BLOCKCHAIN BASED TRUST AWARE FRAMEWORK FOR SECURE AND TRANSPARENT CONVENTIONAL ACADEMIC RESULT PUBLISHING SYSTEM

SHEELA D V[1], DR.ASHOK KUMAR T A[2]

[1]Research Scholar, School of Science Studies, Department of Computer Science and Applications,
CMR University, Bangalore, Karnataka, India
[2]Professor, School of Science Studies, Department of Computer Science and Applications,
CMR University, Bangalore, Karnataka, India
E-mail: [1]sheela.dv@cmr.edu.in, [2]Ashokkumar.t@cmr.edu.in

ABSTRACT

In the evolving landscape of educational assessment and result publishing, blockchain technology holds a transformative approach for managing the examination results. The traditional approach for publishing results possesses various challenges including data security vulnerabilities, delayed result distribution, lack of transparency, administrative inefficiencies and so on. Despit recent efforts using online examination platforms and blockchain based grade storage, existing solutions typically do not integrate decentralized tamper proof storage, automated access control and dynamic trust modeling within a single architecture, leaving result data exposed to manipulation, manual entry errors, weak auditability and limited interoperability. This research presents a novel framework for secure and efficient result publishing BTRP (Blockchain based Trust aware Result Publishing). Initially, the proposed model integrates blockchain technology with an efficient distributed database, utilizing Smart Contracts (SC) to ensure secure data storage and sharing. Secondly, we incorporate a trust-aware feedback mechanism into result publishing, allowing participants to receive feedback based on their behaviour. This feedback is dynamically updated on the blockchain through smart contracts, ensuring that only honest and authorized participants have opportunities for data sharing. Additionally, advanced cryptographic mechanisms are incorporated for feedback submission, which protects the privacy of participant information. Front end architecture of BTRP comprises Student, Examiner and Admin as the participants for result publishing; also authorized login dashboard is design for Examiner and admin participants for updation of results. Comparative analysis highlight BTRP's superiority by addressing known limitations of existing e-learning and blockchain academic systems, such as manual data entry vulnerabilities, privacy concern and access control.

Keywords: *Result Data, Blockchain, Consensus, Smart Contract, Access Control*

1. INTRODUCTION

In the educational eco-system, examination results has always been a critical process, serving as a important phenomena for students, educational institutions and various stakeholders participating in the educational journey. this process has evolved significantly, reflecting changes in technological capabilities, educational policies, and stakeholder expectations[1]-[3].Evolution of result publishing model is given as follows:

• Manual to Digital Transition: Initially, exam results were manually calculated, recorded, and published. This process was labor-intensive and prone to human error. With the advent of computers and the internet, educational institutions began transitioning to digital systems, which offered improved efficiency, accuracy, and the ability to handle larger volumes of data.

• Centralized Systems: The digital era introduced centralized systems for result management and publication. These systems allowed for quicker processing and distribution of results but also introduced concerns regarding data security, privacy, and system reliability.

• Online Access and Distribution: Further technological advancements enabled the online publication of results, allowing students to access their scores via websites and dedicated portals. This method significantly reduced the time between result finalization and access, though it often faced challenges related to website crashes due to high traffic, data accuracy, and authentication issues.

The publishing of academic results is a critical process in the educational sector, involving the declaration of students' performance metrics. Traditionally, this process has been predominantly manual and paper-based, leading to numerous challenges, including delays in result publication, risks of data manipulation, and difficulties in result verification. As digital technology has evolved, educational institutions have started to adopt electronic systems for result management. However, these systems often operate in silos and lack interoperability, leading to inefficiencies and increased opportunities for fraud[1][2].

Blockchain technology, a decentralized and distributed ledger system, has emerged as a promising solution to address many of these challenges. By its nature, blockchain offers immutability, transparency, and security, making it an ideal platform for the transparent and tamper-proof recording of academic results. The application of blockchain in result publishing can revolutionize the way academic records are managed, verified, and shared across the educational ecosystem. One of the key technologies with which it does so is smart contracts, providing a framework, on the one hand, with blockchain technology for the automation and securing of processes. These contracts are programmed with predefined rules and conditions. Once the academic results are fed into the system, they shall be immutable, thus tamper-proof. The contract, therefore, enforces that the respective data is of an immutable nature; thus, its integrity and security are observed. This propagates down to access control, whereby the smart contracts establish and enforce who can view, edit, or distribute academic records based on the established user credentials and roles, thus improving privacy and security of information.Smart contracts thus aid in the easing of the verification process, whereby the results are checked against set criteria to greatly increase the speed of the overall workflow and reduce administrative overhead by automation of the results validation. They promote transparency and the possibility of building a trustful environment with the usage of cryptography[4]-[6]. Managing result data and controlling access to result publishing, recent developments primarily focus on improving security, scalability, and efficiency. One significant advancement is the integration of decentralized identity verification technologies, such as zero-knowledge proofs. These technologies allow entities to prove their identity and permissions without revealing any underlying sensitive information, thereby enhancing privacy and security. Additionally, the transition towards more scalable blockchain platforms like Ethereum 2.0, which implements sharding to improve transaction throughput, addresses previous limitations regarding the handling of large datasets typical in educational or organizational result management. However, these advancements also bring forth challenges. Security remains a paramount concern as the complexity of smart contracts can lead to vulnerabilities that hackers might exploit. The immutability of blockchains also poses a problem when incorrect data is recorded—correcting such errors without compromising the decentralized nature of the technology is complex. Furthermore, the user experience often suffers due to the technical nature of blockchain interactions, which can deter adoption by institutions that manage result data. These problems highlight the need for ongoing research and development to refine the technology and make it more accessible and secure for widespread use.

