E-Lock: A Blockchain Framework for Enhancing Security and Trust in E-Learning

E-Lock: A Blockchain Framework for Enhancing Security and Trust in E-Learning

Kashif Laeeq[1], Muhammad Asad Abbasi[2], Amna Shabbir[3], Abdullah Ayub Khan[4*], Hafsa Habib[5]
[1] Federal Urdu University of Arts, Sciences & Technology, Karachi, Pakistan
[2] Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University
[3] Department of Electronic Engineering, NED University of Engineering & Technology, Karachi, Pakistan
[4] Department of Computer Science, Bahria University Karachi Campus, Karachi 73500, Pakistan
[5] Department of Computing, (FCIT), Indus University, Karachi, Pakistan

Email: kashiflaeeq@fuuast.edu.pk, muhammad.asad@bbsul.edu.pk, aamna@cloud.neduet.edu.pk, abdullahayub.bukc@bahria.edu.pk, hafsahabib76@yahoo.com

Corresponding Author: Abdullah Ayub Khan, abdullahayub.bukc@bahria.edu.pk

Received: 27-08-2024; **Accepted:** 01-12-2024; **Published**: 30-12-2024

Abstract: This paper introduces E-Lock, a blockchain-based framework aimed at enhancing security, scalability, and trust in e- learning systems. By leveraging Polygon's blockchain platform, E- Lock utilizes decentralized ledgers and smart contracts to improve transparency, efficiency, and data security in digital education environment. Polygon's high-throughput, cost-effective architecture overcomes limitations in traditional e-learning platforms, enabling scalable, low-cost transaction management. Through decentralized consensus, cryptographic hashing, and interoperability with the Ethereum ecosystem, E-Lock ensures data integrity, verifiability, and secure operations while reducing vulnerabilities to malicious attacks. The framework empowers educational institutions to maintain data sovereignty, protect intellectual property rights, and foster resilience and transparency in the e-learning ecosystem. This paper provides practical insights and guidance for researchers in the field of Technology-Enhanced Learning (TEL), presenting a comprehensive analysis of the benefits and trade-offs associated with blockchain integration in educational platforms.

Keywords: E-Lock, Blockchain-based framework, E-learning, Technology-Enhanced Learning, Polygon blockchain platform, Online Learning.

1. Introduction

In the modern digital era, the integration of technology in education has fostered the widespread adoption of e-learning platforms. However, concerns persist regarding data security, such as data breaches and unauthorized access. Implementing centralized traditional data management systems makes them prone to risks hence the need for developing emerging strategies.

Blockchain is among the decentralized technologies that facilitate e-learning by providing an assured security, credibility, and verifiable credential system. They allow for incentive and smart contracts and make processes as decentralized and accessible as possible. When it comes to problems like security, privacy, and trust within the e-learning ecosystem, the use of blockchain can be highly effective. Decentralized data management means that control is lodged in the various members of the network as opposed to being concentrated [7]. Blockchain decentralizes data and allows only certain nodes to make changes to it; it can symbolize this through consensus. This system improves security and backup, whereby it becomes challenging for transaction recordings to be

forged or changed without consensus on the network, as shown in Figure 1 below. In other words, decentralization helps increase transparency, security, and reliability due to the distribution of control and responsibilities among the members of the network.

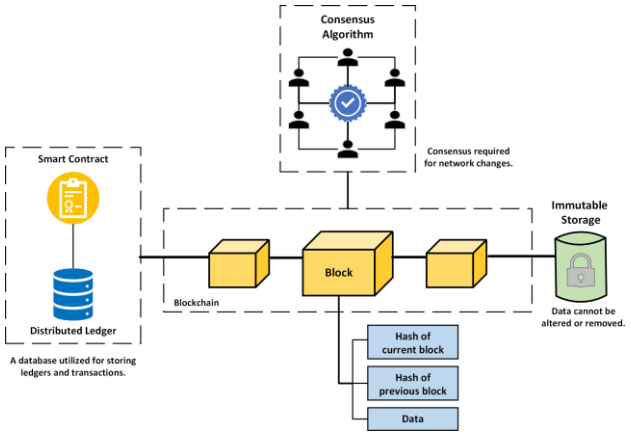


Figure 1. Blockchain mechanism for data protection

In this paper, we propose E-Lock, a novel blockchain architecture suitable for building trustworthy e-learning plat- forms. E-Lock uses global ledgers and self-executed contracts to build up identification and documentation solutions for education that increase openness, speed, and safeguarding. Through the use of secure data storage, E-Lock reduces the probability of having fake transactions and eradications, which creates an appropriate atmosphere for learning and teaching. Fundamentally, E-Lock employs the distributed ledger which is characteristic of the blockchain to promote the consistency and auditable characteristics of data transactions in e-learning applications. Cryptographic hashing [10], decentralization of consensus, and distributed storage make fraudulent control by oppressive centralized servers impossible, diminishing single sources of failure. Such de-centralized architecture not only enhances security but also brings about trust with the stakeholders due to the authenticity and integrity of data. Smart contracts are the key elements of E-Lock's effectiveness; being self-contained digital contracts that are performed when certain circumstances occur. Such smart contracts allow for real-time tracking of data access and utilization in the context of the e-learning environment and thus restore the overall clarity and accuracy of the process [6][9]. This not only reduces human interjection and error that may emanate from deliberate manipulation of the system but also eases frequent tasks such as authentication, access control, and content delivery.

