform content, an expert with 10 years of experience at the e-learning center determined the courses to be included in the study. As a result, a collaborative analysis of the dataset in the various subjects is conceivable. Furthermore, it was decided that a high degree of questionnaire participation was essential, as well as that subjects must be presented for at least two years.

B. Preprocessing using Normalization

The input data is unprocessed and may include missing data and repetitive packets. It has been preprocessed to eliminate redundant and duplicated occurrences and also tidy up missing data. The dataset for the education system is extensive, and hence sample size minimization techniques are needed to be deployed. Because this dataset has a vast range of attributes, feature extraction tools are necessary to exclude the ones that aren't significant. The dataset can be normalized at the pre-processing stage. In the initial step of the normalization process, the z-score is obtained, which is expressed by Equation (1).

$$Z = [(Y - \alpha)/\omega] \quad (1)$$

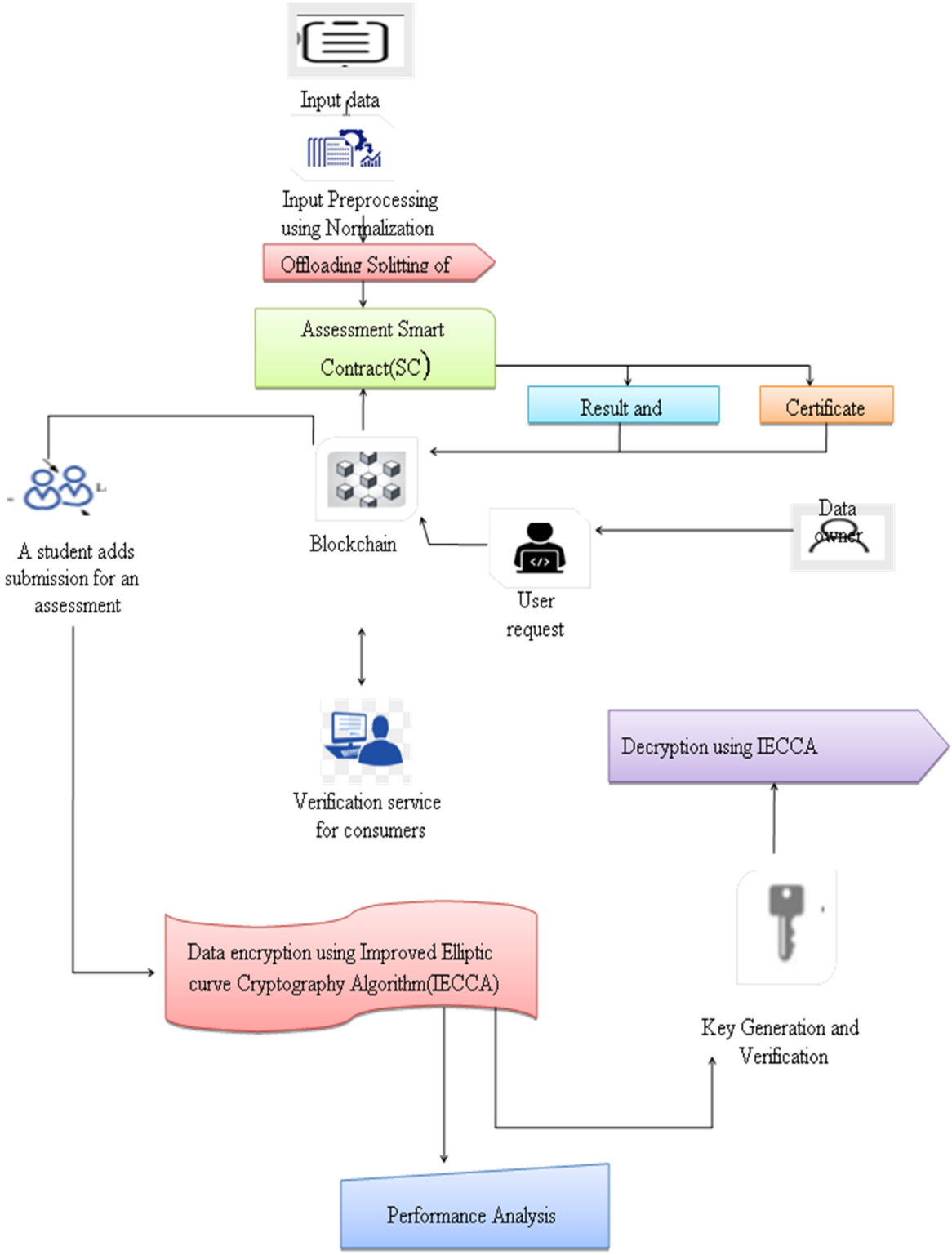

Figure 1. Schematic representation of the proposed method.