Despite the potential benefits of blockchain technology in revolutionizing the result publishing model, several challenges hinder its widespread adoption. The primary problem lies in the integration of blockchain technology with the existing educational infrastructures, which are often outdated and resistant to change. There is a need for a comprehensive strategy that addresses the technological, organizational, and cultural barriers to the adoption of blockchain in educational institutions[7]-[11].

Furthermore, there is a lack of understanding and consensus on the standards and protocols for implementing blockchain-based result publishing systems. This includes issues related to scalability, privacy, and the management of digital identities on the blockchain. Educational institutions also face challenges in ensuring the security and integrity of result publishing data while facilitating their accessibility and verification across different stakeholders, including students, employers, and educational institutions globally[12].

1.1 Motivation and contribution

The rapid evolution of digital technology has accelerated the transition from manual to electronic suystems for academic result management. The traditional electronic systems often operate in silos, lacking interoperability which results in inefficiencies, data inconsistencies and susceptibility to fraudulent activities. Blockchain technology provides a compelling solution to these challenges by decentralization, immutability and transparency. This research is motivated by potential of blockchain and smart contract to revolutionize academic result publishing to enchance security, integrity and accessibility. By integrating blockchain with existing educational infrastructure, the study aima to bridge technological and employers to strengthen the global credibility of academic credentials.

The key contribution of this research:

- Innovative Blockchain Framework for secure and transparent academic result publishing using blockchain and smart contract to enhance data integrity, tamper-resistance and verifiability, overcoming the limitations of centralized systems.

- The Blockchain Integration into existing academic infrastructure address technological, organizational and cultural barriers which enables the smoother adoption for institutions.

- Introducing Trust Management via smart contract and Feedback management mechanism to evaluate the credibility of examination authorities and result performance.

- The system is implemented using Solidity. MetaMask and Ganache. The framework performance evaluates the security, efficiency and real world feasibility through performance testing.

2. RELATED WORK

Several innovative approaches have been introduced in the realm of e-learning and online examination systems, enhancing both the security and efficiency of these platformsReference [13] introduced a pioneering model for e-learning platforms that incorporates cryptocurrency payments for examinations. This model leverages blockchain technology to securely store exam data as smart contracts. However, a potential vulnerability was identified, where the manual entry and database storage of student addresses could be manipulated, potentially compromising the accuracy of student results. In contrast, reference [14] developed a web-based online examination system that streamlines the exam process. This system facilitates the delivery of exam questions and the collection of responses, which are then processed on a server to generate student grades automatically. To further enhance the integrity of online exams, reference [15] implemented an online examination system equipped with face detection technology. This innovation aims to prevent cheating by verifying the identity of students during exams. Upon completion, the system automatically calculates and displays the students' marks. [16] proposed a comprehensive web-based examination system that supports various question types, including multiple-choice questions (MCQs) and essay questions. This system evaluates the difficulty level of questions to improve exam assessment and includes features for automatic marking and generating detailed exam reports.[17] designed a web application to address common issues in existing online examination platforms. This solution includes features such as automatic student logout after the allotted exam time, auto-submission of answers, and auto-marking, alongside generating reports on examination results. It utilizes front-end web development technologies and SQL Server for database management. [18] explored the use of the Ethereum blockchain and smart contracts for storing students' course information and grades at the University of Glasgow. This approach ensures transparency and trustworthiness in grade recording, although a complete case study to validate the system's effectiveness was not provided. [19] crafted an online testing system that employs blockchain technology and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) to enhance security. This system allows only authorized teachers to set exam questions using their private keys, thereby controlling access through the CP-ABE algorithm.Lastly, reference [20] introduced a novel verification framework for centralized ledger databases (CLD), focusing on enhancing external auditability and swift verification. This framework, known as Dasein verification, emphasizes a comprehensive validation process that includes verifying the what, when, and who of transactions to ensure a robust auditing mechanism.

Existing systems have yet to fully harness the decentralized, tamper-proof capabilities of blockchain for secure and transparent academic record-keeping. There is also a noticeable lack of consensus on standards and protocols for implementing such systems, which hampers scalability and cross-institutional operability.

Additionally, there is a need for robust mechanisms for managing digital identities and ensuring data privacy within the blockchain framework. The challenges extend to the legal and regulatory recognition of blockchain-based academic credentials, which remain largely unaddressed. This indicates a substantial need for comprehensive strategies that not only enhance the security and integrity of digital records but also facilitate their accessibility and verification in a globally interconnected educational landscape.

