International Journal of Applied Engineering & Technology

EXPLORING THE POTENTIAL OF BLOCKCHAIN TECHNOLOGY FOR ACADEMIC CREDENTIAL VERIFICATION

[1]Nagaraju Kasukurthi, [2]Dr. Gangadhara Rao Kancharla and [3]Dr. Neelima Guntupalli
[1]Research Scholar, Department of Computer Science and Engineering, University College of Sciences, Acharya Nagarjuna University
[2]Professor, Department of Computer Science and Engineering, University College of Sciences, Acharya Nagarjuna University
[3]Assistant Professor, Department of Computer Science and Engineering, University College of Sciences, Acharya Nagarjuna University
[1]knraju.dwh@gmail.com, [2]kancherla123@gmail.com and [3]neelima.guntupalli80@gmail.com

ABSTRACT

Information is vital for promptly gauging the efficacy of educating. There are inconsistencies and mistakes in educational data since it is often locked in centralised systems. As a consequence of this disintegration, there have been many missed chances, disputes about academic degrees, and ongoing uncertainty over the efficacy of learning. The centralisation of systems has its advantages, but the resulting opaqueness has been a major drawback. To solve this problem, the team has created a protocol for the blockchain that validates credentials obtained via recognised online courses as well as those obtained locally. The immutability, dependability, and precision offered by this technology are unparalleled.Establishing a platform of transparent, verifiable data will pave the way for many blockchain-based applications that seek to improve educational efficiency and equity. By using this protocol, make sure that academic records cannot be altered and can be readily verified. This will make it easier to check credentials and lessen the likelihood of credential fraud. Therefore, this blockchain technology promotes a decentralised perspective on academic achievement, which is advantageous for teachers and students alike.This protocol improves educational data management and ensures stakeholders have correct and trustworthy information. Blockchain technology may boost education efficiency and transparency. This improves the e-learning experience and fosters faith in educational credentials, improving educational results and opportunities for everyone.

Keywords:Academic Degrees, Blockchain, Educational Efficiency, Credential Fraud, E-Learning.

1. INTRODUCTION

Blockchain technology essentially consists of an immutable ledger that records all transactions that have taken place on the network [1]. The technology that was developed by a group of committed programmers under the pseudonym "Satoshi Nakamoto" to storeBitcoin transactions is currently used in other sectors, including healthcare [2], finance, insurance, and law [3]. Blockchain has grown from its early success to become the backbone of every single decentralised application in existence. Since this, and since smart contracts may now be executed, its usage has reached new [4], unparalleled levels.Two parties may transfer assets to one other using software called a smart contract, provided that both parties meet certain conditions. The first step in the basic smart contract life cycle is to record the contract conditions on a ledger that is distributed [5-7]. Thereafter, they become associated with databases and systems, both internal and external. Predefined conditions are evaluated by external elements [8], and the contract waits for their decision.

Lastly, the contract is designed to self-execute when certain circumstances are met via predetermined triggers [9]. Many different types of business applications have been drawn to the ease of using public smart contracts [10], which are a subset of smart contracts deployed on public blockchains. The purpose of this article is to lay out the best practices for using distributed ledger technology (DLT) in online education [11], including blockchain and smart contracts.

Students may get their credits in a blockchain wallet to a decentralised Solidity smart contract they built [12-14]. Tokens are created from the credits and then transferred. Hashing and public key encryption are used to ensure security [15]. Each student and school that signs up for the blockchain is given their private key. A student's blockchain wallet is credited with a token after they finish a registered course [16]. The suggested system is secure since it has been tested against several threats and determined to be impervious to them. Load testing [17], in which the number of institutions using the blockchain platform is increased and the maximum and lowest response times are examined [18], is used to assess the system's scalability.

Solidity is the language used to program the Ethereum smart contract. This article presents a blockchain-based token-based credit transfer ecosystem that is being considered by higher education institutions. Each student has a wallet where they save the tokens that represent their course credits [19]. As they finish each course, their tokens grow. After students finish each course, their instructors will deposit course credits into their wallets using their unique address identifier [20], which is a blockchain with the student's public and private keys digitally signed.

The remaining portion of this paper is structured into five parts. Section2 delves into the Ethereum blockchain platform's design, which is used for credit transfer. Section 3 gives some background on the algorithms used in credit transfer. In Section 4, the proposed system is compared to current credit transfer mechanisms and its scalability and safety are analysed.

2. MODEL FOR THE SYSTEM

Data storage is a crucial component of the system. As seen in Figure 1, understanding how to save and retrieve (process) the data is crucial.