This research paper presents E-Lock as an innovative solution for enhancing security in e-learning environments. By improving platform security, fostering transparency, and streamlining data management, E-Lock creates a more trust- worthy and resilient digital education ecosystem. The paper is structured as follows: Section I introduces the significance of security in e-learning. Section II reviews literature on security issues in e-learning systems, approaches to mitigate these issues, and the effectiveness of current measures. Section III discusses blockchain technology, including its components and impact on information security. Section IV outlines the E-Lock framework, detailing its components, operations, and blockchain selection, compares Ethereum and Polygon, and analyzes the benefits and trade-offs of the chosen blockchain. The paper concludes with the final section.

2. Literature Review

E-learning ecosystem have significantly transformed the delivery of education, providing greater accessibility and flexibility for learners and educators. However, as these systems grow in complexity and user base, they face a range of security threats. Ensuring the confidentiality, integrity, and availability of data is crucial for maintaining trust and functionality within these platforms. In this literature review author explores the security issues in e-learning systems, the techniques for addressing them, and the effectiveness of various countermen- sures, with additional emphasis on cryptography, digital rights management (DRM), and biometric authentication.

A. Security Issues in E-Learning

As an offshoot of computer-based instruction, e-learning, which is also referred to as electronic learning, involves the use of information technology in the delivery of curriculum content and instruction from a distance. Flexible, scalable, and easily accessible, e-learning is slowly finding its way into the education system because it provides learners with content at their discretion. As the world goes digital, there is a need to secure e-learning platforms with a guarantee that users are dealing with genuine platforms. However, e-learning has several risks such as data leakage, weak authentication, phishing, internal threats, viruses, and DoS [1]. These vulnerabilities can lead to concerns with the educational material and resources' authenticity, privacy, and accessibility alongside threats to individual privacy. To address these challenges, an e- learning environment should have strong security features like encryption, strong authentication, and secure data management [2]. These measures contribute to the development of safety for learners and educators in guaranteeing safety against several dangers.

Malicious Attacks: E-learning systems also suffer from attacks such as spyware, Trojan, and adware since these attacks monitor user activities and gain access to personal information [3]. Moreover, as a part of the social engineering attack vector, the attackers can insert concealed code to links in sponsored social media posts, which may lead to the disclosure of personal data or work with spam content.

Hacker Intrusions: These include breaking into e-learning systems through having a loophole in the authentications brute force attack dictionary attack or even an SQL injection attack. In case they get inside, they can modify or delete sensitive data that people study, for example, academic records; and user accounts.

1) Phishing and Spyware: These include breaking into e- learning systems through having a loophole in the authenti- cations brute force attack dictionary attack or even an SQL injection attack. In case they get inside, they can modify or delete sensitive data that people study, for example, academic records; and user accounts.

2) Confidentiality, Integrity, and Availability: According to Rosenberg [13], information security in e-learning systems main elements include confidentiality, integrity, and availability. Confidentiality ensures that information is not disclosed to unauthorized personnel while integrity ensures that data is not tampered with by unauthorized personnel. Availability encompasses the conditions that dictate that systems must run as planned even if interrupted by malicious people.

Security Issue	Description
Data Breaches	Unauthorized access to personal and sensitive data.
Phishing Attacks	Deceptive attempts to obtain sensitive information.
Malware	Infect data confidentiality, integrity, and availability.
Denial of Service (DoS)	Legitimate information is inaccessible by overwhelming illegitimate requests.
Unauthorized Access	Allowing illegal access, and compromising sensitive information.
Ransomware	Malicious software that encrypts files and demands payment for their release.

Table1 CHALLENGING ISSUES IN E-LEARNING ENVIRONMENT

Approaches to Mitigate Security Issues

Some solutions have been suggested in order to overcome var- ious security threats affecting e-learning environments. These countermeasures include increasing authentication measures to improve data transfer encryption and the use of biometric authentication [5].

Cryptography: Security has been proven to be a critical element in e-learning and cryptography is a key enabler of the security of data sent through e-learning systems. It entails transforming data into a form that cannot be understood by anyone who is not supposed to understand it. There are two main types of encryptions:

Symmetric Key Encryption: Involves the use of a single key to lock and unlock the data so this is called the single key system. It is very efficient but, in this method, key management is a very sensitive issue.