Problem Statement: The academic result publishing process in many institutions still relay on centralized, siloed system that are vulnerable to data tampering, suffer from delayed, opaque result dissemination and lack robust mechanisms for privacy preserving verification. Despit recent efforts using online examination platforms and blockchain based grade storage, existing solutions typically do not integrate decentralized tamper proof storage, automated access control and dynamic trust modeling within a single architecture, leaving result data exposed to manipulation, manual entry errors, weak auditability and limited interoperability. This work addresses the problem of designing and evaluating blockchain based, trust aware result publishing framework (BTRP) that can be provide secure, transparent and privacy-perserving result management while quantifying and enchancing the credibility of participating institutions and platforms.

3. PROPOSED METHODOLOGY

This section of the paper focuses on the various methodologies that are implemented in this study and their interactions. It aims at data sharing being efficient as well as secure for result publishing, where a blockchain mechanism is developed to achieve this. The study involves result publishing during the process of data sharing. Various blockchain units are used in the proposed system model work interactively and act as a ledger for the storage of results that are published. This is implemented using Smart Contract for management of data and access control, mechanism of data sharing and Trust Management.

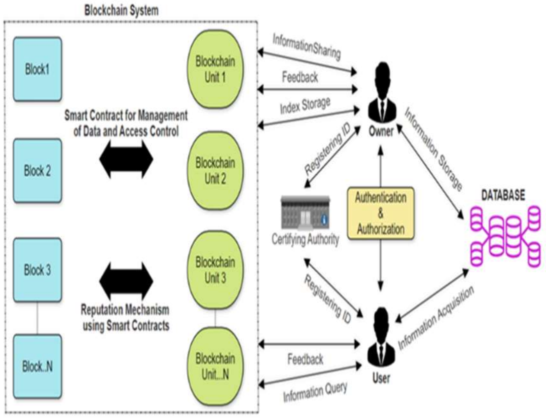

Figure 1 BTRP (Blockchain based Trust aware Result Publishing) architecture

3.1 BTRP (Blockchain based Trust aware Result Publishing)

There are various blockchain units that are used in this section of the paper. The first unit is utilized for deployment of contract while the rest of the blockchain units are used for transactions in the ledger. The blockchain method is used for storing the results that are published acting as a ledger. It assures integrity of data as well as prevents unauthorized access. This mechanism is essential for the authenticity and accuracy of results that are published. For data sharing, crucial data is transmitted to the blockchain process to be published as well as validated. The traditional blockchain system is modified and a hybrid system is adopted that includes an on and off- chain for verification. Every blockchain unit handles the verification that has computations for cryptography as well as encapsulation of the text that is verified into transaction of blockchain. Various parameters that are essential have to be verified which is performed by smart contracts, further a new unit for the transactions that are right is introduced and is written, lastly this unit is combined to the blockchain system using the algorithm for consensus. The transaction consists of its information, respective hash ledger as well as signature of the blockchain unit. The types of transactions that are utilized here are: storing information, information sharing, feedback as well as feedback updating. These transactions are transparent in nature in the blockchain and can be accessed globally. The users can access these transactions by the use of interface that is given by the smart contracts. This also challenges the security of the system; hence the smart contracts keep record of the user account address as well as every blockchain unit's public key. This makes sure that only the blockchain unit that has access can write transactions in the system. The proposed system also uses smart contracts for management of information and access control as well as Trust Management consisting of computations and storage operations.

3.1.1 **Trust and Feedback aware smart contract for result publishing**

This mechanism is utilized for the evaluation of extent of reliability of the institutions and boards that are involved in conducting the examinations while considering the publication of result to be accurate and timely. Additionally, this scheme can also be utilized for feedback of the platforms or interfaces that are used to obtain these results by the users, aiming at information security, experience of user as well as extent of reliability. The relevance and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

usability of this mechanism is altered according to the specific requirements of publishing.

This mechanism involves two major records namely KeyRecord and RevokeRecord. It also uses functions that include map() to record the public key of the students along with the repuation data. The KeyRecord has a list of the student users that access the result that is published while the students that update the value for feedback lower than the threshold is stored in RevokeRecord. The various functions that are utilized for this method is described in detail.

The initialization of the process is performed by the Init() for feedback data of a new student users. While the public key of the student is known 〖PublicKey〗_k, firstly it is established that the 〖PublicKey〗_k is not present in the already existing two records that are mentioned earlier. Once this condition is met, 〖PublicKey〗_k is added to the KeyRecord and feedback data is to be initialized for the student. 〖RepValue〗_k is used to denote the initial value of feedback that is assigned by the system. The total count of feedback received for feedback is expressed as P. Hence, for a new user 〖RepValue〗_k,P=0,NULL,NULL.

The feedback data of the students is obtained by the function Obtain_Feedback(). Here, 〖PublicKey〗_k is used as the input and this function ensures that 〖PublicKey〗_k is present in the KeyRecord.

FeedbackRecord() is the function that ledgers the feedback for feedback. The transaction for the feedback is considered input that is 〖PublicKey〗_k,E_k. In this case, the feedback rating that is encrypted is denoted as E_k. The function has to check for condition that 〖PublicKey〗_k is present in KeyRecord. If the condition is satisfied then the feedback rating E_k is recorded and a relation with 〖PublicKey〗_k is established.