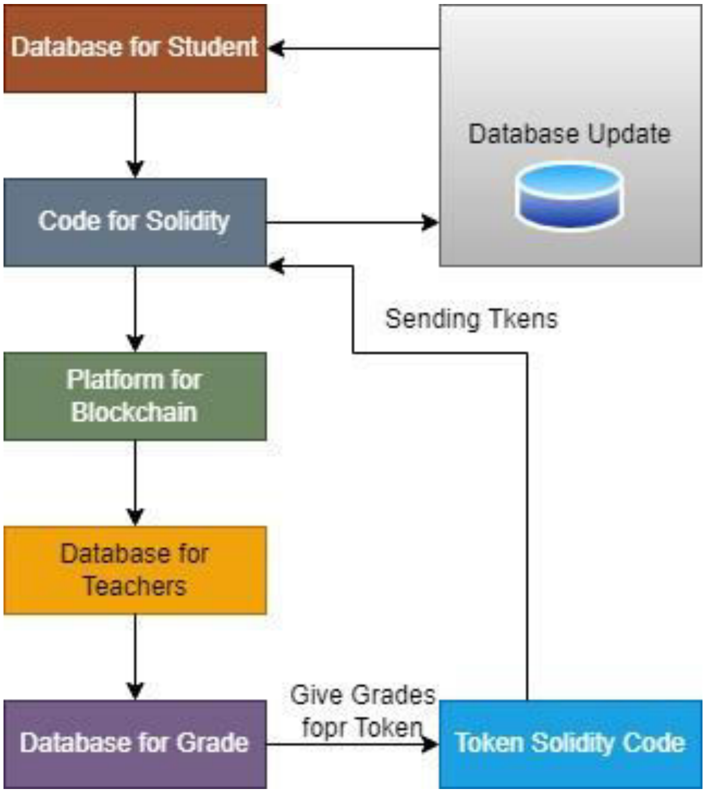


Figure 1: Save and Retrieve Data Process

The database's foundational data is first housed in a.csv file. Students' names, registration numbers, payment details, gender, section, enrolled courses, passwords, blockchain addresses, public keys, and private keys are all part of the metadata included in this CSV file. A student's public key, together with their user ID and password, is required to access the student database. Thethird-party will check the connections between each student and the instructor database once they're in, and it will communicate via the Solidity code base. Everything from grades to credits may be changed by individual teachers for each class. Solidity updates the student database after converting them into the necessary tokens, as seen in Figure 1.

To facilitate the distribution of credits to students via a blockchain wallet, we built a decentralised Solidity smart contract. Tokens are created from the credits and then transferred. Hashing and public key encryption are used to ensure security. Each school and student that signs up for the blockchain receives their unique private key. A student's blockchain wallet will be credited with a token after they finish a registered course.The suggested system is secure since it has been tested against several threats and determined to be impervious to them. An increase in the number of colleges signing up for the blockchain platform allows for load testing to determine the system's scalability by comparing the highest and lowest response times.

3. IMPLEMENTATION

Solidity is the language used to program the Ethereum smart contract. This article presents a blockchain-based token-based credit transfer ecosystem that is being considered by higher education institutions. Each student has a wallet where they save the tokens that represent their course credits. As they finish each course, their tokens grow. Upon finishing each course, instructors deposit course credits into students' wallets using the address identifier, a blockchain with many signatures made up of private and public keys.The first step is to determine how many tokens are currently in circulation. After that, they get the token balance for that particular block address. A function is available to verify the number of tokens that the owner permits to be spent. This function includes the addresses of both the user who owns the money and the user who will spend it. Along with the money to be transmitted, the address for the token's transfer also includes the destination address.

A new function is defined that takes the block address, counts the number of tokens spent, and returns their value.Teachers put course credits into students' wallets after they finish each class using the student's address identification, which is a blockchain with many signatures made of private and public keys.The first step is to determine the entire supply of tokens. After that, they get the token balance for that particular block address. The function to verify the number of tokens that the owner permits to be spent includes the addresses of both the fund owner and the spender. Both the destination address and the amount to be transmitted are part of the specified address for token transfers. A new function is defined that takes the block address, counts the amount of tokens spent, and returns their value.

3.1 Multi-Signature Protocol-Based Blockchain Wallet

Using timestamps and public/private keys, several signatories may collectively certify documents using the multiple-signature protocol, a cryptographic methodology. Its purpose is to verify the authenticity of shared documents (wallets), as seen in Figure 2.

