Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 8526456, 12 pages
https://doi.org/10.1155/2021/8526456

Research Article

Blockchain Ecosystem for Credit Transfer in Education

R. Manoj[1], **Sandeep Joshi**[1], **Utkarsh Dabholkar**[1], **Ganesh Prakash Panicker**[1], **Kevin Peter Kuriakose**[1], **Atef Zaguia**[2] and **Mohammad Monirujjaman Khan**[3]

[1]*Department of Computer Science and Engineering, Manipal UniversityJaipur, Jaipur, Rajasthan, India*
[2]*Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia*
[3]*Department of Electrical and Computer Engineering, North South University, Bashundhara, Dhaka-1229, Bangladesh*

Correspondence should be addressed to Mohammad Monirujjaman Khan; monirujjaman.khan@northsouth.edu

Received 9 July 2021; Accepted 10 November 2021; Published 9 December 2021

Academic Editor: Ahmed A. Abd El-Latif

Data is the key to measuring educational effectiveness promptly. But data and education are trapped and siloed across centralized systems, causing information discrepancies and inaccuracies. This has caused countless delayed opportunities, academic credential disagreements, and never-ending confusion around learning potency. This lack of transparency, despite having its fair share of usefulness, has also been quite burdensome. To alleviate this issue, our team has developed a blockchain protocol that verifies professional certifications that have been earned both locally and through another well-established online educational portal. This system allows accuracy, reliability, and immutability that has never been implemented. This foundation of clear, verified data will then be used further to power blockchain-based applications. The result is that our attempt at a versatile, holistic, and decentralized view of educational performance ensures the best e-learning outcome for students and teachers alike.

1. Introduction

At its core, a blockchain is a ledger that permanently stores information about all transactions on the network that cannot be modified or tampered with. What was once a niche technology that was created by a group of dedicated developers under the alias of "Satoshi Nakamoto" back in 2008–09 for the storage of transaction information made using bitcoin is now used in many industries such as banking, healthcare, insurance, and law. After its initial success, blockchain has evolved to be the foundation of any and every decentralized application that is out there. This, along with the execution of smart contracts, has brought its use to new, unprecedented heights [1, 2].

A smart contract is a program whose responsibility is to conduct asset transfer between two parties while satisfying a condition. The life cycle of a general smart contract consists of first recording the terms of a contract between the parties on a distributed ledger. Then, they relate to internal or external systems and databases. The contract waits for external factors to evaluate predefined conditions. And, finally, the contract self-executes upon fulfilment of conditions via triggers. The easy deployment of smart contracts in public blockchains, also known as public smart contracts, has attracted a wide variety of commercial applications [3, 4]. Our paper aims to provide the most efficient way to use DLT (distributed ledger technology) like blockchain and smart contracts in the field of online education.

We developed a decentralized Solidity smart contract for transferring credits to students through a blockchain wallet. The credits are converted into tokens and are transferred. The security is provided using public key encryption and hashing techniques. The university and students registered on the blockchain are provided with a private key. When a student completes a registered course, the credit is converted into a token and saved in the blockchain wallet. To ensure the security of the proposed system, the impact of various attacks on the system has been analyzed and the system was found to be resistant to those attacks. The scalability of the system is tested by load testing by increasing the number of universities registering on the blockchain platform and analyzing the maximum response time and minimum response time [5, 6].

The Ethereum smart contract is programmed in Solidity. A proposed ecosystem for higher educational organizations for token-based credit transfer using blockchain is presented here. The credit value in the form of tokens is stored in each student's individual wallet, and, after completion of each course, tokens get accumulated in the wallet. Faculties transfer the credits to students' wallets after completion of each course based on the student's address identifier, which is a blockchain with multiple signatures consisting of public and private keys.

The rest of the paper is divided into five sections. Section 2 discusses existing work in the field of blockchain in education, such as credit transfer in the form of tokens, certificate validation, and certificate forgery prevention. Section 3 deals with the architecture of the blockchain platform for credit transfer using the Ethereum blockchain. The algorithms of credit transfer are mentioned in Section 4. The comparison of the proposed system with existing credit transfer methods and analysis of security and scalability are done in Section 5.

2. Literature Review

An effective, secure, and lightweight blockchain [1] to ensure the security of the Internet of Things (IOT) is presented. The model operates on three levels: consensus, cryptographic methods with certificates, and distributed throughput management schemes. The main goal is to reduce computational overhead and the number of blocks created using the consensus algorithm.

The credit platform for higher education institutions in Europe [2] is designed using the blockchain platform and it is modelled on a peer-to-peer distributed network system. The credit platform transfers credits for completion of courses in the form of tokens, and it is a ubiquitous system designed to be aligned with the physical world. This credit platform is beneficial for students and higher education institutions in terms of transparency in view of completed courses and updated information on credit earned. Figure 1 shows Vietnamese blockchain certificate issue system.