Here, α represents the mean of the dataset and ω denotes the standard deviation. And Z is given by Equation (2).

$$Z = \frac{Y - \overline{Y}}{D} \tag{2}$$

Here $\overline{Y}$ represents the mean of the sample, and D denotes the standard deviation of the model. The random sample shall be in the pattern as shown in Equation (3).

$$Z_j = \beta_0 + \beta_1 Y_j + \varepsilon_j \tag{3}$$

Here ε_j denotes the errors, which is relied on the ω^2. Following that, the errors must not depend on one another, as shown below.

$$y_j \sim \sqrt{\omega}\frac{y}{\sqrt{y^2 + \omega - 1}} \tag{4}$$

Here y denotes a random variable. After that, the standard deviation is used to standardize the movements of the variables. The following expression is used to compute the moment scale deviation.

$$M = \frac{\lambda^m}{\varnothing^m} \tag{5}$$

Here m denotes the moment scale.

$$\lambda^m = E(Y - \alpha)^M \tag{6}$$

Here Y represents a random variable, and E denotes the expected value.

$$\varnothing^m = \left(\sqrt{E(Y - \alpha)^M}\right)^2 \tag{7}$$

$$y_\omega = \frac{m}{\overline{Y}} \tag{8}$$

where y_ω denotes the coefficient of the variance.

The feature scaling procedure will then be stopped by setting all of the values to 0 or 1. The unison-based normalizing approach is the name for this procedure. The normalized equation will be expressed as,

$$Y\prime = \frac{(y - y_{min})}{(y_{max} - y_{min})} \tag{9}$$

Once the data has been normalized, the data set can be managed, and the extent and variability of the data may be constant. This stage is mainly for minimizing or eliminating data latency. The normalized data can then be used as a feed for the subsequent phases.

C. Offloading splitting of the data

This process is carried out because the data in the e-learning platform is huge. Offloading and data splitting can be done after preprocessing. Changing an information component in most prior offloading techniques could result in invalid data. This problem can be solved within the information storage technique by scheduling data that will be used soon. As a response, after sending the data, the server sends the id list of the data whose data values will be shared later and then shares the data values of the data in the id list. The id runs down and determines when the valuable info will arrive at the end of the data transmission.

D. Assessment Smart Contract (SC)

Smart contracts are comparable to recorded processes in relational database maintenance systems in that they are a compilation of transactional scripts. Transaction on the blockchain will provoke certain portions of a smart contract code, and they are the only way for peers to change the status of the blockchain. The pre-programmed scripts could execute on blockchain peers and suggest blockchain updates. If the network reaches a consensus, the modifications are adopted. Any alterations that have been approved are permanent. In the hyper ledger composer environment that we employed, Algorithm 1 shows an uncomplicated form of transaction scripts. Every transaction takes a set of input

data and verifies the contractual terms using such input and the current condition of the blockchain. If the evaluations are passed, resources on the blockchain can be produced or changed per the contract requirements by network consensus; otherwise, the transaction would be refused. The schematic representation of the assessment smart contract is shown in Figure 2.

Algorithm 1: Simplified form of transaction scripts in Hyper ledger composer

```
transaction ts(input data)
if contractual factors are satisfied, then . . .
← produce or upgrade blockchain resources
return Transaction Approved ←if network consensus attained
else
return Transaction Refused
end if
end transaction
←do nothing if contractual factors are not satisfied
```

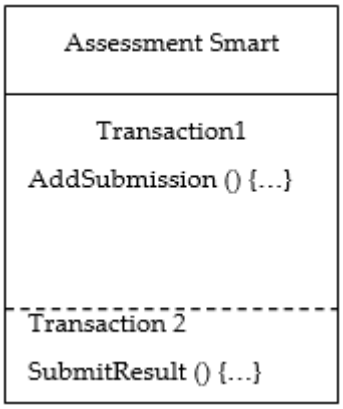

Figure 2. Assessment Smart Contract (SC).