Asymmetric Key Encryption: Involves the use of a pair of keys; public and private keys. Data encryption is done by the public key, and decryption can be done by the private key, which is beneficial for sensitive transactions. Specifically, JCrypTool and Cryptool2 are the most popular when it comes to the application of cryptographic protections in systems of e-learning.

3) Digital Rights Management (DRM): Another requirement to advance e-learning is the usage of Digital Rights Man- agreement (DRM) for the protection of content in the form of intellectual property and copyrights. As for the general definition, DRM enables the creators and organizations to dictate how the content is accessed, shared, or modified. For instance, DRM can be used to restrict access to learning materials, questions, students' performance, and other valuable resources in the system.

4) As a result of DRM, educational institutions are able to keep their content safe from piracy and force only the rightful parties to be allowed to access and alter the important teaching, learning, and educational material.

5) Biometric Authentication: Password, smart cards, and digital signatures [19] are the most often used in e-learning systems but are not very reliable. Passwords can be hacked easily by friends or other people if students share them or simply lose their secrets. However, biometric authentication gives a better solution by using specific physical aspects like fingerprints, and facial, or retina scans.

6) By so doing, biometric authentication confirms that only those who have a permit to access the e-learning platform are the ones who will get an opportunity to do so. Biometric data are more difficult for the hacker to copy or embezzle when compared to passwords or smart cards, which makes this security feature a very strong one.

7) Digital Watermarking: Digital watermarking is another form of security in the e-learning platforms for multimedia materials. Thus, integrated and hidden watermarks, call-outs, or metadata in audio, video, or image forms are used by e- learning systems to avoid piracy. Whenever question papers or any important study material are watermarked digitally, it becomes difficult for the data to be stolen or tampered with.

B. *Effectiveness of Security Measures*

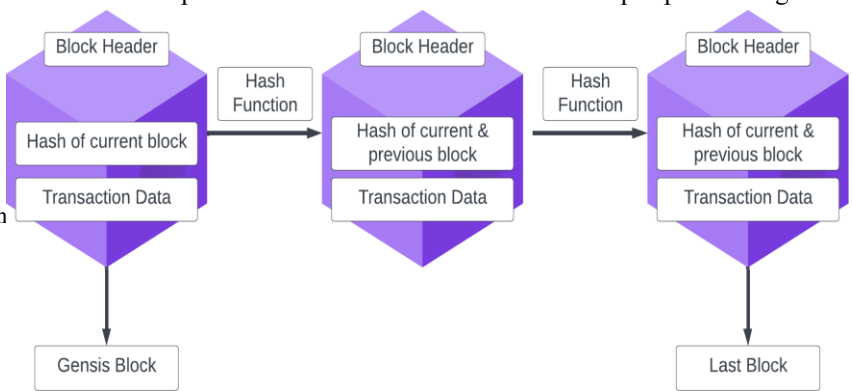
The effectiveness of these countermeasures has been proven to enhance the security of e-learning platforms; despite the fact that each of the strategies discussed here has its drawbacks.

- **Cryptography** is very useful in protecting data in transmission, but its efficiency is usually determined by key management and secure encryption algorithms. In Symmetric Key Encryption, the entire procedure is faster, but not secure as Asymmetric Key Encryption, which while being more secure may take longer time in real usage.
- **DRM** makes it easier to implement measures that protect the rights of authors and owners of other material that is used in an e-learning platform to prevent unauthorized sharing of that material. That said, DRM should be used to ensure that it doesn't overwhelm the users while at the same time offering protection to the rich learning resources available online.
- **Biometric authentication** is especially useful in this case since it would be hard for an imposter to pretend to be someone else since they include biological characteristics. However, biometric data must be stored securely to avoid leakages, and issues to do with the privacy of biometric information have to be considered.
- **Digital watermarking** Multimedia content protection goes a notch higher with digital watermarking which helps hackers to be easily detected whenever they steal or misuse content. However, it is more effective for protecting static content than for securing dynamic data or live communication.

I. BLOCKCHAIN TECHNOLOGY

Blockchain is a novel technology that was first put into practice with the creation of Bitcoin by Satoshi Nakamoto. Essentially, it functions as a digital ledger where transactions are recorded in a distributed and decentralized manner. It is widely regarded as a highly secure, transparent, immutable, and decentralized system.

The blockchain is a network of computers that maintains a secure and unique public ledger consisting of various data,



including transactions, in a decentralized and transparent manner without requiring central authority. It belongs to the distributed ledger technologies, which depend on a public registry that can be accessed and altered by multiple nodes on the network. To approve changes, nodes need consensus from any node on the network. The blockchain technology is composed of blocks chained together, containing transactions that are validated by the entire network of nodes as shown in Figure 2.

