TRUSTED FRAMEWORK FOR E-LEARNING USING BLOCKCHAIN TECHNOLOGY (E-LBC)

UGC CARE APPROVED

ABSTRACT

Blockchain plays an important role in the real-world applications by providing immutability, provenance, and peer- executed smart contracts. The prominent characteristics of a blockchain, could increase security, trust, and openness to online learning. In this work, it is proposed a blockchain-based e- learning platform that has been developed as a proof-of-concept to improve assessment transparency which enables curriculum customization in the higher education sector. The development of a framework for learning using blockchain has the ability to issue credentials and automate assessments which is considered as an effective E-learning mechanism. The proposed framework demonstrates to end users, including students and teaching staff, the advantages of a blockchain back-end, The development is both pedagogical and content-neutral. Smart Contract built for the access in different levels enables trust in access. The Preliminary analysis of the framework built is analyzed on a real time basis which shows improved performance and provides assurance in online education providers, assessment processes, educational portfolio for their credentials.

Index Terms: *Blockchain,Credit System, E-Learning, SecuredLearning, Smart Contract.*

M. R. SUMALATHA
Department of Information Technology Anna University (MIT) Chennai - 44

ROZEN BERG
Department of Information Technology, Anna University (MIT) Chennai - 44

K. N. BALASUBRAMAIUM
Department of Information Technology, Anna University (MIT) Chennai - 44

I. Introduction

The power of the technology involved, blockchain, which is predicted to generate significant disruptions in a number of industries, including financial products, management of supply chains and identity management, has been proved by the rise of cryptocurrencies. Smart contracts, which are integrated self-executing programmes that establish a contract and

automatically implement promises through the exchange or exchange of digital assets when certain conditions are satisfied, are embedded in blockchains that can execute them. This is referred to as blockchain 2.0. Smart contracts may be incredibly powerful and can run any user-defined code since they can be Having to turn, as is the case for well-known ecosystems like the Blockchain and Hyperledger deployments, which allow user-defined machine states and unrestricted com- putations. [1]

[2] raised the possibility of smart contracts for e-learning by stating that ”education payment systems may automatically validate the execution of online courses through standard- ized online evaluations.” Blockchain technology and smart contracts can benefit poor countries or emerging markets by allowing reliable corporate transactions. [3]. According to, this may lead to higher-quality academic qualifications, more mutual recognition, and an open, global education market in e-learning.

II. Related Work

A. Assessing E-Learning Complexity

The unique characteristics of e-learning, determining its ef- fectiveness requires combining evaluations of students' learn- ing outcomes using conventional methodologies (such as final exams) with evaluations of their learning process by examining students' varied e-learning information . E-learning assessment is difficult because of the wide range of e-learning data, though. An autonomous e-learning assessment paradigm is required in order to lessen the workload for online educators and to increase the impartiality of the e-learning evaluation.[4]

B. Lack of a unified e-learning assessment standard

Usage of the same e-learning platform, courses may well have e-learning assessment demands that differ substantially from one another. [5] The inability to recognise and transform learners' e-learning successes into credit or certification results in a significant drop in student interest and prevents the growthof online education. [6]

C. Insecurity of e-learning digital certificates

The majority of certifications gained through online edu- cation are awarded and maintained as certificate authorities, which are quicker to locate than paper credentials but also more prone to theft and manipulation because of internet risks (such as hackers). [7] For the moment being, the

security of cryptographic keys still depends on the centralised manage- ment of the Provides The control (CA) ecosystem. However, the CA ecosystem's repute is rapidly declining and on the verge of collapse. [8]

One of the most cutting-edge technologies of recent years, blockchain technology offers potential for fresh approaches to the aforementioned issues. One of the most innovative new technologies of recent years, blockchain, has gained appeal in a variety of contexts, including academic, business, and research ones. [9] Satoshi Nakamoto first introduced the idea for a friend electronic system of payment in his paper titled "The Blockchain." Bitcoin was invented in 2008. Distributed ledgers, consensus-building procedures like PoW, PoS, and DpoS, timestamps, PBFT, and encryption methods like SHA256, a hash encryption method, and the digital asym- metric block cipher are some of the key technical concepts. The advantages of block - chain for decentralization, security, auditability, and anonymity are also discussed. [10]