After completing the course studies, the learning user may submit a certification request to the department of education, and the education authority will verify the learning user's course credit balances. If the course credit balances reach the required level for course completion, a digital certificate with detailed information is generated and digitally signed by the education authority and the learning user one by one. As a new digital certificate block, the digital certificate with a double digital signature is permanently registered in the blockchain. The credits for the course digital certificate are deducted from the course credit wallet at the same time, and the learning achievement score associated with the digital certificate is added to the learning user's certificate wallet.

Assessments can be done out inside the blockchain using the proposed platform. Smart contract assessments are peer-executed, which means that peers on the blockchain shall conduct the exact computations and agree on the final score, considerably minimizing the odds of manipulation. We tried to inspire educators to perform evaluations with maximized openness and officially register modifications or contingent interventions by standardizing evaluations into a sequence of open phases implemented by a peer group, reducing tension and disputes among teachers and students.

Assessor marking and automated marking were the two types of assessments we investigated. Assessor marking is the conventional method of a lecturer utilizing their best expertise to grade a student's work. Any standard marking methodology can be used in this format; the distinction is that the scores are entered digitally and stored in the blockchain. Automated marking represents the tests performed by a machine and offers results and feedback to the assessor. It can reduce physical labor and provide real-time

feedback. Such marking methods are becoming more prevalent, especially in subjects like computer science.

Figure 3 depicts the interplay of two transactions that were supposed to complete the assessment smart contracts.

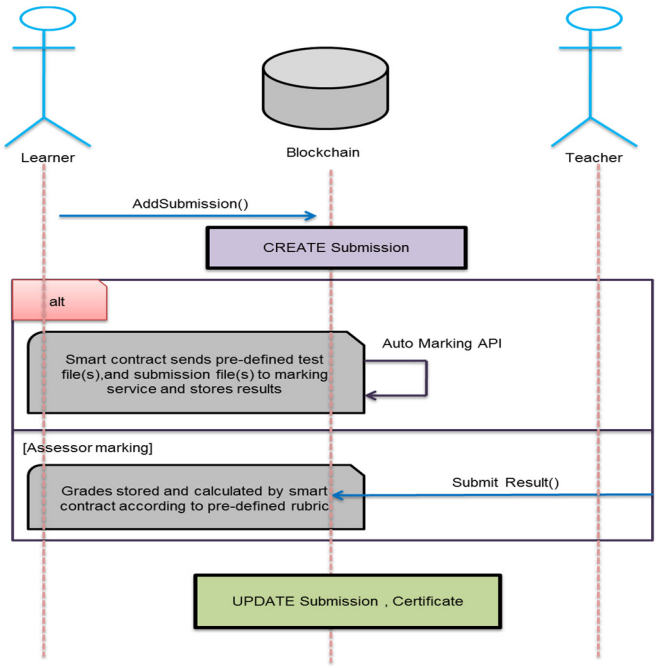

Figure 3. Diagram representing transactions (blue arrows) for an assessment effort.

Whenever a submission resource is modified with a pass mark, references to the submission shall be included in the necessary certificate resources as proof of evaluation satisfaction for both the ADDSUBMISSION and SUBMITRESULT processes. A student uses the ADDSUBMISSION transaction to record a submission (evaluation try) on the blockchain. The use of the blockchain to store submissions assures that they are private and unchangeable. Data are zipped and transformed into base64 data strings in our proposed method. When submitted files are too massive in real-world cases, a data server might be required to record submissions instead, with a checksum recorded on the blockchain. Algorithm 2 explains the transactions in the assessment smart contract.

(a) Automated marking

The ADDSUBMISSION transaction might quickly deliver automatic evaluation findings. Test files for automated marking are maintained on the blockchain, ready to be delivered along with students' submission files to the appropriate extrinsic automated marking service. Just one simple automatic marking service was implemented in our demonstration system. It was a standalone web application, which performed a string equivalency check. Although this was merely a simple equivalency check, it demonstrated the blockchain's capacity to perform automated tests.