ReceiveRating() is the function used to obtain the ratings that are given as feedback by the users within a particular time period, while considering 〖PublicKey〗_k as well as time period as the input. The function has to check for condition that 〖PublicKey〗_k is present in KeyRecord. If the condition is satisfied then returns the feedback for feedback associated with 〖PublicKey〗_k withing the specified time frame.

The student data is updated using the function Updating(). In this case, the input is 〖PublicKey〗_k,PRating,NRating,E_V, 〖Decrypt〗_V. Here, the positive as well as the negative rating that is obtained by the student in the recent time frame is denoted as PRating and NRating respectively. The combined feedback value of all the ratings that is encrypted within the specified time is given as E_V, while the parameter used for decryption is expressed as 〖Decrypt〗_V. The ratings that are positive as well as negative can be verified and validated using the parameters E_V and 〖Decrypt〗_V. The initial task of the function includes to check for condition that 〖PublicKey〗_k is present in KeyRecord. If the condition is satisfied then queries are performed on the feedback data that is related with 〖PublicKey〗_k, prior feedback value 〖RepValue〗_oldas well as the count of feedback P_old. The updated feedback data is formulated as given below using the parameters 〖RepValue〗_new, P_new,E_V and 〖Decrypt〗_V.

$$P_{new} = PRating + NRating + P_{new} \text{ ----------- } (1)$$

〖RepValue〗_new= ((ω_1.PRating+ω_2.NRating) (P_new)^(-1))+ 〖RepValue〗_old.P_old/P_new ----------------(2)

Considering the equations (1) and (2) given above, the incentive factor is denoted as ω_1, the penalty factor is indicated as ω_2 and lastly the threshold for feedback is given as ω_V. The function verifies if the updated value meets the following constraint 〖RepValue〗_new is greater than ω_V. If the condition is satisfied the updated data is added to the ledger, else KeyRecord and 〖PublicKey〗_k is revoked and the 〖PublicKey〗_k to added to the RevokeRecord and finally the student data is deleted. The algorithm for the Trust Management using Smart Contracts is given in detail below

Algorithm	**Trust Management using Smart Contracts**
Step 1	Users;
Step 2	$Feedback \{ int\ RepValue, P; string\ E_V, Decrypt_V \}$
Step 3	*Feedbackvalue {string ev; int time}*
Step 4	Set $\omega_1, \omega_2, \omega_V$.
Step 5	*Map(* *string is greater than or equal to R* *) RepRecord;*
Step 6	*Map(* *string is greater than or equal to F* *) FeedbackRecord;*
Step 7	create *KeyRecord, RevokeRecord;*
Step 8	//Function $Init(PublicKey_k)$
Step 9	$message.send = owner$

Step 10	$PublicKey_k$ is not in *KeyRecord, RevokeRecord;*
Step 11	*KeyRecord.push(*$PublicKey_k$*)*
Step 12	$RepValue_k = \frac{\omega_1+\omega_2}{2}$
Step 13	*RepRecord(*$PublicKey_k$*)=* $(RepValue_k, 0, NULL, NULL)$
Step 14	//Function *Obtain_Feedback(*$PublicKey_k$*)*
Step 15	$PublicKey_k$ in *KeyRecord*
Step 16	Return (*RepRecord[*$PublicKey_k$*]*)
Step 17	//Function *FeedbackRecord(*$PublicKey_k, E_k$*)*
Step 18	$message.send = owner$
Step 19	$PublicKey_k$ in *KeyRecord;*
Step 20	*FeedbackRecord[*$PublicKey_k$*].push(* $E_k, block.time$*)*
Step 21	//Function *ReceiveRating(* $PublicKey_k, initial_{time}, final_{time}$*)*
Step 22	$PublicKey_k$ in *KeyRecord;*
Step 23	Create *evRecord;*
Step 24	For every *Feedbackvalue* in *FeedbackRecord [*$PublicKey_k$*]* do
Step 25	If $initial_{time}$ *is less than or equal to Feedbackvalue.time is less than or equal to* $final_{time}$ *then*
Step 26	*evRecord.push(Feedbackvalue. ev);*
Step 27	Return *evRecord;*
Step 28	//Function *Updating(* $PublicKey_k, PRating, NRating, E_V, D$ *)*
Step 29	$message.send = owner$
Step 30	$PublicKey_k$ in *KeyRecord;*
Step 31	$P_{old} = Reputationdata[Publickey].P;$
Step 32	$RepValue_{old} = Reputationdata[Publickey].RepVal$
Step 33	Computation of $RepValue_{new}, P_{new}$
Step 34	If $RepValue_{new}$ *is greater than* ω_V then
Step 35	*RepRecord[*$PublicKey_k$*]=(* $RepValue_{new}, P_{new}, E_V, Decrypt_V$*)*
Step 36	Else
Step 37	Revoke $PublicKey_k$ in *KeyRecord*
Step 38	*RevokeRecord.push(*$PublicKey_k$*);*

3.1.2 Smart Contract for Management of Result Data and Access Control

The process of result publication can be automated using smart contracts for management of data. Such as, rules and constraints can be applied in regard to the users who have to access the data. For instance, only students having credentials that are correct as well as approved by the institutions can access the results that are published. This also enhances the security of the proposed system. The Smart contract for management of Data invokes the Trust Management initially to gather the student user information and designs a keyword record KeywordRecord. The map() is used for construction of list relating to the keywords along with the withheld stored data. Additionally, ShareRecord is utilized for sharing information transactions among the student users.