The development of a model in Vietnam [3] has successfully solved major issues in online educational systems like fake certificates and degrees. This model is developed for preventing certificate forgery. As far as blockchain is considered, this technology is widely used for its efficiency in keeping the data in decentralized form. Even though, when it comes to storing and analyzing any sort of data, the centralized system is always preferred, there is less control over stored data in the centralized form of the authority. To overcome this issue and to make it less complex, the model allows the user to have the data in itself and can grant permission to the users who wish to see it, as shown in Figure 1. By using blockchain, the authentication of certificates becomes easy as it deals with the blockchain address of the recipient, the public key of the issuer, and, obviously, the general information about the certificate, like when it was issued, and so on.

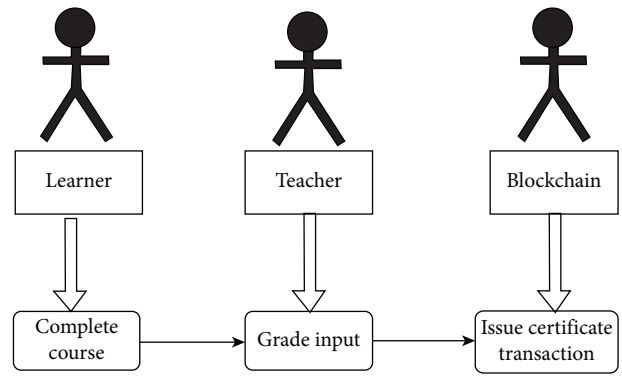

Figure 1: Vietnamese blockchain certificate issue system.

The blockchain-based system for diploma certificate issue and verification for the University of Zurich [4] is designed as a complete solution, as shown in Figure 2. Certificate forgery and fake certification are increasing, and there is fraud in academic grades as well. Diploma certificates are issued in digital form and the drawbacks of paper certificates and security issues are solved using cryptographic protocols.

To verify a student's certificate and other academic details [5], the verifier's registration on the blockchain platform is required. The next process is sending the address block to the university. The university then creates an address that contains two types of signature, one using the public key of the university and the other using the verifier's private key. The blockchain platform can be added to the existing education model with minor modification and less complexity, and with better transparency.

A blockchain-based educational framework [6] is proposed to prevent academic certificate forgery and digital transfer of credits among students, universities, and other stakeholders. Students get tokens when credits are granted for completing courses in university, and credits form the transaction for mining the block, which is added to the existing blockchain. This method of token transfer provides better security and transparency, and data can be stored in a digitally verifiable format which cannot be modified.

The outcome of learning [7] results from recognizing learners and transferring credits upon course completion. When credits for graduation are completed, rewards in the form of diplomas and tokens are given to learners. The major issues are in implementation, adopting changes from centralization to a decentralized blockchain platform, and measurement of learning outcomes. The students should be satisfying the requirements of learning before graduating.

Communications between learners and educational institutions are stored and there exists a public layer [8], where the data integrity of the information in private layers is verified and the authentication of the private layer is verified. The educational institutions are higher education institutes or teachers who participate in the network. Authenticated data stored in private blocks is backed up in the public layer for use in verifying and validating transactions and

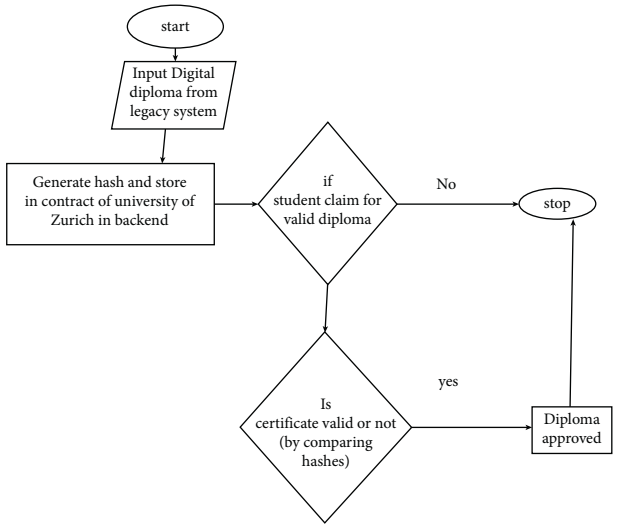

Figure 2: Diploma certificate issue and verification for the University of Zurich.

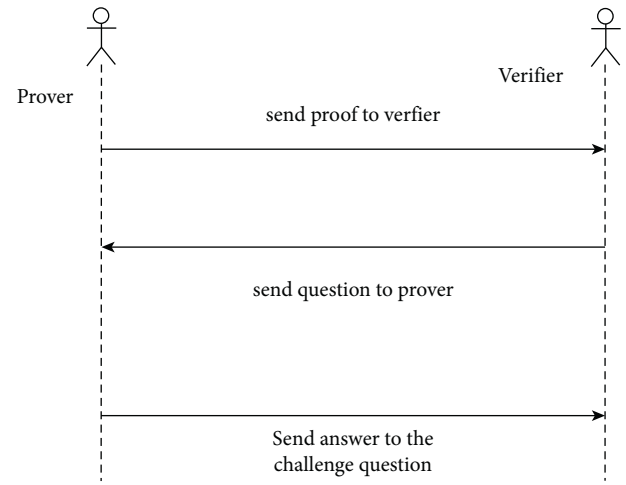

Figure 3: Zero knowledge proof for security.

interactions between learners and educational institutions in the future.