(b) Assessor marking

The course's educator uses the SUBMITRESULT transaction to upgrade a submission's evaluation outcome on the blockchain for assessor marking. Grades could be calculated in various methods, including by the educator, the applications, or the blockchain SC. Because the grades estimation formula would already be kept on every blockchain peer in the predefined evaluation rule, we chose to develop the last of these in our system. Teachers can use a grade description grid to submit grades. Smart contracts produce final rates based on pre-determined percentages and regulations. Teachers could then use comments to make changes to the final mark. This gives a way to make mark moderating more transparent.

(c) Credential generation

The availability of evaluation transactions on the blockchain provides a reliable and unchangeable record of a student's progress. Our platform's credentials are invariably traceable to past transactions, which anyone can verify and make public if the learner so desires. Teachers can demonstrate and authorize a certificate on the blockchain using the SIGNCERTIFICATE transaction, which is optional. It is used to mimic the explicit "degree conferral" procedures in real-world institutions. It also acts as the last stage for any automated due diligence before a learner receives a certificate for a course. Multiple signatures may be required based on the syllabus or course structure.

Algorithm 2: ADDSUBMISSION and SUBMITRESULT transactions in the assessment SC

```
transaction ADDSUBMISSION (input data)
    CREATE Submission objects
    if assessment is automated then
        GET test files from the blockchain
        POST files to the marking service
        GET results from marking service
        UPDATE Submission asset with returned results
        if results are a pass then
            UPDATE Certificate
        end if
else
        ASSIGN a teacher to the submission
end if
Transaction rejected if conflicts occur
return Transaction Accepted
end transaction
transaction SUBMITRESULT (input data)
    COMPUTE result
UPDATE Submission object
if Submission graded as pass then
        UPDATE Certificate
    end if
end transaction
```

E. Improved Elliptic Curve Cryptography Algorithm (IECCA)

The IECCA is a public-key cyber security technique that relies on elliptic curves over finite regions. The Equation (10) defines an elliptic curve.

$$r^2 + qr = q^3 + cq + d^4 \tag{10}$$

Elliptic curve procedures: an elliptic curve's most important attribute is that we can design a strategy for adding the two locations on the curvature to get a third point. The basic features of addition are satisfied by this addition strategy. A finite Abelian group is formed by the vertices as well as the addition function. Researchers require an additional zero value 0, which will not meet an elliptic formulation, in order for add to be explicitly specified for any two points. A vertex on the curve is assumed to be zero. The variety of different points, along with the zero, is indeed the order of contour. After defining addition of two points, designers may establish multiplier jQ as the total of j duplicates of Q, in which j is a positive number as well as Q is a point. That is $2Q = Q + Q$.

The elliptic curve encryption algorithm is a discrete algebra encryption method that replaces the multiplicative group of a finite set with an elliptic curve grouping. With a key length of 1/10, it delivers a similar level of security to the RSA encryption scheme. In order to engage in the interaction, the client develops a public key, distributes it among the clients to engage in the interaction, and then creates a private key using the ECDH (elliptic curve

Diffie–Hellman) algorithm in the encryption system by using an elliptic curve algorithm. First, the message is conveyed by encrypting it with the secret key, then receiving it and decrypting it.

To ensure security, the confidential data that must be kept hidden is encrypted before transmission. The IECCA algorithm is used to offer protection. The private key is generated using the chosen prime number and universal point. The private key creation alters based on the prime number. The proposed algorithm varies from the existing ECC in order to further reduce the size of the keys generated, and hence the computation overhead can be minimized. The succeeding steps demonstrate the IECCA algorithm:

Input: Prime number, x, y, private data.

Output: Index values for encrypted points.

3.1. Encryption Algorithm

Choose a relevant curve Ep(x,y) and determine all the Ep(x,y) points.

Every point on the curve is allocated to the alphabet, number, and unique character.

Allocate index values to the alphabet, number, and unique character to develop an index table.

Choose global point P with higher-order m in Ep(x,y).

The sender and receiver select the private key.

Evaluate the public key of senders and receivers.

The sender's and receiver's secret key is estimated.

Obtain the private data and map to equivalent points that are created from step 2.

Points that are created for private data are fed as an input for encryption.

By employing the universal point P, an arbitrary integer and receiver's public key estimate the encrypted points.

Encrypted points and their equivalent character are mapped to the index value assigned in step 3.

The resulting index value is fed as an input for assessment.

3.2. Decryption Algorithm

Input: Index values, Prime number, x, y.