Fig. 2. Blockchain architecture

A. ***Components of blockchain***

A blockchain is a linked list of blocks that contains sets data. Each block has a cryptographic hash in its transaction list and another hash of the previous block. Transactions' hash is stored in a cryptographically secured data structure called a Merkle tree. The following represent the basic terminology for blockchain:

- *Node* - A node is a computer or device linked to a blockchain, possessing either a complete or partial record

of the blockchain. Nodes may serve different functions within the network.

- *Blockchain* - A blockchain is a decentralized record kept by interconnected nodes, forming a chain of blocks. Each complete node holds an entire and authentic version of the ledger.
- *Block* - A block comprises various records, such as transactions, within the blockchain. It includes hashes representing its current state and its connection to the preceding block.
- *Merkle tree* - A Merkle tree is a hierarchical arrangement of hashed transaction data, culminating in a single root hash. It serves to maintain the security and efficiency of the blockchain.
- *Consensus* - Consensus is a protocol allowing nodes to unanimously approve newly generated blocks without central oversight. Different methods, like proof-of-work or proof-of-stake, enable block addition in a blockchain.
- *Miners* - Miners are nodes tasked with crafting new blocks in a blockchain by compiling transactions. They are usually incentivized with cryptocurrency rewards. In specific scenarios like an LMS blockchain, miners may not be applicable.
- *Smart Contract* - Smart contracts [9] are automated agreements encoded with specific terms. They execute transactions automatically when predefined conditions are fulfilled, eliminating the need for intermediaries.
- *Peer-to-Peer Network* - A peer-to-peer network is a decentralized system where nodes interact directly with one another, eliminating the need for a central server. In blockchain, these networks enable distributed consensus and data sharing among participants.

B. Information Security in Blockchain Systems

Information security is crucial for all users of information systems, particularly within blockchain systems, which handle sensitive transaction data requiring protection against unauthorized access. Since blockchain operates over the internet, it involves virtual communication among network participants, making it susceptible to security threats. According to Li et al. [20], various popular blockchain systems have experienced real attacks, highlighting the importance of security measures.

The IA triad—confidentiality, integrity, and availability —serves as a foundational security model, as discussed by Samonas [21]. These elements are essential for securing information within blockchain systems, particularly when considering Bitcoin, the first major blockchain implementation. Rui Zhang et al. [22] emphasize the need for these security properties to prevent attacks on blockchain networks.

- **Confidentiality:** It is important that the transaction data should be saved in such a way that only those who have permission to use it should be allowed to touch the data to guarantee its authenticity.
- **Integrity:** Integrity of the data is very important, more especially in the environments where the data processing is distributed such as vehicle registries and warehouse receipts where certain data are not supposed to be changed by anyone other than those authorized to do so.
- **Availability:** It must allow the participation of multiple users and make it possible for any of them to view transactions at any one time in any location.
- **Consistency:** The ledger must always be synchronized across all the participants even though the architecture and the processes involved differ from one financial institution to the other.
- **Anonymity:** The user identities have to remain safe so that the particular data will only be accessible to specific individuals, regardless of the issues such as the constant need for the user to authenticate.
- **Unlink-ability:** Interactions should not be associated since this would present more info about the users which is sensitive.
- **Double-Spending Prevention:** There must be ways to avoid various problems such as double spending where the same digital coin is used to pay for something more than once.

C. Blockchain based E-Learning Systems

The Massachusetts Institute of Technology (MIT) has tested a system called Blockcerts for the issuing and sharing of digital credentials [14]. With this, this initiative highlights how blockchain can offer verifiable and portable attestation that does not depend on central authorities.

The study of Sun et al. [12] suggests the application to resolve the challenges of e-learning systems: the use of blockchain. Blockchain provides an efficient, secure, and trans- parent way of recording resources, replaces middlemen with smart contracts, and expands the credibility of achievements with certificates. This approach has the potential to transform online education but can claim this only after effective practice and experimentation.

A paper by Miah [13] explains how the idea of blockchain can revolutionize the manner in which educational records are

maintained by offering an unalterable and transparent system of recordkeeping of academic records. Thus, they describe the possibilities of blockchain to fight against the fabrication of academic records and to make the employers' and academic institutions' verification process more effective.

The author Ubaka-Okoye [15] has suggested a Blockchain framework for e-learning to ensure improved data integrity, security, and credibility. However, the area of scalability and the regulation of the same issue present a significant problem in the generalized use of the service.

Incorporating blockchain technology into an e-learning platform for reliability is addressed by Ramasamy [16]. The subject of this research is how de-centralization can reinforce security, transparency, and access in the e-learning environment. The paper also looks at how blockchain will help streamline credential verification and bring about confidence in academic transcripts.

Samala [17] presents different possibilities for blockchain application including increasing the security and openness of academic certificates, improvement of administrative actions, and implementation of new paradigms of lifelong learning and certification.