There are three stages in the advancement of blockchain applications [9], namely, cryptocurrencies, smart contracts, and applications of blockchain in healthcare, government projects, and education. Blockchain technology frameworks are created for mapping learning outcomes in education. The various applications of blockchain are certificate validation and management and students' identity verification, as well as providing a database of students' certificates and other students' information needed for continuing their education.

The main features of the framework are the distributed consensus protocol and wallet of the blockchain, along with the protocol of multiple signatures, which is a cryptographic protocol that verifies and validates the digital data in relation to suitable consensus or agreement [10]. The validity of digital data is validated by multiple signatures on the document. The concept of zero knowledge proof is shown in Figure 3 and is used for security. The usage of these signatures prevents harmful transfer of credits among students. Whenever a new educational institution is added, a node is generated, and a wallet is created on the blockchain. The blockchain address is composed of both public and private keys for signing and validating academic documents.

The blockchain framework for the transfer of credits after completion of a course [11] from one academic institution to another is a potential area in the market. This will create similarity in the academic and certificate validation system, irrespective of location and language differences. The framework for reducing the complexity of the educational system will be integrated with the existing system and it should be transparent.

The students and educators who take part in online education [12] are responsible for designing and allowing the schemes for storing learning information. Distributed storage of information using blockchain technology provides authentication, privacy of data, and availability of information. There is a chance of attack on these educational records. The blockchain architecture should provide methods to solve the security issues.

The software application enables students and academic institutions to verify the identities of participants and also guarantees integrity and validity [13]. Information privacy is ensured using the ECC encryption system. The blockchain platform prevents the possibility of certificate forgery. Organizations create an appropriate system for certificate validation and do proper authentication of the information.

An open platform for official educational records [14] can be of benefit by issuing official certificates for proof of completion of a course and providing higher degree security. Digitally stamped certificates are provided by blockchain, which gives integrity to the document. This method of credit transfer makes the platform more secure and scalable. The distributed consensus mechanism called "proof of work" provides a blockchain framework suitable for storing educational records.

"Blockchain also provides storage for these academic credentials as transactions" [15]. Universities verify all these academic credentials and secure them using cryptographical mechanisms, such as multiple signatures and encryption.

Due to the absence of proper antiforgery methods for certificate generation, digital certificates generated by the blockchain framework are proposed [16]. This ensures data security and reduces the chances of forgery. This certification system is more transparent and its information is accurate.

The blockchain will store a student's achievements after completing a course, such as grades, credits, and weightage [17, 18]. The diploma is awarded to students who successfully complete the course. This process provides better security and transparency for storing and retrieving learning outcomes.

3. System Model

One of the most integral parts of the system is data storage. It is important to know how to store and access the data, as shown in Figure 4.

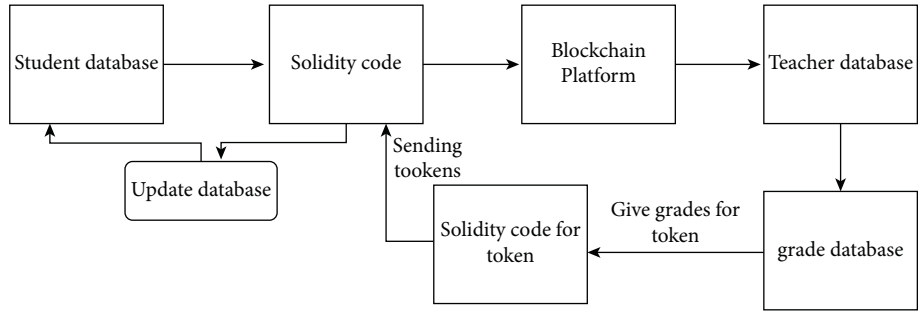

Figure 4: Education ERP model.

Initially, all the important information that comprises the database is stored in a .csv file. This .csv file will contain metadata that includes key information such as student name, registration number, fee payment information, gender, section, registered course(s), password, blockchain address, public key, and private key. The student will gain access into the student database by providing their user ID, password, and public key that is unique to everyone. Once they are in, it will interface with the Solidity code base and a third party will verify the links of each student with the teacher database. This includes the grades and credits completed and can be modified by individual professors for their respective subjects. These are then converted into appropriate tokens by Solidity which is then updated on the student database, as shown in Figure 4.

We developed a decentralized Solidity smart contract for transferring credits to students through a blockchain wallet. The credits are converted into tokens and are transferred. The security is provided using public key encryption and hashing techniques. The university and students registered on the blockchain are provided with a private key. When a student completes a registered course, the credit is converted into a token and saved in the blockchain wallet. To ensure the security of the proposed system, the impact of various attacks on the system has been analyzed and the system was found to be resistant to those attacks. The scalability of the system is tested by load testing by increasing the number of universities registering on the blockchain platform and analyzing the maximum response time and minimum response time.

4. Implementation

The Ethereum smart contract is programmed in Solidity. A proposed ecosystem for higher educational organizations for token-based credit transfer using blockchain is presented here. The credit value in the form of tokens is stored in each student's individual wallet, and, after completion of each course, tokens get accumulated in the wallet. Faculties transfer the credits to students' wallets after completion of each course based on the student's address identifier, which is a blockchain with multiple signatures consisting of public and private keys.