Output: Private message.

Index values that are created from the data encryption algorithm are fed as an input for decryption.

The receiver shall utilize the similar curve type Ep(x,y) and utilize the similar index table in the sender facet.

The attained index value is mapped onto equivalent characters and equivalent encrypted IECCA points expressed within the index table.

For the decryption procedure, the product of the receiver secret key, an arbitrary number, and a universal point must be subtracted from the encrypted points.

IECCA points are mapped into equivalent characters in the index table, which is the plaintext of information.

4. Performance Analysis

The proposed blockchain uses smart contracts on a public permissioned blockchain to satisfy educational evaluations and customized curriculum. It demonstrates how this new technology may improve a variety of key learning experiences, including assessments, curriculum customization, and learner privacy. By improving transparency and authenticity while maintaining fine-grained security controls on student data, it was able to increase trust in educational procedures and certifications.

The behavior of the suggested methodology is represented in this section. We contrast the proposed algorithm with the conventional methods. The system is simulated using LAN and the simulation parameters of the presented system are portrayed below in Table 1.

Table 1. Simulation specifications of the suggested system.

Parameters	Values
Energy transmission	70 m
Energy sampling	30
Energy amplitude	0.0123 m
Energy aggregate	5 kWh
Primary user	150
Secondary user	150
Number of packets	Random of 10–15
Square area size	1000×1000 m^2
Velocity	[10,40] m/s

4.1. Security Level

The security level is a measure of the strength that a cryptographic primitive, such as a cipher or hash function, achieves. The security level of the suggested mechanism gets compared. Other current strategies are compared in order to reveal the efficiency of the suggested improved elliptic curve cryptography algorithm (IECCA).

The level of security of various encryption methods is examined and contrasted in Figure 4. The analyzed techniques are DES, RSA, AES, and the suggested IECCA. For file size 20 MB, the level of security is 83% of IECCA, 78% of DES, 76% of RSA, and 70% of AES. Likewise, the security level is examined for 40, 60, 80, and 100 MB file sizes. The graph displays the suggested IECCA attains a higher level of security when contrasted with alternate encryption methods.

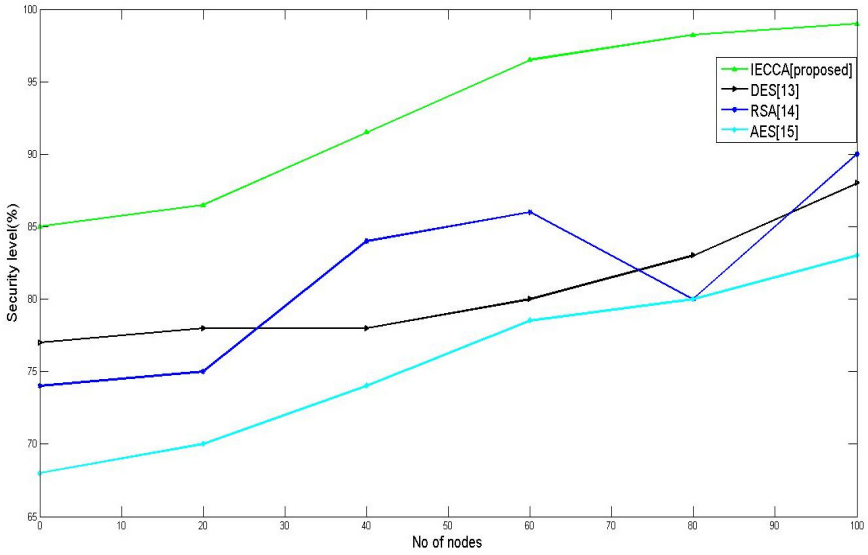

Figure 4. Comparison of security level (%) for various file sizes for existing vs. proposed method.

4.2. Execution Time

Figure 5 displays the efficiency of the proposed and current methods for different file sizes, such as 20 MB, 40 MB, 60 MB, and 80 MB, compared in terms of execution times. The findings are evaluated and compared to other methods such as DES, RSA, and AES. As a consequence of the results, it was discovered that the suggested approach outperforms the alternate methodologies in terms of performance.