The functions utilized for this algorithm are explained in detail below. The index list for the information inside the blockchain is established using the function Store(). This transaction uses input as (Keyword, 〖PublicKey〗_onwer, loc, 〖rand〗_owner , 〖RepValue〗_owner, 〖RepValue〗_V). Here, the keyword and stored information location is denoted as Keyword and loc respectively. The feedback value for the information owner as well as the threshold that is established by the owner is denoted as 〖RepValue〗_owner and 〖RepValue〗_V respectively. The random number that is used at the time of encryption of information is denoted as 〖rand〗_owner. 〖PublicKey〗_onwer and 〖RepValue〗_owner and firstly verified to be right before invoking the function Obtain_Feedback(). If the range of 〖RepValue〗_V is correct then Keyword is added to KeywordRecord. The pertinent information of stored transactions is obtained using the Search(). The input taken is Keyword, which is checked to be present in KeywordRecord. If so, all the relevant information is retrieved. The transactions for sharing of information is performed using Sharing() for student users, having input 〖PublicKey〗_onwer, 〖PublicKey〗_user, 〖ID〗_transaction. The working and algorithm for this process is explained in detail below.

Algorithm	**Smart Contract for Management of Data and Access Control**
Step 1	Owner location;

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 2	*Store{string* $PublicKey_{onwer}, rand_{owner}, loc, RepV$ *}*
Step 3	*Sharing{string* $PublicKey_{onwer}, PublicKey_{user}, ID_{transaction}$ *}*
Step 4	*Map(* $string\ equal\ to\ or greater\ than\ stor$ *) StoreRecord;*
Step 5	Create $string$[] *KeywordRecord*
Step 6	Create sharing[] *ShareRecord*
Step 7	//Function *Store(Keyword,* $PublicKey_{onwer}$, *loc,* $rand_{owner}$ *,*$RepValue_{owner}, RepValue_{V}$*)*
Step 8	$message.send = owner;$
Step 9	$PublicKey_{onwer}$ in *KeyRecord*
Step 10	$RepValue_{owner}$ is not false;
Step 11	$0\ less\ than\ equal\ to\ RepValue_{V}$ && R
Step 12	*StoreRecord[Keyword].push(Keyword* *,* $PublicKey_{onwer}$, *loc,* $rand_{owner}$ *,*$RepValue_{owner}, RepValue_{V}$*)*
Step 13	*KeywordRecord.push(Keyword)*
Step 14	//Function *Search(Keyword)*
Step 15	*Keyword* in *KeywordRecord*
Step 16	Return (*StoreRecord[Keyword])*
Step 17	//Function *Sharing(*$PublicKey_{onwer}$, $PublicKey_{user}$, $ID_{transaction}$*)*
Step 18	$message.send = owner;$
Step 19	$PublicKey_{onwer}$, $PublicKey_{user}$ in *KeyRecord*
Step 20	$RepValue_{user}\ greater\ than\ or\ equal$
Step 21	*ShareRecord.push(*$PublicKey_{onwer}$, $PublicKey_{user}$, $ID_{transaction}$*)*

3.1 Secure Result Publishing

a. Initialization Phase

System Setup by the Certificate Authority (CA): The CA configures the system by defining cryptographic parameters such as the prime field, elliptic curve coefficients, and three cyclic groups . It also establishes a hash function and a bilinear pairing function, and it generates keys for managing identities and feedback.

Registration of Blockchain Members (BMs): Each member of the blockchain selects a private key, derives the corresponding public key, and publishes it. They initialize the blockchain ledger and deploy smart contracts for managing the system.

Identity Verification and Certification: users apply to the CA by securely transmitting their unique IDs and public keys. The CA checks for any prior registrations, signs the data, and issues identity certificates.

Feedback Certificate Issuance: To maintain anonymity in feedback processes, users register for special certificates. They submit commitments along with zero-knowledge proofs to validate these commitments.

b. Data Sharing Phase

Secure Data Storage: Data owners encrypt files using keys generated from their private keys combined with random numbers. The encrypted data and its metadata are stored in a blockchain-accessible distributed database.

Data Access Requests: Data users request access to specific data by looking up transactions on the blockchain using predefined keywords. They must satisfy the feedback criteria set by the data owners to proceed.

Authorization for Data Sharing: Upon successful verification of the data user's credentials and feedback score, the data owner shares an encrypted decryption key. This allows the data user to access the requested data securely.

c. Feedback and update phase

Feedback Submission and Confirmation: After the data sharing transaction, participants rate each other's conduct. This feedback, encrypted for security, is submitted to the blockchain where it is verified and logged by blockchain members.