Firstly, the total number of tokens in existence is decided. Then the token balance from the specific block address is obtained. There is a function to check the number of tokens the owner allows to spend, which contains the address for the user who owns the funds and the user who will spend the funds. The address specified for transferring the token also consists of the address of where it should be transferred and the amount to be transferred. Another function is created, which contains the block address and measures the spent tokens and the value of the number of tokens.

4.1. Blockchain Wallet Based on Multiple Signature Protocol. The multiple signature protocol is a cryptographic protocol with multiple parties jointly signing documents with timestamps and public and private keys. It is used for validating shared documents as shown in Figure 5.

4.2. Universities Registering to Blockchain. A node is randomly chosen as the commutator node. The commutator node shares a link with the new university to join the blockchain. The new university node generates a blockchain wallet and a blockchain address, along with the public and private keys. After generating the blockchain address, the new node will connect to another university node already available in the network. A token is generated from the existing node and sent to the new node blockchain address. This communication between the nodes generates a hash value and appends it to the newly created block as a block address. To inform other nodes in the network, the address is replicated and sent to all the nodes in the network.

4.3. Student Registration under a University within a Blockchain. The student details are verified by the university to generate a student ID. While issuing a student ID, a student data block is generated. The block is then added to the chain as per the distributed consensus protocol. A public key and a private key are issued to verify the student's credentials. The university uses a multiple signature protocol to generate a blockchain wallet address for the student. The public key of the university and student is used to generate a wallet for the student. The student ID and wallet ID are rehashed to form a node in the network and are informed of all the other nodes in the network. After this process, token transactions can be done between the student and the university. Figure 6 shows the system model.

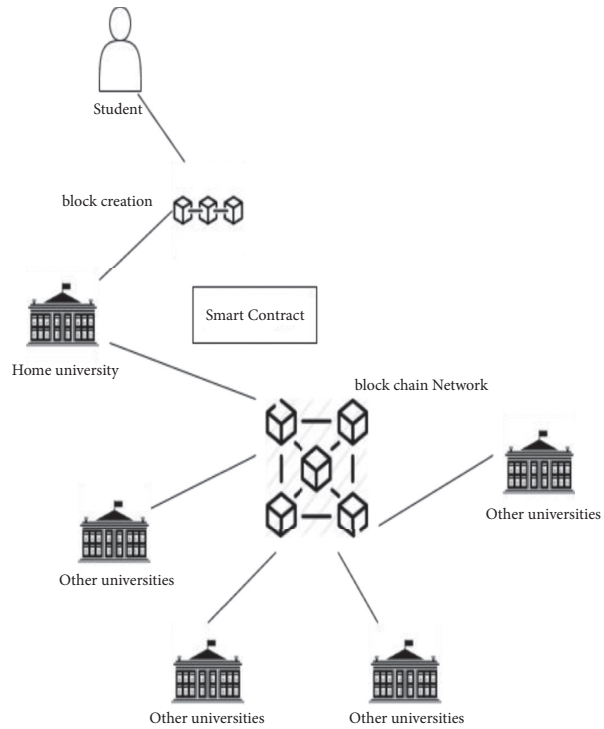

Figure 5: Blockchain wallet.

4.4. Contract Secure Math. Overflows in the arithmetic operations in Solidity are wrapped below. This will lead to bugs, since programmers have the assumption that overflows lead to errors in standard programming languages. Secure math reverts the transactions when arithmetic overflow occurs and restores the assumption of the programmer. Using the library, all bugs are eliminated, in contrast to operations which are not checked and are recommended (Algorithm 1).

4.5. Contract Receipt Approval and Callback. The contract receipt approval and callback enables the user to execute contract functions that receive approval and execute functions in just one call (Algorithms 2–5).

4.6. Contract ERC 20 Token. The Ethereum token standard (ERC-20) defines the rules for implementing tokens on Ethereum. This gives developers the capability to program how tokens will work in the ecosystem. The token standard explains the operation and actions the token contract should implement.

4.7. Contract Owned. To modify the nature or behavior of a function, we use modifiers. The condition of the modifier should be satisfied while the function is executed, or else an exception will be thrown.

4.8. Contract ERC Token Addition. This contract contains symbols, labels, and decimals, which are additional features of the ERC-20 Token. There are appropriate functions to manage the balance of tokens.

4.9. ETH Rollback Functions. They assist the user in reclaiming any currency that was deployed by him inadvertently or through some other error.

5. Results and Discussion

The results obtained are discussed in terms of security and scalability of the system. In the security analysis part, the proposed system is analyzed for different types of attacks in the network. In the second part, the scalability of the system is analyzed.

5.1. Security Analysis. The common attacks are considered, and their impact is analyzed.

5.1.1. Replay Attack. It is a common cyberattack in peer-to-peer networks. In this attack, the attacker disguises its identification by seizing the messages from a particular peer and replaying them. In blockchain technology, every node acts as both a client and a server. Assume that there is a normal user, an attacker, and a server in the blockchain network. Signed and encrypted messages are sent between normal users and the server, and vice versa. The attacker impersonates a normal user or server, as shown in Figure 7. Ettercap 0.8.3.1 is used to simulate a replay attack and, after analysis and verification, it is proved that the ecosystem can resist the replay attack.