Security in e-learning has been a huge concern, but blockchain technology holds great solutions to improve security. Some of the characteristic features like immutability, decentralized verification, and secure authentication, solve issues like data integrity, authentication, contended and content distribution, and identity verification [10]. It was also suggested that e-learning platforms can be secured by using blockchain to enhance users' trust, enhance the transparency of academic credentialing, and prevent fraud and unauthorized access [6]. Through these modern strategies, e-learning platforms will promote safer experiences for digital learning thereby enhancing the confidence of the users.

3. Propose Framework, E-Lock

The proposed framework, E-Lock, is based on blockchain technology which is inherently decentralized and cannot be altered. This makes it possible that the data put in the e- learning ecosystem cannot be tampered with or manipulated by other people. Blockchain, decentralized ledgers, and smart contracts improve security, transparency, efficiency, and trust in the e-learning setting. The proposed main E-lock framework is depicted in Figure 3.

*A. **Components of E-Lock***

The essentials of the E-Lock framework are node identity confirmation and a distributed data exchange system, with a reward system for nodes, proof of stake to validate a block, a consensus mechanism to safeguard against unauthorized access, and the use of permission (private) blockchain. This framework has the objective of ensuring data accuracy, and credibility among the users to achieve a safe and efficient e-learning atmosphere.

*1) **Decentralized Data Management:*** E-Lock employs a de- centralized ledger system utilizing blockchain technology, spreading data across nodes and requiring consensus for modifications. This approach enhances security, resilience, and redundancy by mitigating single points of failure and reducing susceptibility to attacks. Decentralization distributes control and responsibility among network participants, fostering trust and transparency. This distributed architecture mitigates the risks of single points of failure and minimizes vulnerability to malicious attacks.

Immutable Ledger: At its core, E-Lock leverages blockchain's immutable ledger to ensure the integrity and verifiability of data exchanges within e-learning platforms. Through cryptographic hashing and distributed storage, E-Lock provides undisputable proof of data authenticity and integrity, fostering trust among stakeholders.

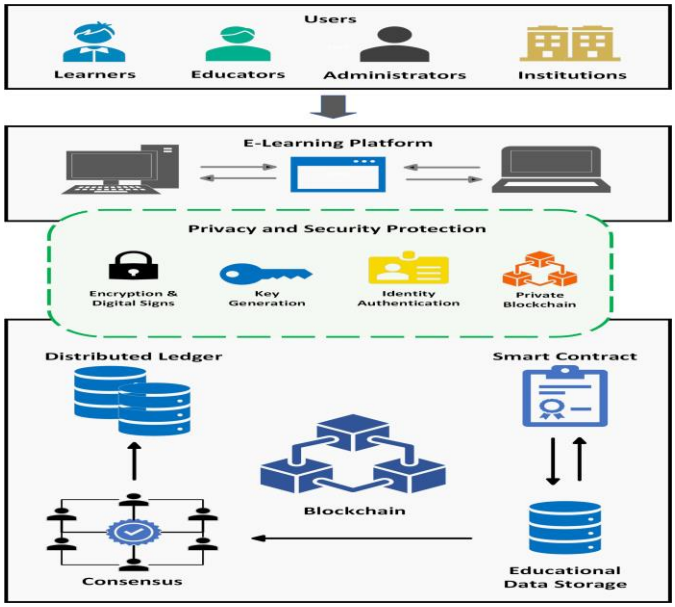


Fig. 3. Block diagram of E-Lock framework

2) ***Smart Contracts for Automation:*** E-Lock utilizes smart contracts, which enable autonomous digital agreements executed upon predefined conditions. These contracts [6] facilitate real-time monitoring of data access and usage, enhancing transparency and accountability throughout the e-learning ecosystem [9]. By automating processes such as authentication, access control, and content delivery, E-Lock minimizes human intervention, reducing the risk of errors and manipulation.

3) ***Tamper-Proof Data Management:*** E-Lock ensures tamper- proof data management, mitigating the risk of fraudulent activities and unauthorized alterations [7]. Blockchain, as a decentralized and distributed ledger, records transactions in a secure and immutable manner. Each block in the chain contains a cryptographic hash of the previous block, creating an achronological and unchangeable record of data. This fosters a conducive environment for learners and educators by providing a secure and trustworthy ecosystem.

4) ***Data Sovereignty and Institutional Autonomy:*** Empowers educational institutions to uphold data sovereignty, safeguarding sensitive information and preserving institutional autonomy. By entrusting data management to a decentralized network of nodes, E-Lock mitigates risks associated with data monopolization and external interference.

5) ***Transparent Credential Verification:*** The proposed frame- work facilitates transparent credential verification through decentralized ledgers, ensuring the authenticity and validity of educational credentials. This enhances trust within the e- learning ecosystem and mitigates the risk of credential fraud.

B. ***E-Lock Operations***

The E-Lock framework starts with the establishment of the blockchain network, consensus algorithms, and the establishment of an educational data transaction register. Next is user registration where educators and learners create their public-private keys for authentication. Smart contracts are then used when addressing different functionalities.