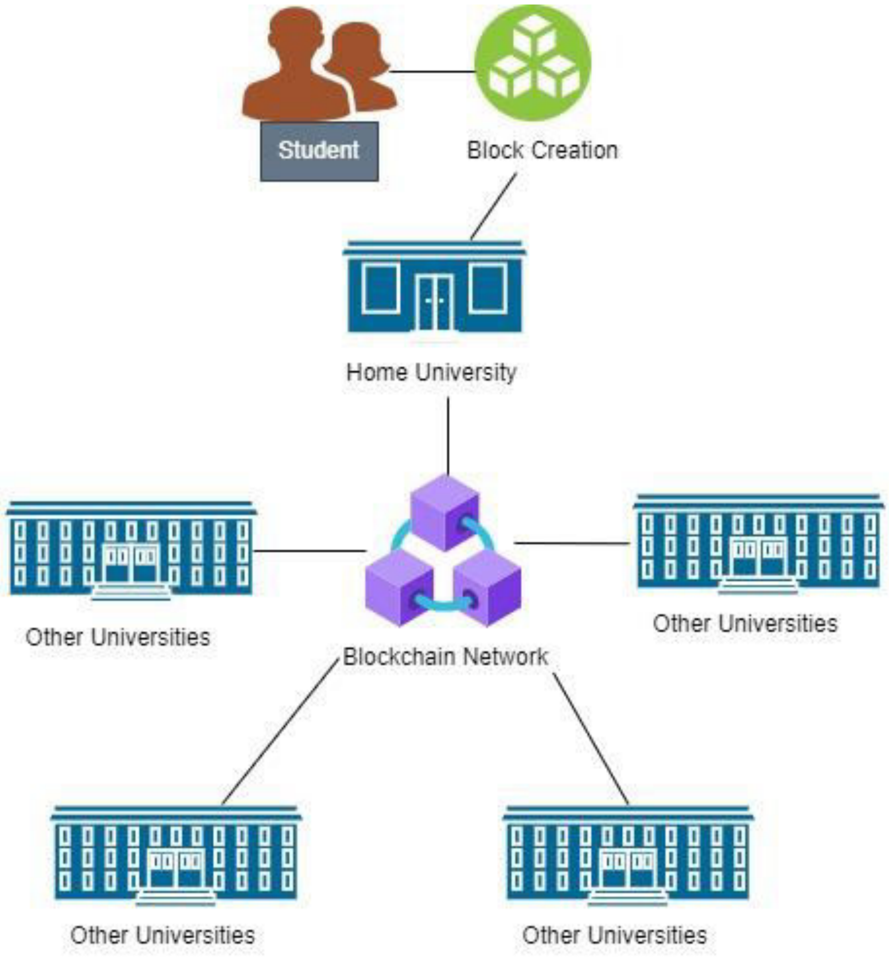


Figure 2 Blockchain Wallet

3.2 University Blockchain Registration

The commutator node is selected at random. The new school may join the blockchain using the commutator node's shared connection. The newly installed university node creates a blockchain wallet, an address, public and private keys, and the blockchain itself. The new node will join the network by connecting to an existing university node after it has generated the blockchain address. A token is created and transmitted to the address on the blockchain of the new node by the current node. A hash value is generated via this inter-node communication and added to the freshly created block as its address. Every node in the network receives a copy of the address to disseminate the information.

3.3 University Student Registration on aBlockchain

The university establishes a student ID after verifying the student's record. A student data block is created during the process of generating a student ID. The distributed consensus process then adds the block to the chain. The student's credentials are verified by issuing a public key and a private key. A student's blockchain wallet address is generated by the institution using a multiple-signature technique. A student's wallet is created using the university and the student's public keys.A node in the network is constructed by rehashing the student's ID and wallet ID, and this node is notified about all the additional nodes in the network. Once this is complete, the student and the educational institution will be able to conduct token transactions. The system model is shown in Figure 3.