Blockchain application possibilities in the field of education include the construction of a global knowledgebase for edu- cation, security or self-verification of educational credentials, secure tuition payments, and the distribution and management of educational funding. [11] [12] Due to a lack of documented application areas and theoretical support, the utilization of blockchain education technology is still in its infancy. [13] It might be difficult to find a specific example that applies to blockchain-based online learning platforms. When it comes to credit allocation and certifications for online courses, a blockchain-based approach called EduCTX was proposed, although it only solved the security problem of credit storage. [14] [15]

D. Overview of all related work

III. Proposed Work

The exception of straightforward token transfers, all network nodes in the conventional ledger cryptocurrency system have the same obligations and are completely equal to one another in terms of authority. The three main types of blockchains are public, consortium, and private, each with various degrees of decentralisation. While private blockchain chooses to give up sovereignty in favour of speedier networks and less expensive reading and writing costs, public blockchain chooses to be completely dispersed but operates gradually in case of network propagating and block reading and understanding.

A. System Architecture

The network structure of the blockchain-based typical exam- ple is more intricate than the process that takes place, which must enable the realisation of several educational activities. Additionally, the network design with a node role and a single blockchain is inappropriate for usage in e-learning systems since the learning system's uniqueness requires that the user nodes be segregated into at least two different roles, instructors and learners. In the structure created, the network allows user.

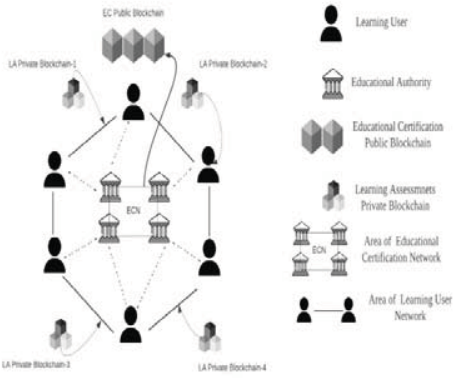

Fig. 1. Architecture Diagram for E-LBC

Nodes to enter and exit in two different sorts of roles, and each role has particular powers:

- Learning Users, shown in Figure by the red nodes.
- Education Authorities, represented in Figure as the blue nodes
- Education Certification Network (ECN): The blue region in the center of the Figure designates the ECN
- Learning Assessment Local Networks

1. *Learning Users:* The enthusiastic individuals in using the systems to study online can join up for a private account and apply to become a learner user node. There is greater than one Course Credit Wallet and a Certificate Wallet under the learner user's individual account. The credits earned from the learning user's online learning activities are added to his or her own Course Credit Wallet. Once a course has been successfully completed, the training user can utilise their remaining course credits to exchange the authentication process for the associated courses.

2. *Education Authorities:* Universities, private schools, training facilities for certain talents, etc. are only a few exam- ples of the types of schools or other educational institutions that might join the network as an education authority node and conduct online classes or tests using the technology. Just before the courses are formally exposed to the learning users, the education authority node can add the learning assessment rules of its own courses to each related smart contract for course credit calculation.

A smart contract is implemented on the proposed system's blockchain once it has been submitted by the education author- ity and approved by all of its learners. After then, the education authority is no longer the owner of the smart contract due to the autonomous execution of the smart contracts, and is com- pletely free to stay out of the course learning assessment and management process. Additionally, the system only allows the education authority nodes to issue legitimate digital certificates for their own courses.

It is developed that the network topology of the blockchain- based e-learning evaluation and certification system based on various node responsibilities and the connections between them.system, which includes three different network types and two different blockchain types. The network structure of the proposed system is described in detail below using the depiction in Figure: (LUN): Learning User Network The largest red region in Figure represents the LUN, a completely decentralised P2P network made up of all nodes of learning users who join the system for e-learning activities. Each learning user's personal account identity is tied to all infor- mation pertaining to his or her learning data records, learning accomplishments, and digital certifications. Users who arelearning can send messages using their own account IDs inan anonymous manner.

3. *Education Certification Network:* The blue region in the center of the Figure designates the ECN, which is a completely decentralized P2P network comprised of all nodes with depart- ment of education in the system. The blue blockchain symbol in Figure, referred known as the Educational Certification Public Blockchain, correlates to the ECN. All ECN nodes are responsible for the ongoing upkeep and distributed of the Public Blockchain. When a ministry of education issues a new digital certificate, its contents are broadcasted to every- one education authority nodes throughout the ECN and then verified using a consensus method. Prior to being included to the Public Blockchain for enduring preservation, the issuing authority encrypts a validated digital certificate as a digital signature.