These are the authentication of the user, the control of access to various contents, and the distribution of content. Next comes the flow of educational data entry and an execution of validation techniques to check the credibility of the data. Users' activities' records are set and confirmed through transactions while valid transactions form blocks that are added to the blockchain successively. The access control policies are facilitated by smart contracts [9] in which only the permitted users can access certain resources. The education delivery platform provides an optimized delivery of content when education content is to be delivered at certain times,

and a safe assessment of student performances which is recorded on the blockchain. It is also important to note that credential verification is done through transparent methods thus employers and institutions can verify the same. Monitoring and auditing are performed constantly to maintain the protection and integrity of the networks as well as to align with set regulations. The engagement of users is promoted with input from the users used to improve the platform in case of any recommendations by the users. New problems are solved depending on the existing needs to maintain the scalability, security, and performance of the system, with regular maintenance and updates. The procedure of E-Lock has been shown in Figure 4 and, Procedure-E-Lock exhibits the flow of the E-Lock process in the framework.

The pseudocode for creating a node in the e-learning environment is described in detail in Pseudocode-E-Lock. The creation of nodes depends on whether the request is from an institution or not. It includes the generation of keys, creation of address, connection initiation, beta computation, and distribution of registration to other nodes in the network.

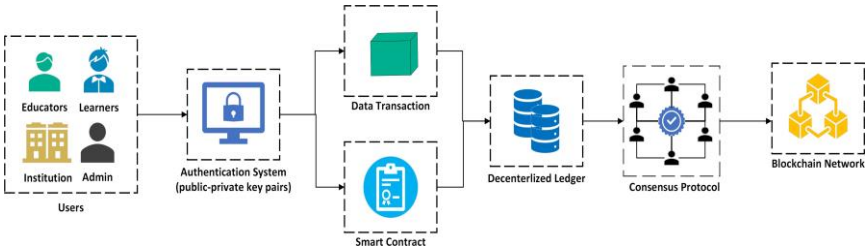


Fig. 4. Block diagram of E-Lock procedure

1 Procedure-E-Lock
1: Initialize_Blockchain_Network
2: Register_Users_And_Generate_Keys
3: Deploy_Smart_Contracts
4: Enter_And_Validate_Educational_Data
5: Manage_And_Validate_Transactions
6: Form_And_Add_Blocks
7: Control_And_Authorize_Access
8: Deliver_Content_And_Conduct_Assessment
9: Manage_And_Verify_Credentials
10: Monitor_And_Audit_Network
11: Handle_User_Interactions_And_Feedback
12: Perform_Maintenance_And_Updates

C. *Blockchain Platform for E-Lock Framework*

Therefore, the E-Lock framework has to identify the most effective and appropriate web-based blockchain platform in the context of performance, security, and scalability for e-learning systems. Some of the leading blockchains on the market that differ in terms of advantages and disadvantages for blockchain implementation include Ethereum and Polygon [11, 12, 13, 14]. Here, the author presents a thorough analysis of these platforms, which culminates in the justification for the choice of the most appropriate blockchain for the E-Lock framework.

2 Pseudocode-E-Lock

```
Input: Node registration application
Output: A freshly created node L in the e-learning network
If (Request ==Institution):
        Create a full node L
Else
        Create a lightweight node L
End if
        (public_key, private_key) ← Generate_Keys();
        Address ← Concatenate(Institution_Name(), public_key);
        Wallet_Address ← Concatenate(Institution_Name(), public_key);
        Initialize_Connection();
        Address ← Address + Node_IP_Address();
        Beta ← Calculate_Beta(Threshold);
for each node n ∈ Total_Nodes - Beta Do
        Distribute_Registration(Node_List, L);
End for
        L ← Finalize_Registration(Node_List);
```

Comparison of Ethereum and Polygon Platforms: Ethereum is one of the first complex blockchains and a leading platform for smart contracts and decentralized applications (dApps) verified by the Ethereum network. Polygon, on the other hand, is a Layer-2 solution that is designed to help solve the Ethereum scaling problem whilst remaining interoperable with Ethereum. In table 2, the author compares these two platforms based on key criteria relevant to the E-Lock framework.

Criteria	Ethereum	Polygon
Transaction Speed	15-30 transactions per second (TPS)	Up to 65,000 TPS
Transaction Costs	High gas fees, especially during network congestion	Low transaction fees, typically a fraction of Ethereum's costs
Security	Highly secure due to its large number of nodes and decentralization	Inherits Ethereum's security but has a smaller network of validators
Scalability	Limited scalability, struggles with high network activity	Built for scalability, handling high throughput with ease
Ecosystem Support	Largest dApp ecosystem, extensive developer resources	EVM-compatible, benefits from Ethereum's ecosystem while providing enhanced scalability

TABLE II COMPARISON OF ETHEREUM AND POLYGON

Based on the comparison, Polygon is chosen as the preferred blockchain platform for the E-Lock framework. Several factors influenced this decision:

- **Cost-Effectiveness:** The significantly lower transaction fees associated with Polygon make it a more practical choice for an e-learning system [20, 21, 22, 23], where small and frequent transactions (such as issuing digital certificates, recording attendance or processing payments) are com- mon.
- **Scalability:** The ability to handle up to 65,000 trans- actions per second makes Polygon a suitable option for accommodating a large number of users [24, 25, 26], ensuring the system remains responsive and efficient as the platform scales.