Rating Aggregation and Feedback Adjustment: Feedback ratings are gathered and decrypted collectively by blockchain members to update feedbacks. This leverages homomorphic encryption to ensure privacy and accuracy.

Resolution of Disputes Over Ratings: The system provides mechanisms for addressing disputes over feedback. Users can challenge negative ratings, leading to verification and potential adjustment of feedbacks based on the evidence provided.

4. EXPERIMENTAL SETUP

The experimental configuration involves implementing the proposed system within a testing environment. Solidity programming is used for constructing and designing smart contracts on Blockchain platforms. It's used to create smart contract. contracts that implement business logic and generate a chain of transaction records in the blockchain system. Meta Mask is crypto currency wallet that is equipped with a key vault, secure login, its token wallet, and token exchange everything you need to manage your digital assets. We can use to pay by crypto currencies or if someone wants to receive crypto. We will use it here to get ID account on the Ethereum network, then check if the user belongs to this network or not and pay the crypto to submit answers to the network. Ganache helps us to test or inspect states as it gives us a bench of private keys that can generate address with it for enabling us to run tests. It allows us as well to check if there is a new block that has been added to blockchain and the amount of crypto taken form account per transaction. It will be used to have a similar situation like a local blockchain network to run our module test and make transactions to save data in blockchain network.

In the process of developing our blockchain-based system for results publication, we employed the Truffle Suite, a widely used development environment and testing framework for Ethereum smart contracts. Post-deployment, Truffle saved the contract artifacts, which contain the ABI and the deployed address, among other pieces of information. These artifacts are vital for the front-end of our system to interact with the deployed smart contract.

4.1 Blockchain based Result Publishing

This section of the results shows the user interface based application. The blockchain based academic result publishing system is designed with three primary participants: Student, Examiner, Administartor(University)

Figure 2 showcases a streamlined student web interface, admin dashboard and examiner dashboard to publish and view the academic results.

- Roll Number and Student Name Input Fields ensure that authorized students can access their academic record.
- Submit/View button – on submission, the system fetches result from the blockchain ledger.
- Results are retrieved from the blockchain which guarantess the data integrity and instant verification.

The interface ensures that student can securely view their academic result without the risk of unauthorized modification.

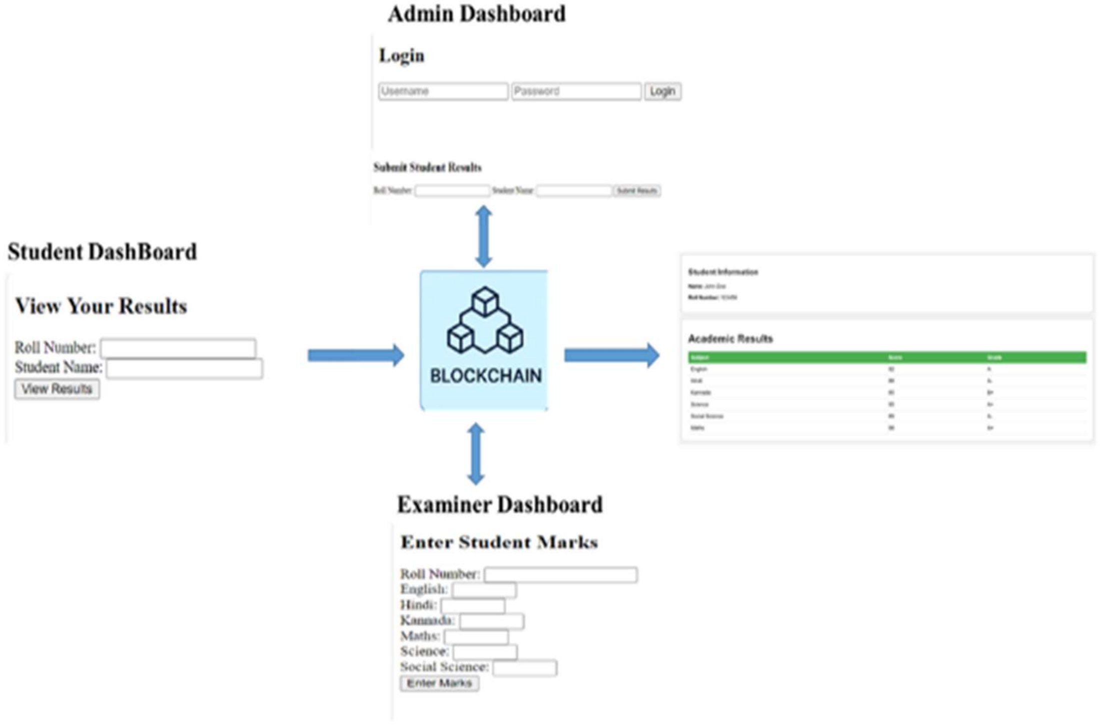

Figure 2 The interface for blockchain based academic result publishing system

4.1.1 Examiner

Figure 2 displays an examiner's dashboard designed for entering academic marks. The interface includes a form with fields for the student's roll number and marks for various subjects including English, Hindi, Kannada, Maths, Science, and Social Science. After inputting the scores, the examiner can submit the data through the "Enter Marks" button, which would likely store the information in a centralized database or a blockchain ledger for secure and permanent and tamper proof record keeping. This tool streamlines the process of mark entry, ensuring efficiency and accuracy in the evaluation process.