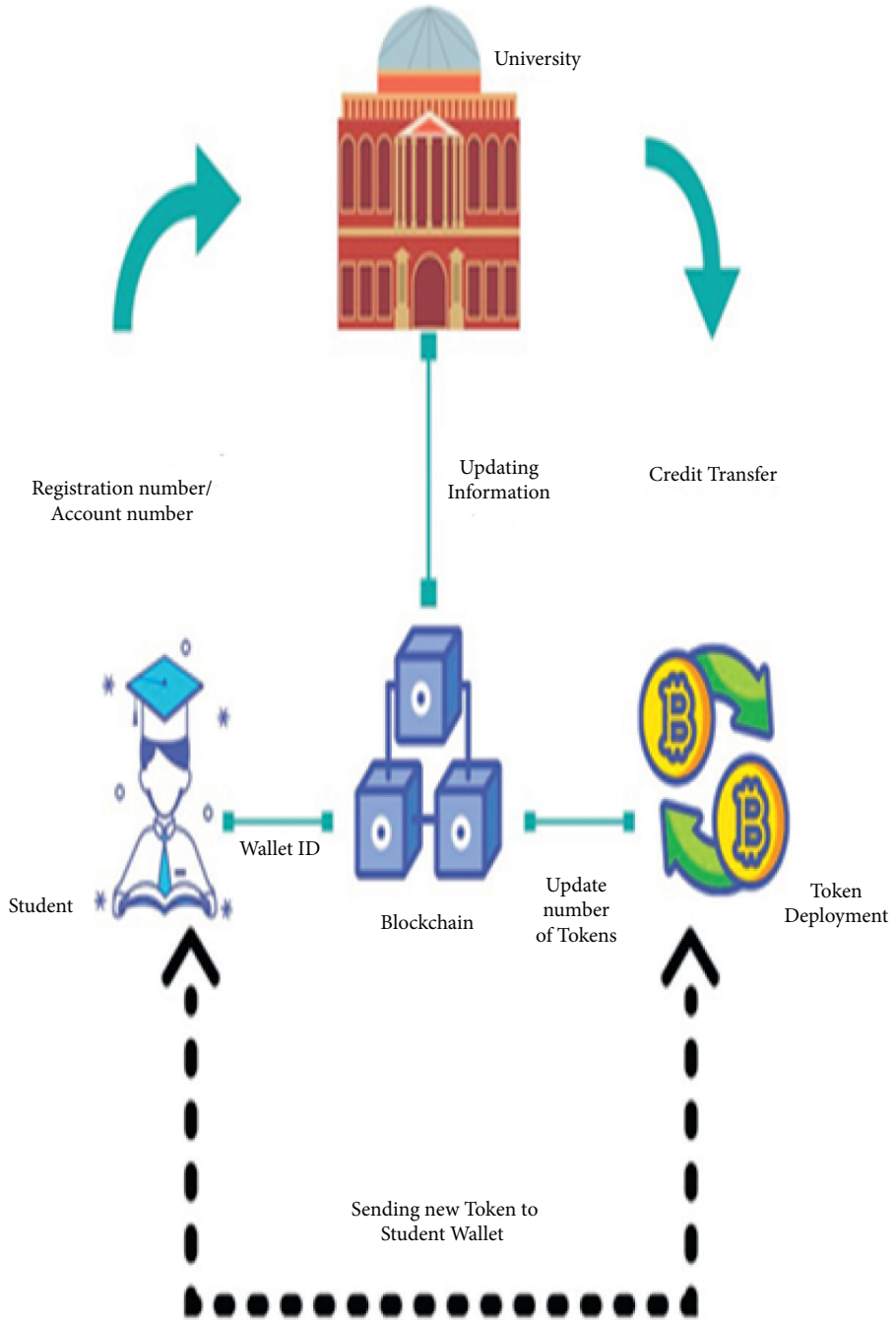

Figure 6: System model.

5.1.2. Sybil Attack. In peer-to-peer networks, similar data must be supported with many nodes in a clustered fashion. If any attack is present in the cluster, then the attacker can establish different identities with the help of virtualization. Thus, attackers can impersonate different identities and take control of the network, as shown in Figure 8.

The proposed system defends against the Sybil attack with two-factor authentication. The forged identities of Sybil nodes cannot join the network since they fail to authenticate themselves. So, no advantage can be taken by Sybil nodes with the help of multiple identities. To verify our analysis, a virtual box is used to include a blockchain using forged identities. Analysis confirms that the proposed ecosystem can resist Sybil attack.

5.1.3. Collusion Tamper Attack. Successfully committed transactions with the blockchain will be shared and kept in a single node. When the network size is small, the majority of nodes collude to tamper with the stored transaction data at the beginning stage of the blockchain network. The proposed scheme updates the data periodically to the public Ethereum. As the number of nodes increases, the chain of data protection implemented in the scheme shows that the

```
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.