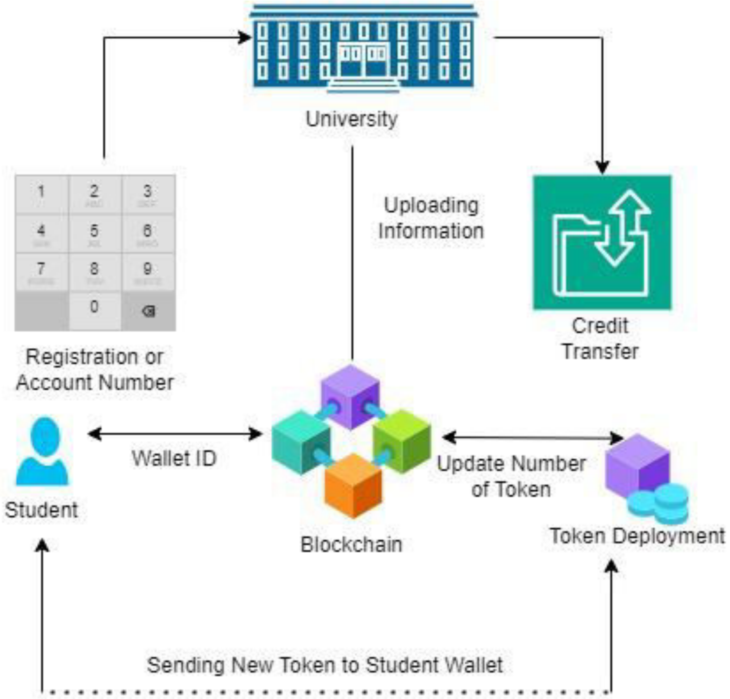


Figure 3 System Model

3.4 Secure Math for Contracts

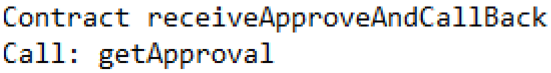
The following is a wrapper for Solidity overflows in the math operations. The programming community generally believes that overflows cause mistakes in most languages; therefore, this might potentially cause issues. When an arithmetic overflow happens, secure math rolls back the transactions and gets the programmer back to their original assumptions. Unlike suggestions for unchecked activities, using the library guarantees that all problems will be removed (See Algorithm 1).

```
Contract SecureMath
Function secAdd
Pass In: unsigned integer A and unsigned integer B
Add A and B and pass value to C
Require C to be greater than or equal to A
Pass Out: unsigned integer C
Endfunction
Function secSub
Pass In: unsigned integer A and unsigned integer B
Subtract B and A and pass value to C
Require B to be lesser than or equal to A
Pass Out: unsigned integer C
Endfunction
Function secMul
Pass In: unsigned integer A and unsigned integer B
Multiply A and B and pass value to C
Require A to be equal to or C/A equal to B
Pass Out: unsigned integer C Endfunction
Function secDiv
Pass In: unsigned integer A and unsigned integer B
Divide A and B and pass value to C
Require B to be greater than 0
Pass Out: unsigned integer C
Endfunction
```

Algorithm 1 Secure Math for Contracts

3.5 Approval of Contract Receipt and Callback

The user may execute contract functions that obtain permission and execute them in a single call using the contract's receipt approvals and callback feature (refer to algorithm 2).

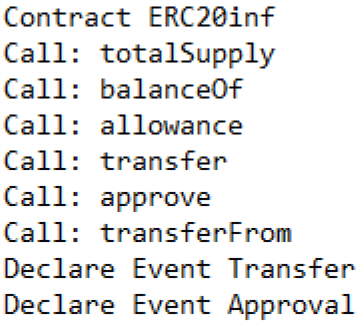


```
Contract receiveApproveAndCallBack
Call: getApproval
```

Algorithm 2 Contract for single-call get/run function.

3.6 Token for the ERC 20 Contract

Token implementation regulations on Ethereum are laid forth in the Ethereum Routing Standard (ERC-20). This allows programmers to control the functionality of tokens inside the ecosystem. The protocol for how a token contract should work and what it should do are detailed in the token standard (see algorithm 3).



```
Contract ERC20inf
Call: totalSupply
Call: balanceOf
Call: allowance
Call: transfer
Call: approve
Call: transferFrom
Declare Event Transfer
Declare Event Approval
```

Algorithm 3 ERC-20 Interface

3.7 Contract-owned

Modifiers are used to change the behaviour or characteristics of a function. The function will throw an exception if the modifier's condition is not met while it is being performed.

3.8 ERC Token Contract Addition

Additional elements of the ERC-20 Token, like as signs, labels, and decimals, are included in this contract. Token balance management is facilitated by suitable features.

3.9 Functions for Rolling Back ETH

If the user deploys cash by mistake or by some other fault, they will help him retrieve it.

4. Results and Discussion

Results are analysed for system security and scalability. The suggested system undergoes security analysis to identify various sorts of network assaults. The second section analyses the system's scalability.

4.1 Analysis of Security

The prevalent attacks are examined, and their consequences are analyzed.

4.1.1 Attack with Replay

The cyberattack is typical in peer-to-peer networks. The perpetrator of this attack hides its identity by intercepting and retransmitting communications sent by a specific peer. The idea behind blockchain is that each node may do double duty as a server and client. Take the blockchain network, where a server, an attacker, and an average user all exist. When communicating between the server and regular users, communications are signed and encrypted. As seen in Figure 4, the perpetrator assumes the identity of a legitimate user or server (attack with replay). The ecosystem was shown to be resilient after simulating a replay attack using Ettercap 0.8.3.1 and doing analysis and verification.