By leveraging blockchain based storage, the examiner interface ensures that all submitted marks are:

- Immutable – Once recorded, marks cannot be altered without authorization
- Transparent – Authorized participants can verify submissions
- Efficient – Streamlines the evaluation and result publishing process.

4.1.2 Admin dashboard

Figure 2 depicts an administrative dashboard for submitting student results. It features a form with input fields for "Roll Number" and "Student Name," followed by a "Submit Results" button. This interface would typically be used by school administrators to officially record students' final grades into the system after they have been verified and finalized. It simplifies the administrative process, allowing for an organized and efficient way to handle student academic records. The login interface with fields for "Username" and "Password," followed by a "Login" button. It's a standard login screen design that would be the entry point for users to access a secure area of a website or application, such as an admin panel or a dashboard for a management system. Once the credentials are submitted the system performs verification by cross checking the encrypted credentials stoored in the blockchain backed database. Once authenticated all subsequent transactions are recorded on chain for integrity.

5. RESULTS AND DISCUSSION

The evaluation of BTRP highlights its strong performance in both efficiency and scalability for academic result publishing. As the number of authorized accesses rises, the result publishing time increases in a linear pattern while maintaining low latency. This demonastrates the system's ability to process multiple credentials simultaneously without delays. Similarly, publishing data to the blockchain exhibits a linear growth in time, indicating the additional data is managed effectively without causing significant computational overhead. Throughput analysis confirms that the system can scale with heavier transaction loads, sustaining a satisfactory transaction per second (TPS) rate.

5.1 Throughput

Throughput represents the speed at which a system can handle requests or complete operations within a specific period. For, blockchain based platforms, it is commonly expressed as Transactions Per Second (TPS), which measures how many successful transactions the network can process each second. Achieving high throughput is essential for handling numerous operations concurrently, particularly during peak activity periods. This capability enchances the system's scalability and contributes to its overall performance and efficiency.

Table 1 BTRP throughput comparison

No of Transactions	Throughput
4	2.7
8	3.2
12	4.5
16	5.3
20	6.1

The graph illustrates the correlation between transaction volume and throughput in the BTRP system. As transaction increase from 4 to 20, the throughput rises accordingly, reflecting enchanced system performance. The throughput is 2.7 TPS at 4 result publishing transaction loads. It demonstrate the system's capability and reliability as transaction volume grows.

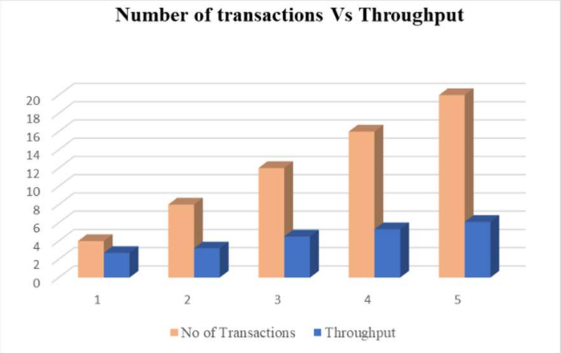

Figure 3 Throughput

5.2 Latency

Latency refers to delay between initiating a request and receiving the corresponding response. In blockchain environments, it represents the duration required for a transaction to be processed and validated on the network. Reduced latency enables faster transaction completion, which is critical for enchancing system responsiveness and delivering a better user experience, particularly for application that demand real time operations such as result publishing.

Table 2 BTRP Latency comparison

No of transactions	Avg Latency (s)
4	15
8	18.5
12	22
16	30
20	35

The table 2 and figure 4 show the Average Latency for different numbers of transactions in the BTRP system: The average latency starts at 15.0 seconds for 4 transactions and increases to 35.0 seconds for 20 transactions. The graph demonstrates a steady increase in latency with the number of transactions, reflecting the growing time required as the system handles more transactions. This updated latency data suggests improved efficiency compared to the previous values, maintaining lower latency, making BTRP scalable.

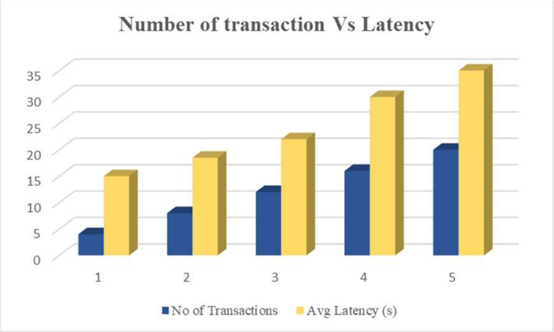

Figure 4 Latency

5.3 Comparative Analysis with Existing Model

Table 3 shows the comparsion between the BTRP framework demonstrates significant advancements over exisiting systems in the domain of secure academic result management. A comprehensive comaparative analysis reveals that BTRP not only integrates the strengths of prior approaches but also introduces novel mechanisms in trust management, privacy preservation and automated integrity enforcement.