```
Contract receiveApproveAndCallBack
Call: getApproval
```

Algorithm 2: Contract to get and run function in single call.

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

Algorithm 3: ERC token standard 20 interface.

probability of the collusion tamper attack decreases as the number of nodes in the chain increases.

5.2. Scalability Analysis

5.2.1. Scalability Load Test Analysis. The hash of student information is added to the blockchain through the proposed scheme. The processes of block generation and data submission are done in an asynchronous mode. The evaluation parameters analyzed are minimum, average, and maximum response time.

The load test was conducted on an open-source software platform, Apache JMeter 5.2. A simulation of 100–800 virtual institutions with the same number of events but varying sets of storage requirements was conducted to analyze the scalability of the system. Figure 9 denotes the performance of the system with the response time for storage requests on the y-axis and the varying number of virtual institutions on the x-axis. The results show that the scalability measured in terms of response time is greater as the number of virtual institutions is increased. The results show that the maximum response time is less than 10 ms. This

```
Contract MujToken is ERC20Interface, Owned, SecureMath
Declare String Public symbol
Declare String Public name
Declare uint8 public decimals
   Declare uint totalSupply
Declare mapping(blockAddress => uint)balances
Declare mapping(blockAddress => mapping(blockaddress => uint)) allowed
Function Token Public
Assign symbol = "Muj"
Assign name = "MujToken"
Assign decimals = 0
   Assign totalSupply = 100
Assign balances
[0x219b9F6848Cc61E09A6B4a6c96E0E7a04BdbBf52] = totalSupply;
Call: Transfer(blockaddress(0),
0x219b9F6848Cc61E09A6B4a6c96E0E7a04BdbBf52, totalSupply)
Endfunction
Function totalSupply
   Return totalSupply-balances[blockaddress(0)]
Endfunction
Function balanceOf
Pass in: blockAddress tokenOwner
Assign balance[msg.sender] = safeSubtract(balance[msg.sender], tokens)
Assign balance[to] = safeAddition(balance[to], tokens)
Call: Transfers(msg.sender, to, tokens)
true
Endfunction
Function approved
Pass in: blockAddress spend and Uint tokens
Assign allow[msg.sender][spender] = tokens
Call: Approvals(msg.sender, spender, tokens)
true
Endfunction
Function transferFroms
Pass in: blockAddress from, blockAddress to, uint tokens
Assign balance[from] = safeSubstract(balance[from], tokens)
Assign allow[from][msg.sender] = safeSubstract(allow[from][msg.sender], tokens);
balance[to] = safeAddition(balance[to], tokens)
Call: Transfers(from, to, tokens)
Return true
Endfunction
Function allowances
Pass in: blockAddress tokenOwner, blockAddress spender
Return allow[tokenOwner][spender];
Endfunction
Function approveAndCall
Pass in: blockAddress tokenOwner, Uint tokens, Bytes data
Assign allow[msg.sender][spender] = tokens Call:Approvals(msg.sender, spender, tokens)
Call:receiveApproveAndCallBack (spender).getApproval
(msg.sender, tokens, this, data);
Return true Endfunction
```

Algorithm 4: ERC token with additional data and assisted token transfers.