- **Compatibility with Ethereum:** As a Layer-2 solution [8], Polygon is EVM-compatible, allowing developers to use existing Ethereum tools and libraries while benefiting from improved performance and lower costs.
- **Security Considerations:** Polygon is less decentralized than Ethereum, it still inherits a substantial portion of Ethereum's security characteristics. For the purposes of the E-Lock framework, this level of security is adequate to ensure data integrity and authenticity in an e-learning context [10].

2) ***Benefits and Trade-offs of the Chosen Blockchain****:* The decision to use Polygon for the E-Lock framework presents several benefits but also entails some trade-offs [15, 16, 17, 18, 19], as summarized by the author in table 3.

Aspect	Benefits	Trade-offs
Transaction Fees	Lower costs make it suitable for frequent micro-transactions	Fees could still increase during times of high network activity
Performance and Scalability	High throughput supports a large number of users	Reduced decentralization compared to Ethereum
Ecosystem Compatibility	EVM compatibility enables easy porting of dApps from Ethereum	Smaller developer community than Ethereum
Security	Inherits many of Ethereum's security features	Relies on Ethereum's security, making it not entirely independent

TABLE III BENEFITS AND TRADE-OFFS OF THE POLYGON PLATFORM

The selection of Polygon aligns with the primary objectives of the E-Lock framework by ensuring cost-efficiency, scalability, and adequate security. However, the trade-offs in decentralization and ecosystem size [27, 28, 29] should be considered in future development plans, particularly as the platform grows.

4. Conclusion

This research paper introduces E-Lock, a blockchain- based framework designed to enhance security and scalability in e-learning environments through Polygon's blockchain platform. E-Lock employs decentralized data management and smart contracts to ensure transparency, integrity, and accountability, effectively addressing common issues like data tampering, unauthorized access, and scalability limitations. By automating authentication and access control with smart contracts, E- Lock minimizes human error and streamline operations, while Polygon's cost-efficient transactions and high throughput support the system's scalability needs. Although trade-offs in decentralization and a smaller validator set exist, E-Lock's decentralized architecture, cryptographic hashing, and real-time monitoring foster a resilient ecosystem that protects academic freedom and intellectual property. This approach represents a paradigm shift in security management for e-learning, providing a robust foundation for a secure and transparent digital education landscape. As blockchain technology advances, E-Lock holds significant potential to redefine Technology Enhanced Learning (TEL) by offering a reliable, scalable, and trusted framework for digital education.

References

[1] E. Kelso, A. Soneji, S. Rahaman, Y. Soshitaishvili, and R. Hasan, “Trust, Because You Can’t Verify:Privacy and Security Hurdles in Education Technology Acquisition Practices,” arXiv.org, 2024. https://arxiv.org/abs/2405.11712v2 (accessed Nov. 06, 2024).

[2] Harjinder Singh Lallie, A. Thompson, Elzbieta Titis, and P. Stephens, “Understanding Cyber Threats Against the Universities, Colleges, and Schools,” arXiv (Cornell University), Jul. 2023, doi: https://doi.org/10.48550/arxiv.2307.07755.

[3] R. Hassan, W. Wahi, N. H. A. Ismail, and S. A. B. Awwad, “Data Security Awareness in Online Learning,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 4, 2022, doi: https://doi.org/10.14569/ijacsa.2022.0130432.

[4] S. Khatri, A. K. Cherukuri, and F. Kamalov, “Global Pandemics Influence on Cyber Security and Cyber Crimes,” Feb. 2023, doi: https://doi.org/10.48550/arxiv.2302.12462.

[5] P. Chatterjee, R. Bose, S. Banerjee, and S. Roy, “Enhancing Data Security of Cloud Based LMS,” Wireless Personal Communications, Mar. 2023, doi: https://doi.org/10.1007/s11277-023-10323-5.

[6] Khan, M., Alam, M., Zaman, H. (2024). ”Blockchain and Smart Contract- Based Frameworks for Secure E-Learning Systems: A Comparative Review.” International Journal of Learning Analytics and Artificial Intelligence for Education, 12(1), 15-32.

[7] Nguyen, L., Dinh, C., Duong, H. (2023). ”Enhancing Security and Privacy in Blockchain-Based Learning Management Systems.” Journal of Educational Technology Research and Development, 71(3), 331-350.