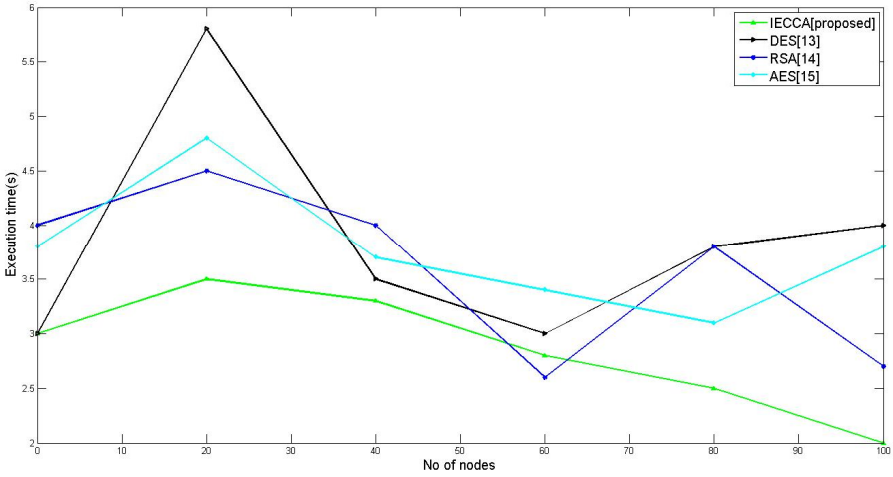

Figure 5. Comparison of execution time (s) for various file sizes for existing vs. proposed method.

4.3. Energy Consumption

To evaluate the effect of utilizing blockchain technology on the sources of the education sector, we calculated the average utilized energy per hour for the servers. Figure 6 displays a comparison between the average utilized energy by such servers with blockchain. It indicates that the proposed blockchain consumes less power than the conventional methods, and hence it proved to be effective in terms of energy utilization.

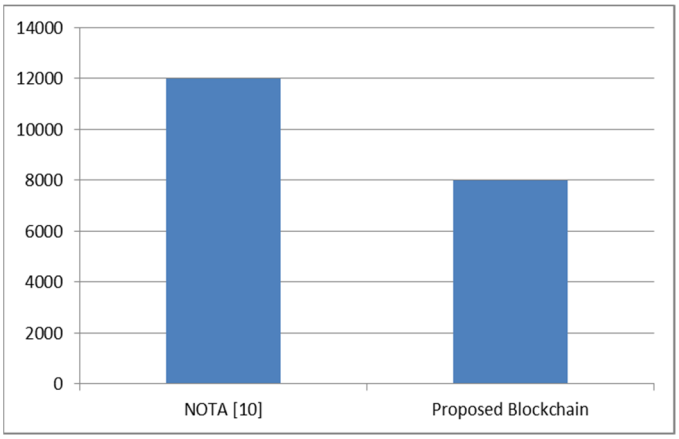

Figure 6. Comparison of energy consumption (Joules) for the existing and proposed method.

5. Conclusions

We have designed and implemented a trust-based blockchain system for the students' performance assessment in the e-learning platform. The suggested system used smart contracts to complete evaluations and courses while also collecting feedback on its advantages. We demonstrated how blockchain technologies could improve transparency and confidence in evaluation processes and educational certificates. In the context of e-learning, we further explained how adaptable access control regulations might be attained on an authorized blockchain. Furthermore, to enhance the trust in the assessment, we have introduced an encryption method using the improved elliptic curve cryptography algorithm (IECCA), which further improved the trust of the evaluation in the e-learning platform. The security level is increased in the proposed system as compared to existing methodologies and the trust is enhanced by the proposed algorithm. By this proposed approach, we got highly secured data transmission with smaller time of execution and energy consumption.