```
Contract receiveApproveAndCallBack
Declare blockAddress Public owner
Declare blockAddress Public newOwner Event OwnershipTransferred
Function Ownedtoken() Public
Assign ownertoken = msg.sender Endfunction
Modifier onlyOwnertoken
msg.sender to be equal to ownertoken
Function transferOwnership
   Pass In: blockaddress newOwner
   Assign newOwner = newOwner
Endfunction
Function acceptOwnership
Require msg.sender to be equal to newOwner
Call: ownerTransfer
Assign owner = newOwner
Assign newOwner = blockaddress(0) Endfunction
```

Algorithm 5: Contract owned.

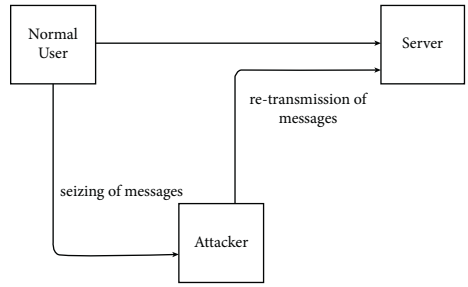

Figure 7: Replay attack.

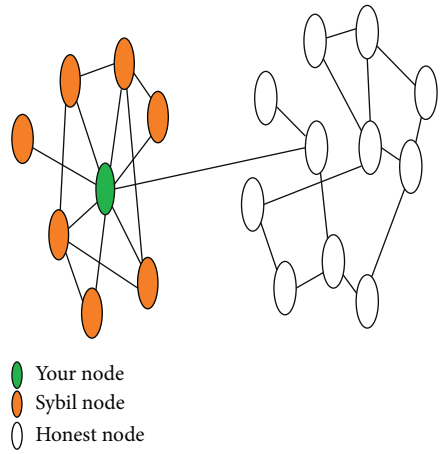

Figure 8: Sybil attack.

shows that the system could be used for real-time applications using blockchain.

5.2.2. Request Scalability Test Analysis. The request for token generation is sent asynchronously. Up to 100 requests are sent from the Dapp to Ethereum. The average time taken to provide the tokens is calculated. It has been found that the Rinkeby Test network can process 20 transactions per second. Figure 10 compares the number of requests with time to the time taken to process the request by varying the requests.

5.2.3. Comparison to Existing Schemes. The proposed scheme is compared with existing works in terms of scalability and security analysis. Table 1 compares the scalability in terms of load test analysis and response time.

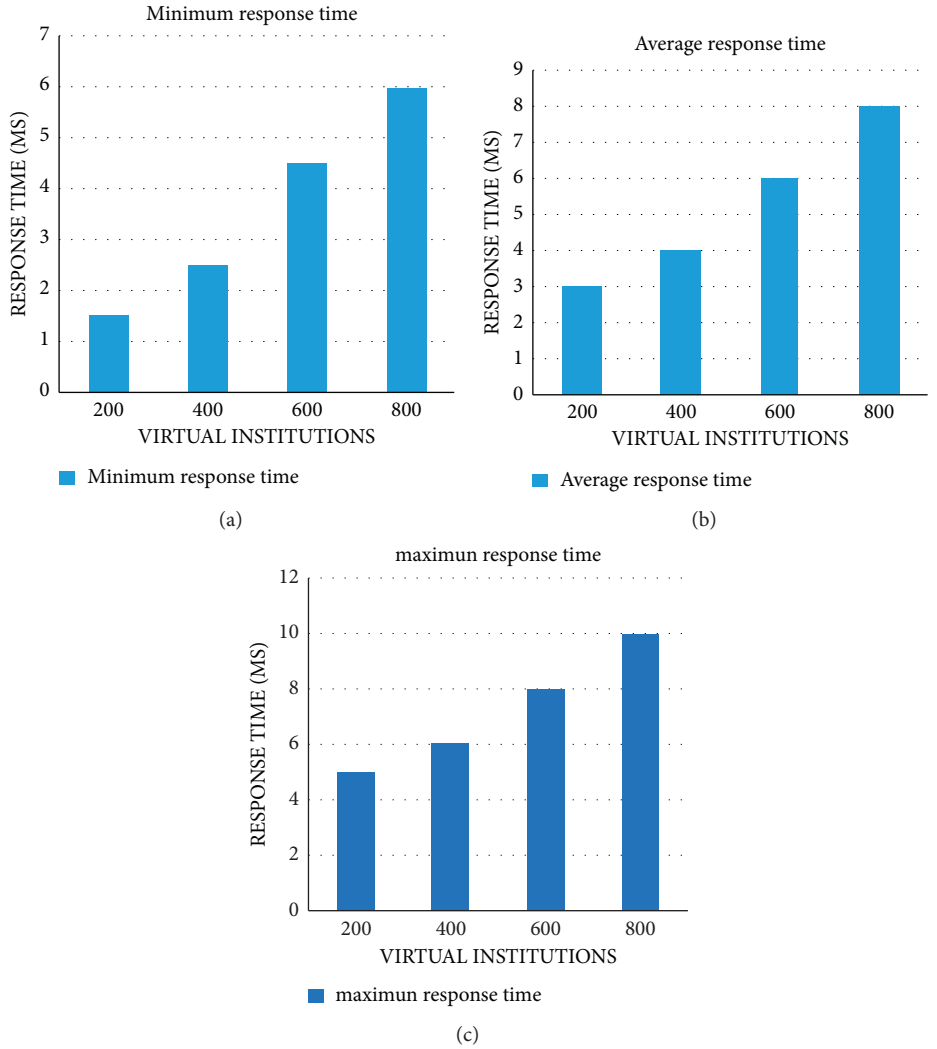

Figure 9: (a) Minimum response time. (b): Average response time. (c): Maximum response time.

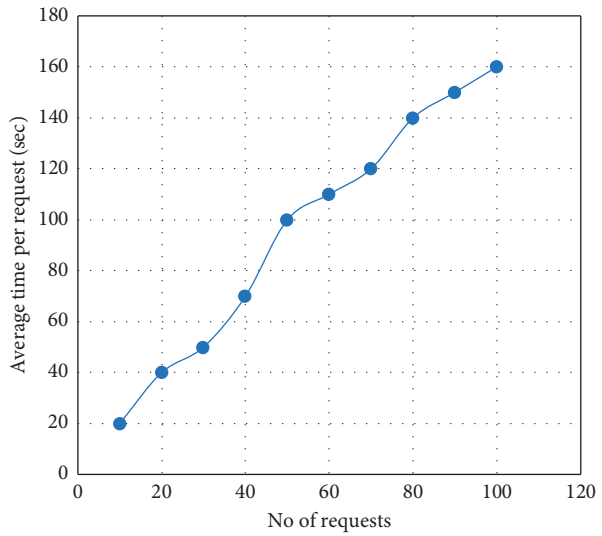

Figure 10: Average time per request.

Table 1: Scalability analysis comparison.

Schemes	Load test analysis	Checking maximum response time	Checking minimum response time
Proposed scheme	Yes	Yes	Yes
EduCTX [2]	Yes	No	No
VECefblock [3]	No	No	No
CredenceLedger [15]	Yes	No	No

Table 2: Scalability analysis by considering various attacks.

Schemes	Security techniques used	Replay attack	Collision tamper attack	Sybil attack
Proposed scheme	Yes	Yes	Yes	Yes
EduCTX [2]	Yes	Yes	No	No
VECefblock [3]	Yes	No	No	No
Credence ledger [15]	Yes	No	No	No

Table 2 compares security analysis in terms of the impact of attacks.

In this paper, a framework for decentralized credit transfer in educational systems is proposed. It follows a distributed approach with load sharing and thereby reduces the complexity of using the educational system with security. But building a secure and optimized blockchain technology remains a challenge in this paper. In the near future, we will try to design a secure proposed model with the help of efficient techniques, such as deep learning models [19, 20], multiobjective evolutionary optimization [21, 22], hyperchaotic maps [23–25], and deep repressor [26, 27].

6. Conclusion

The work details existing technologies in the educational system with blockchain and then proposes a framework for decentralized credit transfer in educational systems. It follows a distributed approach with load sharing and thereby reduces the complexity of using the educational system with security. The system converts the credits of students into tokens which can be used for enrolling in different courses at universities. The proposed scheme provides security and scalability of student data in the educational systems. We developed a decentralized Solidity smart contract for transferring credits to students through a blockchain wallet. The credits are converted into tokens and transferred. Security is provided using public key encryption and hashing techniques. The university and students registered on the blockchain are provided with a private key. When a student completes a registered course, the credit is converted into a token and saved in the blockchain wallet. To ensure the security of the proposed system, the impact of various attacks on the system has been analyzed and the system was found to be resistant to those attacks. The scalability of the system is tested by load testing by increasing the number of universities registering on the blockchain platform and analyzing the maximum response time and minimum response time.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Taif University Researchers Supporting Project Number (TURSP-2020/114), Taif University, Taif, Saudi Arabia.

References