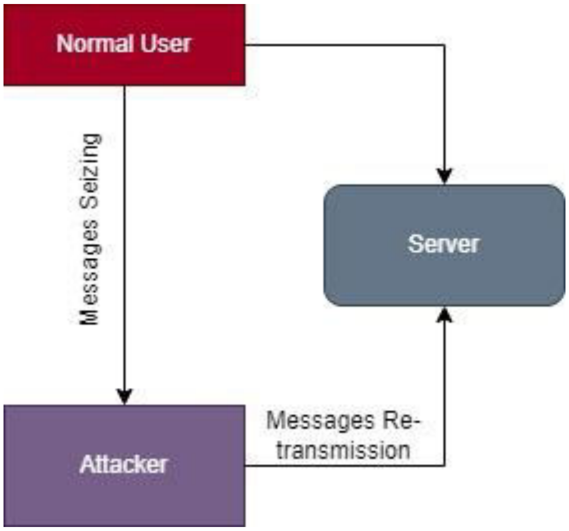


Figure 4 Attacks with Replay

4.1.2 Sybil Attack

Clusters of nodes supporting comparable data are essential in peer-to-peer networks. The use of virtualization allows an attacker to create several identities in the event of a cluster attack. As seen in Figure 5, this allows attackers to assume many identities to gain control of the network.The suggested system protects itself from the Sybil attack by using two-factor authentication. Sybil nodes with fake identities are unable to join the network due to their inability to authenticate. Therefore, Sybil nodes cannot benefit from using many identities. Verifying the findings involves using a virtual box to incorporate a blockchain that employs false identities. The suggested ecology can withstand Sybil's attack, according to the analysis.

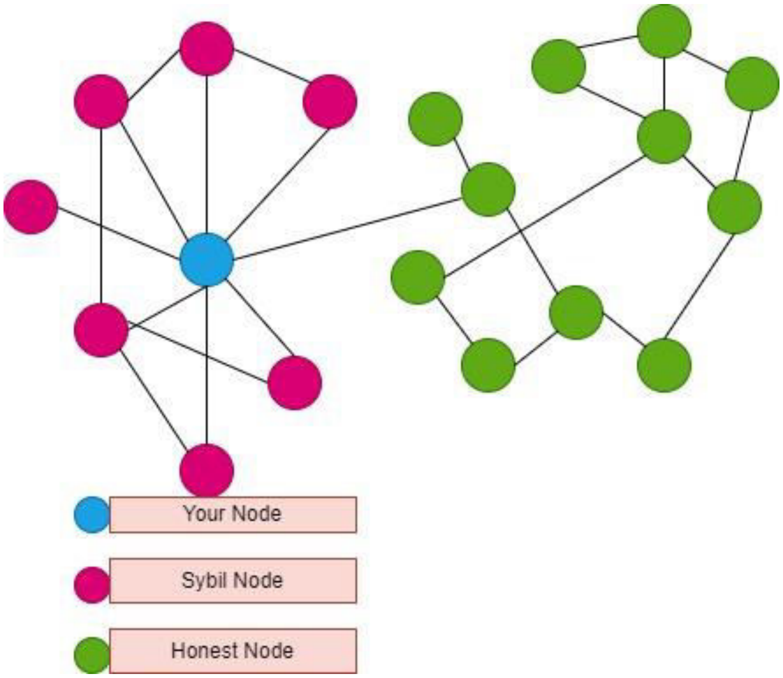


Figure 5 Sybil Attack

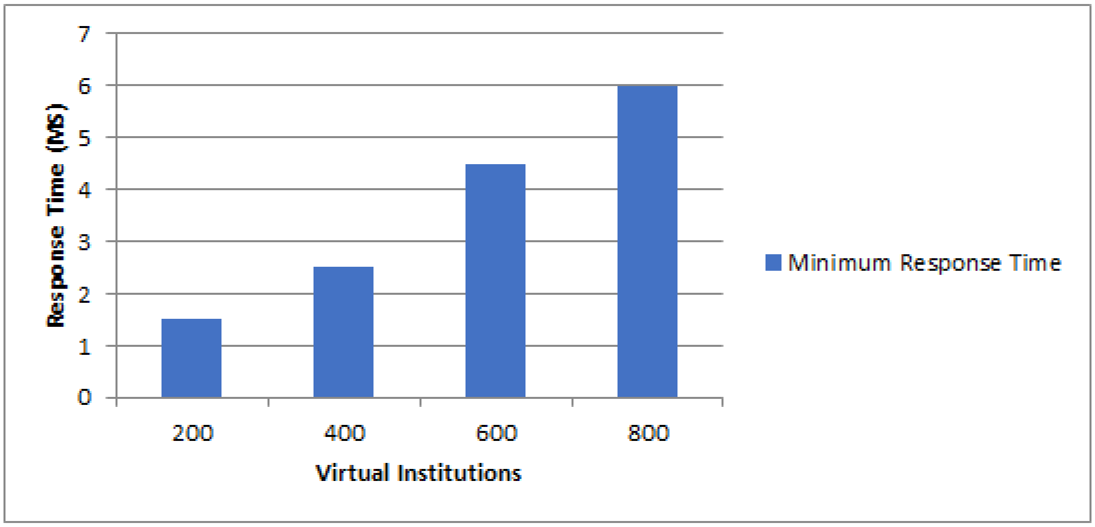
4.1.3 Tampering with Collusion

A single node will store and distribute all blockchain transactions that have been successfully committed. In the early stages of a blockchain network, when the number of nodes is minimal, most of them will conspire to alter the recorded transaction data.The suggested technique would regularly update the data on the public Ethereum network. The scheme's data protection chain demonstrates that the likelihood of a collision tamper assault drops with increasing chain length, which makes sense given the increasing number of nodes.