Funding: The author extends his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a Large Group Research Project under grant number 37–40.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Nemade, A.E.; Kadam, S.S.; Choudhary, R.N.; Fegade, S.S.; Agarwal, K. Blockchain technology used in taxation. In Proceedings of the 2019 IEEE International Conference on Vision towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019; pp. 1–4.
2. Rahardja, U.; Hidayanto, A.N.; Hariguna, T.; Aini, Q. Design framework on tertiary education system in Indonesia using blockchain technology. In Proceedings of the 2019 7th International Conference on Cyber and IT Service Management (CITSM), Jakarta, Indonesia, 6–8 November 2019; Volume 7, pp. 1–4.
3. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
4. Gajendran, N. Blockchain-Based secure framework for elearning during COVID-19. *Indian J. Sci. Technol.* **2020**, *13*, 1328–1341.
5. Krishna, A.V.N.; Babu, A.V. Pipeline Data Compression and Encryption Techniques in E-Learning environment. *J. Theor. Appl. Inf. Technol.* **2007**, *3*, 37–43.
6. Lara, J.A.; Aljawarneh, S.; Pamplona, S. Special issue on the current trends in E-learning Assessment. *J. Comput. High. Educ.* **2020**, *32*, 1–8. [CrossRef]
7. Al-Malah, D.K.A.R.; Aljazaery, I.A.; Alrikabi, H.T.S.; Mutar, H.A. Cloud Computing and its Impact on Online Education. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Baghdad, Iraq, 15–16 December 2020; Volume 1094, p. 012024.
8. Naveed, Q.N.; Qureshi, M.R.N.M.; Shaikh, A.; Alsayed, A.O.; Sanober, S.; Mohiuddin, K. Evaluating and ranking cloud-based e-learning critical success factors (CSFs) using combinatorial approach. *IEEE Access* **2019**, *7*, 157145–157157. [CrossRef]
9. Naveed, Q.N.; Qureshi, M.R.N.; Tairan, N.; Mohammad, A.; Shaikh, A.; Alsayed, A.O.; Shah, A.; Alotaibi, F.M. Evaluating critical success factors in implementing E-learning system using multi-criteria decision-making. *PLoS ONE* **2020**, *15*, e0231465. [CrossRef] [PubMed]
10. Bansal, R.; Gupta, A.; Singh, R.; Nassa, V.K. Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic. In Proceedings of the 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 3 July 2021; pp. 194–202.
11. Naveed, Q.N.; Alam, M.M.; Qahmash, A.I.; Quadri, K.M. Exploring the Determinants of Service Quality of Cloud E-Learning System for Active System Usage. *Appl. Sci.* **2021**, *11*, 4176. [CrossRef]
12. Alruwaili, F.F. e-Learning Chain: A Secure Blockchain Approach to e-Learning & Certification Systems. *e-Learning* **2020**, *11*, 16.
13. Li, C.; Guo, J.; Zhang, G.; Wang, Y.; Sun, Y.; Bie, R. A blockchain system for E-learning assessment and certification. In Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 9–11 August 2019; pp. 212–219.
14. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2020**, *23*, 1–23. [CrossRef]
15. Sastry, J.B.; Banik, B.G. A novel blockchain framework for digital learning. *Technology* **2021**, *12*, 15. [CrossRef]
16. Cheriguene, A.; Kabache, T.; Kerrache, C.A.; Calafate, C.T.; Cano, J.C. NOTA: A novel online teaching and assessment scheme using blockchain for emergency cases. *Educ. Inf. Technol.* **2021**, *14*, 1–18. [CrossRef] [PubMed]
17. Liang, X.; Zhao, Q. On the design of a blockchain-based student quality assessment system. In Proceedings of the 2020 International Conference on High-Performance Big Data and Intelligent Systems (HPBD&IS), Shenzhen, China, 23–25 May 2020; pp. 1–7.
18. Sun, X.; Zou, J.; Li, L.; Luo, M. A blockchain-based online language learning system. *Telecommun. Syst.* **2021**, *76*, 155–166. [CrossRef]
19. Ma, S. Using Blockchain to Build Decentralized Access Control in a Peer-to-Peer e-Learning Platform. Ph.D. Thesis, University of Saskatchewan, Saskatoon, SK, Canada, 2018.
20. Shivhare, R.; Shrivastava, R.; Gupta, C. An Enhanced Image Encryption Technique using DES Algorithm with Random Image overlapping and Random key Generation. In Proceedings of the 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India, 28–29 December 2018; pp. 1–9.
21. Rao, V.; Sandeep, N.; Rao, A.R.; Niharika, N. FPGA Implementation of Digital Data using RSA Algorithm. *J. Innov. Electron. Commun. Eng.* **2019**, *9*, 34–37.
22. Dong, X.; Randolph, D.A.; Rajanna, S.K. Enabling privacy-preserving record linkage systems using asymmetric key cryptography. *AMIA Annu. Symp. Proc.* **2019**, *2019*, 380–388. [PubMed]