[8] Patel, A., Shah, R., Mehta, V. (2023). ”Scalability Challenges and Solutions in Blockchain Applications for E-Learning.” IEEE Transactions on Education, 66(4), 399-412.

[9] Zhang, R., Lee, Y., Lim, S. (2024). ”Smart Contracts and Automation in Decentralized Learning Platforms: A Framework for Enhanced Transparency.” Blockchain Research Journal, 9(2), 99-118.

[10] Garcia, E., Rivera, L. (2024). ”Exploring the Role of Cryptographic Hashing in Secure Blockchain-Based E-Learning Platforms.” Journal of Information Security and Applications, 71, 103197.

[11] Yoon, J., Park, H., Kang, M. (2023). ”Comparing Blockchain Platforms for Educational Applications: Ethereum vs. Polygon.” Digital Education Research Review, 17(2), 289-305.

[12] Sun, H., Wang, X., Wang, X. (2018). Application of blockchain technology in online education. International Journal of Emerging Technologies in Learning, 13(10).

[13] Miah, M. (2020). Blockchain technology in peer-to-peer elearning: Opportunities and challenges. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 4901).

[14] Capece, G., Levialdi Ghiron, N., Pasquale, F. (2020). Blockchain technology: Redefining trust for digital certificates. Sustainability, 12(21), 8952.

[15] Ubaka-Okoye, M. N., Azeta, A. A., Oni, A. A., Okagbue, H. I., NicholasOmoregbe, O. S., Chidozie, F. (2020). Blockchain framework for securing e-learning system. Institutions, 27, 28.

[16] Ramasamy, L. K., Khan, F. (2024). Blockchain-Based E-Learning Plat- form: Transforming Education Through Decentralization. In Blockchain for Global Education (pp. 103-123). Cham: Springer Nature Switzerland.

[17] Samala, A. D., Mhlanga, D., Bojic´, L., Howard, N. J., Pereira Coelho, D. (2024). Blockchain Technology in Education: Opportunities, Challenges, and Beyond. International Journal of Interactive Mobile Technologies, 18(1), 20-42.

[18] Mohd Alwi, Najwa Fan, Ip-Shing. (2009). Information security man- agement in E-learning. 1 - 6. 10.1109/ICITST.2009.5402507.

[19] C.-C. Lee, C.-T. Li, Z.-W. Chen, and Y.-M. Lai, “A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System,” Information Technology And Control, vol. 47, no. 2, Jun. 2018, doi: https://doi.org/10.5755/j01.itc.47.2.18506.

[20] Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841

[21] Samonas, S., Coss, D. (2014). THE CIA STRIKES BACK: REDEFIN- ING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN

[22] SECURITY. Journal of Information System Security, 10(3).

[23] Zhang, R., Xue, R., Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), 1-34

[24] Khan, A. A., Laghari, A. A., Baqasah, A. M., Bacarra, R., Alroobaea, R., Alsafyani, M., & Alsayaydeh, J. A. J.(2025). BDLT-IoMT-a novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity. The Journal of Supercomputing, 81(1),1-22.

[25] Khan, A. A., Yang, J., Laghari, A. A., Baqasah, A. M., Alroobaea, R., Ku, C. S., ... & Por, L. Y.(2025). BAIoT-EMS: Consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things. Engineering Applications of Artificial Intelligence, 141, 109838.

[26] Khan, Abdullah Ayub, Asif Ali Laghari, Abdullah M. Baqasah, Roobaea Alroobaea, Ahmad Almadhor, Gabriel Avelino Sampedro, and Natalia Kryvinska."Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing."

[27] Khan, A. A., Chen, Y. L., Hajjej, F., Shaikh, A. A., Yang, J., Ku, C. S., & Por, L. Y.(2024). Digital forensics for the socio-cyber world (DF-SCW): Anovel framework for deepfake multimedia investigation on social media platforms. Egyptian Informatics Journal, 27, 100502.

[28] Khan, A. A., Laghari, A. A., Baqasah, A. M., Alroobaea, R., Gadekallu, T. R., Sampedro, G. A., & Zhu, Y.(2024). ORAN-B5G: A Next Generation Open Radio Access Network Architecture With Machine Learning for Beyond 5G in Industrial 5.0. IEEE Transactions on Green Communications and Networking.

[29] Khan, A. A., Laghari, A. A., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Bacarra, R., & Alsayaydeh, J. A. J.(2024). Secure Remote Sensing Data with Blockchain Distributed Ledger Technology: ASolution for Smart Cities. IEEE Access.

[30] Khan, A. A., Dhabi, S., Yang, J., Alhakami, W., Bourouis, S., & Yee, L.(2024). B-LPoET: Amiddleware lightweight Proof-of-Elapsed Time (PoET) for efficient distributed transaction execution and security on Blockchain using multithreading technology. Computers and Electrical Engineering, 118, 109343.