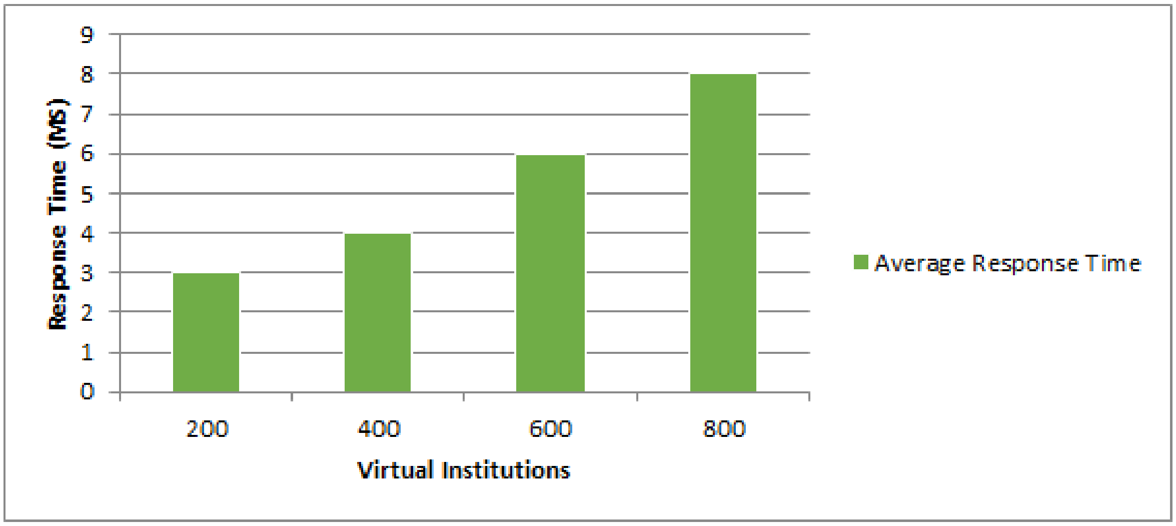
4.2 Analysis of Scalability

4.2.1 Analysing Scalability Load

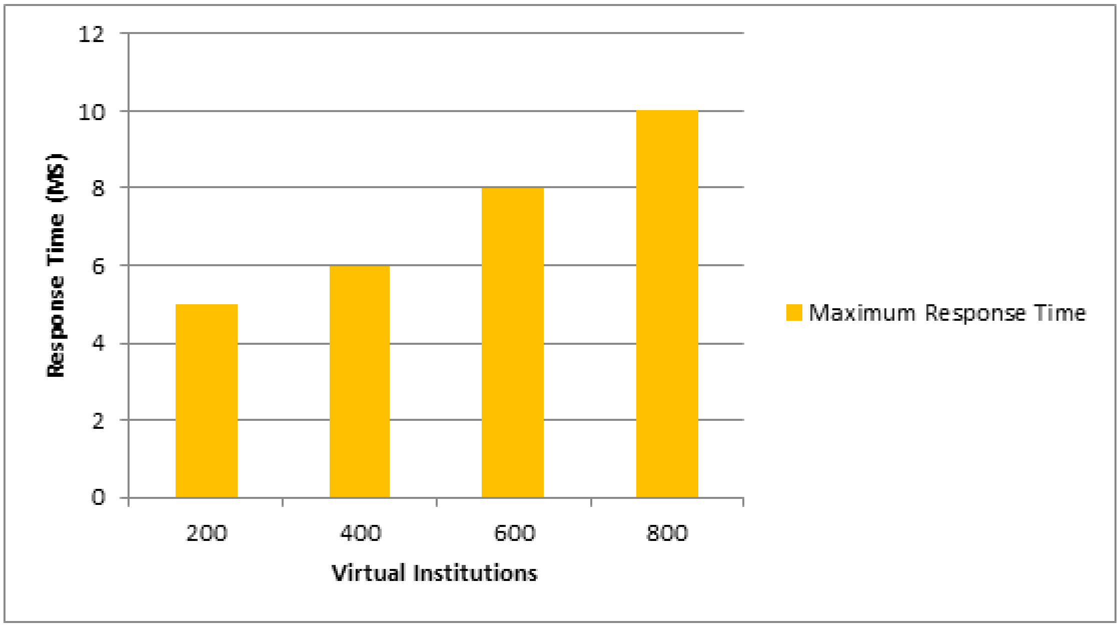
The suggested technique adds the student's information hash to the blockchain. Data submission and block creation are both executed asynchronously. Maximum, average, and lowest reaction times are the assessment metrics that are examined.The load test was performed using Apache JMeter 5.2, an open-source software platform. To assess the system's scalability, it was simulated in a variety of virtual institutions with identical event volumes but different storage needs. Figure 6 (a-c) shows the system's performance with, on the y-axis, the time it takes to respond to storage requests and, on the x-axis, the number of virtual institutions. The results demonstrate that the reaction time metric, which measures scalability, improves with the addition of more virtual institutions.According to the results, the fastest possible reaction time is around 10 milliseconds. The system's potential for usage in blockchain-based real-time applications is shown below.