[1] S. N. Mohanty, K. C. Ramya, S. S. Rani et al., "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

[2] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: a blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2020.

[3] B. Nguyen, T. Dao, and B. Do, "Towards a blockchain-based certificate authentication system in Vietnam," *PeerJ Computer Science*, vol. 6, p. 266, 2020.

[4] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *Proceedings of the Business Information Systems Workshops*, pp. 185–196, Seville, Spain, June 2019.

[5] E. Karataş, "Development of Ethereum blockchain based document verification smart contract for moodle learning management system," *Information Technology Journal*, vol. 11, no. 4, pp. 399–406, 2018.

[6] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," *Journal of Computing in Higher Education*, vol. 32, no. 1, pp. 109–134, 2019.

[7] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: a systematic review," *Applied Sciences*, vol. 9, no. 12, p. 2400, 2019.

[8] G. Chen, B. Xu, M. Lu, and N. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, 2018.

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? -A systematic review," *PLoS One*, vol. 11, no. 10, 2016.

[10] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of used cryptography in blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.

[11] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, and R. I. Pradhan, "A distributed credit transfer educational framework based on blockchain," in *Proceedings of the Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T)*, Allahabad, India, September 2018.

[12] J. C. Farah, A. Vozniuk, M. J. Rodriguez-Triana, and Gillet, "A blueprint for a blockchain-based architeture to power a distributed network of tamper-evident learning trace repositories," in *Proceedings of the IEEE 18th International Conference on Advanced Learning Technologies (ICALT)*, Mumbai, India, July 2018.

[13] C. BouSaba and E. Anderson, "Degree validation application using solidity and Ethereum blockchain," in *Proceedings of the Southeast Con*, Huntsville, AL, USA, April 2019.

[14] M. Han, Z. Li, J. S. He, D. Wu, Y. Xie, and A. Baba, "A novel blockchain-based education records verification solution," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, Fort Lauderdale Florida USA, October 2018.

[15] R. Arenas and P. Fernandez, "CredenceLedger: a permissioned blockchain for verifiable academic credentials," in *Proceedings of the IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, Germany, June 2018.

[16] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," in *Proceedings of the IEEE International Conference on Applied System Innovation*, Chiba, Japan, April 2018.

[17] B. Duan, Y. Zhong, and D. Liu, "Education application of blockchain technology: learning outcome and meta-diploma," in *Proceedings of the IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Shenzhen, China, December 2017.

[18] T. Arndt and A. Guercio, "Blockchain-based transcripts for mobile higher-education," *International Journal of Information and Education Technology*, vol. 10, no. 2, pp. 84–89, 2020.

[19] D. Singh, V. Kumar, V. Yadav, and M. Kaur, "Deep neural network-based screening model for COVID-19-infected patients using chest X-ray images," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 35, no. 03, p. 2151004, 2021.

[20] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.

[21] G. Hu, S.-H. K. Chen, and N. Mazur, "Deep neural network-based speaker-aware information logging for augmentative and alternative communication," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 2, pp. 138–143, 2021.

[22] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[23] B. Gupta, M. Tiwari, and S. Singh Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.

[24] Xu Yang and T. Qiu, "Human activity recognition and embedded application based on convolutional neural network," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 1, pp. 51–60, 2021.

[25] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.

[26] D. Jiang, G. Hu, G. Qi, and N. Mazur, "A fully convolutional neural network-based regression approach for effective chemical composition analysis using near-infrared spectroscopy in cloud," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 1, pp. 74–82, 2021.

[27] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.