Table 3 Comparative Analysis between BTRP and existing model

Features	**BTRP (Proposed System)**	**Crypto-based e-learning[21]**	**Blockcerts [22]**	**Ethereum based Information system [23]**
Blochchain for results	Yes(Full storage)	Yes(Smart Contract)	No	Yes (Grades)
Immutability	High	Medium	low	High
Access Control	Dynamic	Static	Role-based	Role-based
Trust Management	Yes(Credibility scoring)	No	No	No
Privacy Protection	ZKP+Encryption	Partial	None	Basic
Automated Verification	Yes(Smart Contract)	Partial	Yes	Yes
Anti-Tampering	High(Trust +Immutability)	Vulnerable(Manual entry)	Low	Medium
Scalability	High(6.1 TPS)	Moderate	Moderate	Moderate

6. CONCLUSION

The proposed framework addresses significant challenges inherent in traditional result publishing methods, including issues of security, transparency, and efficiency. Through the development and implementation of a blockchain-based system, the study showcases how academic records can be managed in a more secure, immutable, and accessible manner. The findings highlight the potential of blockchain technology to revolutionize the educational sector, providing a robust solution for the verification and sharing of academic achievements. Experimental evaluation within an ethereum-based environment demonstrates the framework’s efficiency, scalability and robustness through performance metrics such as transaction throughput and latency under varying load conditions. Comparative analysis with existing e-learning, blockchain credential and online examination system highlights BTRP’s superiority in incorporating automated verification, trust management and privacy preservative features. Furthermore, the research opens avenues for future studies to explore the integration of blockchain in various educational processes, emphasizing the need for continuous innovation and adoption of digital technologies in academia. This work stands as a testament to the transformative power of blockchain, paving the way for its wider acceptance and implementation in educational institutions worldwide.

Declaration:

Funding Declaration: The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Ethical approval: Not applicable, did not involve human or animal participants.

AI Writing: Not used any AI tool of write the paper.

REFERENCES:

[1] Deenmahomed, Haïdar AM, Micheal M. Didier, and Roopesh K. Sungkur. "The future of university education: Examination, transcript, and certificate system using blockchain." *Computer Applications in Engineering Education* 29.5 (2021): 1234-1256.

[2] Agrawal, Kanika, et al. "An extensive blockchain based applications survey: Tools, frameworks, opportunities, challenges and solutions." *IEEE Access* 10 (2022): 116858-116906.

[3] Do, Ba-Lam, et al. "Blockchain for Education: Verification and Management of Lifelong Learning Data." *Computer Systems Science & Engineering* 43.2 (2022).

[4] Ali, Sura I. Mohammed, Haitham Farouk, and Hussien Sharaf. "A blockchain-based models for student information systems." *Egyptian Informatics Journal* 23.2 (2022): 187-196.

[5] Pfeiffer, Alexander, et al. "Blockchain technologies for the validation, verification, authentication and storing of students' data." (2020).

[6] Chivu, Raluca-Giorgiana, et al. "The role of blockchain technologies in the sustainable development of students' learning process." *Sustainability* 14.3 (2022): 1406.

[7] Sikuyuba, Mweemba, and Jackson Phiri. "The Management of Examination Malpractice Using Blockchain Technology." *Computer Science On-line Conference*. Cham: Springer International Publishing, 2022.

[8] Samanta, Ashis Kumar, Bidyut Biman Sarkar, and Nabendu Chaki. "A blockchain-based smart contract towards developing secured university examination system." *Journal of Data, Information and Management* 3 (2021): 237-249.

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

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

[11] Singh, Anuraj, and Vishwas Singh Kushwaha. "Result Publishing System Using Asymmetric Key Encryption." *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*. IEEE, 2022.

[12] Thilagavathi, M. "Blockchain-based framework for online entrance examination and score card verification system." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.1S (2021): 388-398.

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

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

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

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

[17] T. M. Fagbola, A. A. Adigun, and A. O. Oke, ''Computer-based test (CBT) system for university academic enterprise examination,'' Int. J. Sci. Technol. Res., vol. 2, no. 8, pp. 1–7, 2013.

[18] J. Rooksby and K. Dimitrov, ''Trustless education? A blockchain system for university grades1,'' Ubiquity, J. Pervasive Media, vol. 6,

no. 1, pp. 83–88, Nov. 2019, doi: 10.1386/ubiq_00010_1.

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

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

[21] Chen, L., and Zhang, Y. “A Blockchain-Based Cryptocurrency Framework for Secure E-learning System,” in International Journal of Educational Technology in Higher Education, 20(1), pp. 45, doi: 10.1186/s41239-023-00412-1.

[22] Narayanan, A., and Rajkumar, B.(2022). “Design and Implementation of a Secure Online examination System with Automated Submission and Evaluation,” in Journal of Information Technology in Education, 21(3), pp. 112-128, doi: 10.18002/jite.v21i3.7012.

[23] Brown, A., Balasubramaniam, S., and McGettrick, A. (2021), Blockchain-Based Academic Transcript Management: A Case study at the University of Glasgow. IEEE Access, pp. 104567-104578, doi:10.1109/Access.2021.3098765