(a)



(b)



(c)

Figure 6 (a) Minimum Response Time, (a) Average Response Time, (a) Maximum Response Time

4.2.2 Analyze Requested Scalability

Token generation requests are sent asynchronously. The Dap may communicate with Ethereum up to 100 times per second. On average, it takes this amount of time to hand out the tokens. Rinkeby Test network throughput was determined to be 20 TP/s. Figure 7 displays the correlation between the query processing time and the total number of replies during a certain time frame, where the requests were changed.

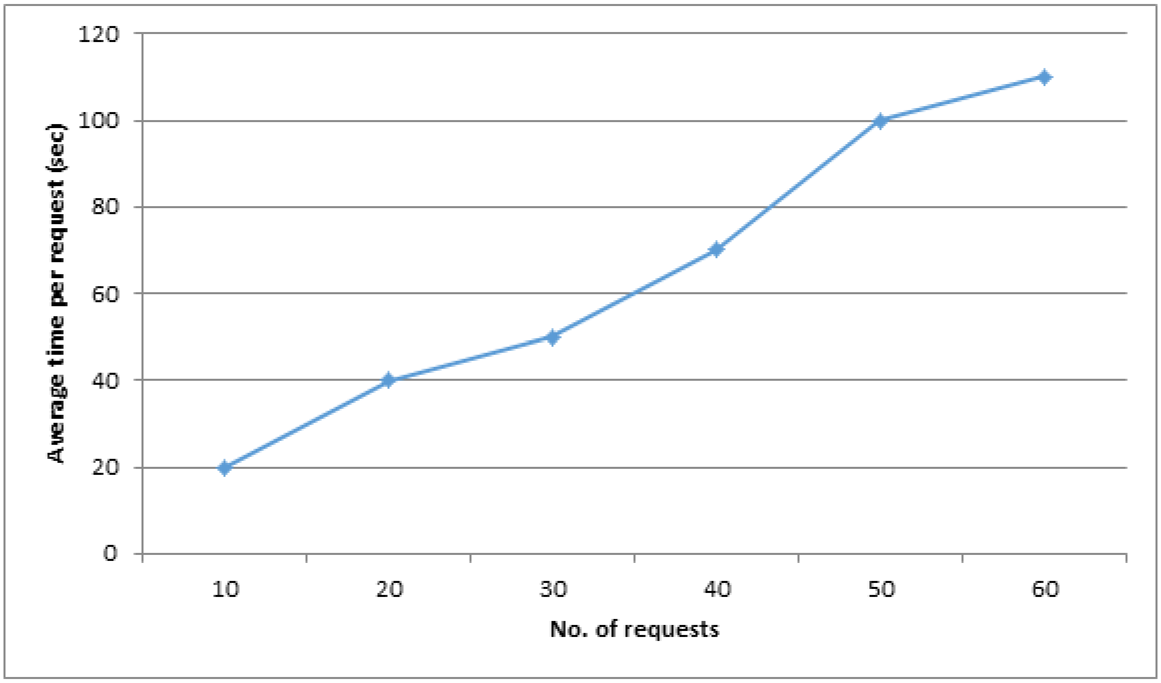


Figure 7 Correlations between the Query Processing Time and the Total Number of Replies

4.2.3 Existing Scheme Comparison

Scalability and security analysis are used to compare the proposed strategy with previous efforts. Table 1 analyses the scalability based on response time and load test analysis.

Table 1 Analyses the Scalability based on Response Time and Load Test Analysis

Strategies	Load Test Analysis	Maximum Response Time Checking	Minimum Response Time Checking
Proposed Strategy	Yes	Yes	Yes
EduCTX	Yes	No	No
VECefblock	No	No	No
Credence Ledger	Yes	No	No

Attack impact comparisons are shown in Table 2. A proposal for a decentralized system of educational credit transfer is made in this article. It simplifies the process of utilizing the educational system while ensuring security by using a distributed method with load sharing. However, this research acknowledges that developing blockchain technology that is both safe and optimized is still a problem. Plans include using effective methods like deep repressor, hyperchaotic maps, Multi-objective evolutionary optimization, and deep learning models to construct a safe suggested model.

Table 2 Attack Impact Comparisons

Strategies	**Used Security Techniques**	**Replay Attack**	**Collision Tamper Attack**	**Sybil Attack**
Proposed Strategy	Yes	Yes	Yes	Yes
EduCTX	Yes	Yes	No	No
VECefblock	Yes	No	No	No
Credence Ledger	Yes	No	No	No

5. CONCLUSION

The paper lays out the current educational system's blockchain-based technology and then suggests a solution for decentralized credit transfer. To make the educational system more user-friendly and secure, it uses a distributed method that shares the burden. Students may redeem their credits for tokens that can be used to register for various courses at institutions via the system.The suggested plan ensures the safety and scalability of educational institutions' student data. To facilitate the distribution of credits to students via a blockchain wallet, built a decentralized Solidity smart contract. Tokens are created from the credits and then transferred. Cryptography and hashing based on public keys provide security. A private key is given to the school and any pupils who have registered on the blockchain. A student's blockchain wallet will be credited with a token after they finish a registered course.The suggested system is secure since it has been tested against several threats and determined to be impervious to them. Load testing, in which the number of institutions using the blockchain platform is increased and the maximum and lowest response times are examined, is used to assess the system's scalability.

REFERENCE

1) Kumar, K. Sunil Ratna, et al. "Iot and data mining techniques to detect and regulate of the solar power system." 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2023.

2) Cuya, Kennedy C., and Thelma D. Palaoag. "Revolutionizing Academic Integrity: The Emergence of Blockchain for Credential Verification-A Bibliometric Perspective." *Nanotechnology Perceptions* (2024): 264-290.

3) Rustemi, Avni, et al. "A systematic literature review on blockchain-based systems for academic certificate verification." *IEEE Access* 11 (2023): 64679-64696.

4) Ayarnah, Amin, Kobby Mensah, and Raphael Odoom. "Exploring Blockchain Technology and Digital Certificates in the Education Sector." *Bentham Science* 10.9789815124750123010005 (2023).

5) 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.

6) Tariq, Aamna, Hina Binte Haq, and Syed Taha Ali. "Cerberus: A blockchain-based accreditation and degree verification system." *IEEE Transactions on Computational Social Systems* 10.4 (2022): 1503-1514.

7) Effiong, Mercy Ebiot. *A Framework for the Adoption of Blockchain Technology in Academic Certificate-Verification Systems: A Case Study in Nigeria*. Diss. MSc Thesis, Tallinn University of Technology, Tallinn, Estonia, 2020.

8) Sayed, Rakibul Hasan. *The potential of blockchain technology to solve the fake diploma problem*. MS thesis. 2019.

9) Bhaskar, Preeti, Chandan Kumar Tiwari, and Amit Joshi. "Blockchain in education management: present and future applications." *Interactive Technology and Smart Education* 18.1 (2021): 1-17.

10) Marouan, Adil, et al. "Empowering education: leveraging blockchain for secure credentials and lifelong learning." *Blockchain Transformations: Navigating the Decentralized Protocols Era*. Cham: Springer Nature Switzerland, 2024. 1-14.

11) J. Gera, K. Sushma and S. R. Polamuri, "RECS Methodology for Secured Data Storage and Retrieval in Cloud," *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2023, pp. 1426-1429, doi: 10.1109/ICSCDS56580.2023.10105033.

12) Mahankali, Srinivas, and Sudhir Chaudhary. "Blockchain in education: a comprehensive approach–utility, use cases, and implementation in a university." *Blockchain technology applications in education*. IGI Global, 2020. 267-293.

13) R. Suhasini, B. Ratnamala, G. Sravanthi, K. P. Kumari and S. R. Polamuri, "Detecting Fake News on Twitter by Using Artificial Intelligence," *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*, GHAZIABAD, India, 2023, pp. 594-598, doi: 10.1109/AECE59614.2023.10428322.

14) Li, Zoey Ziyi, et al. "Blockchain-based solutions for education credentialing system: Comparison and implications for future development." *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2022.

15) M. K. B, M. S. Kumar, F. D. Shadrach, S. R. Polamuri, P. R and V. N. Pudi, "A binary Bird Swarm Optimization technique for cloud computing task scheduling and load balancing," *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, Chennai, India, 2022, pp. 1-6, doi: 10.1109/ICSES55317.2022.9914085.

16) Al Hemairy, Mohamed, et al. "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution’s accreditation: UAE case study and system performance (2022)." *Education and Information Technologies* (2024): 1-30.

17) Dharmalingam, Ramalingam, et al. "Framework for digitally managing academic records using blockchain technology." *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2021*. Springer Singapore, 2022.

18) I. L. Manikyamba and S. R. Polamuri, "Spectrum Sensing-Optimized Data Transformation," *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)*, Bangalore, India, 2023, pp. 1-6, doi: 10.1109/ICCAMS60113.2023.10525989.

19) Nadeem, Nida, et al. "Hybrid Blockchain-based Academic Credential Verification System (B-ACVS)." *Multimedia Tools and Applications* 82.28 (2023): 43991-44019.

20) Loukil, Faiza, Mourad Abed, and Khouloud Boukadi. "Blockchain adoption in education: A systematic literature review." *Education and information technologies* 26.5 (2021): 5779-5797.