4. *Learning Assessment Networks:* (LANs; sometimes known as LLN-X for the Learning Assessment Local Network of Education Authority X): In the system, each LAN is a local network that's also dynamically constructed by a single education department. Each LAN is depicted in Figure as an area with a purple edge containing a node of an education department and all of the nodes of its real-time learning users. The node of the education department X, which acts as the central node of the local network, is close to each node of a LAN-real-time X's learning users. Users of the actual learning in education department X can publish learning data for the related courses in LAN-X and download materials.

The Learning Evaluation Private Chain X (LA Private Blockchain-X) is shown in Figure as a purple blockchain- icon next to the LAN-X and corresponds to the LAN-X of the education authority X. Each learning user's LAN-X data is automatically analysed and transformed into course credits by turning on the smart contracts implemented just on LA Private Blockchain-X. The original learning data and course credits are subsequently bundled in blocks and persistently kept just on LA Private Blockchain-X as a source for future digital certificate issuance.

B. Smart Contract Design

The suggested system is made up of three functional com- ponents that may be described as follows and is based on the network architecture that was previously provided.

- The module for transmitting course credits and assessing e-learning runs in each LAN by creating course value blocks or uploading them to the relevant LA private blockchain.
- Tokenized issue and secure storage module: The LAN and the ECN both make use of this useful module. Check the LA Public Blockchain in LAN once the learning user's course credits have indeed been resolved before determining whether or not to offer the digital certificate. The education authority produces the SSL signing, which is placed into to the EC Open Chain following completing double digital signing, if the credits are sufficient to satisfy the need of completion of the course. After asking a third party to pay a quick visit to the EC Public Blockchain, the learning user may use both of their public keys. Decrypting and verifying the user's ssl signature requires both the learning user and the educational authority.
- The "e-learning certification distribution module" is an active module that uses a smart contract to work in the LUN. E-learning vouchers are automatically distributed based on the

percentage of learning accomplishment ratings. The learning success scores of each educational user within the LUN are periodically totaled throughout a certain time frame. Only the learning user is permitted to use the vouchers for the suggested system.

1. *E-Learning Assessment and Credit Exchange:* Any min- istry of education X inside the scheme it has the capacity to create and carry out the Course Generation Contract (CGC- X), an outsource the work. The CGC-X contract can fully autonomously compute learning users' specific course credits based just on points scored criteria of multi - variable e- learning information (including such durations of study time, exam scores, online comment activities, etc.) specified inside it. The idea of the Scholastic Credit Bank, which aims to standardise the assessment of e-learning by creating a set of universal standard credits, may also be helpful to us. The ability to create one's own LA Private Blockchains for one's Standard Credit Contracts X is available to educational bodies (SCC-X). Through these agreements, some course credits can be automatically converted to the system's accepted common standard credits.

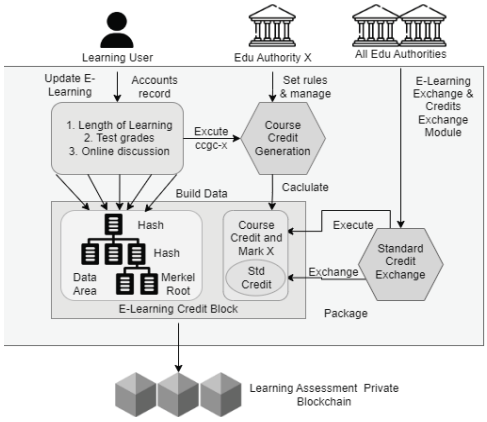

Fig. 2. Block Diagram for credit exchange

- Initializing the login in step one
- Record the data from the online course.
- The next step is calculating the course credit.
- Exchange of the regular credit is step four.
- The course credit wallet is filled up in step 5 when creditsare earned

2. *Digital Certificate Issuance and Secure Storage:* The education authority will examine the learning user's program credit balances when the learning user has finished the course study and submits a certification application. If the course point balances reach the appropriate level for course comple- tion, a digital certificate containing complete information is created and successively validated by the education department as well as the learning user. The double digital signature-enabled modern electronic certificate block has been put permanently to the EC Public Chain. The relevant learning accomplishment score is added to the studying user's Certificate Wallet while the credits for the class digital identity are concurrently removed from the Course Credit Wallet.

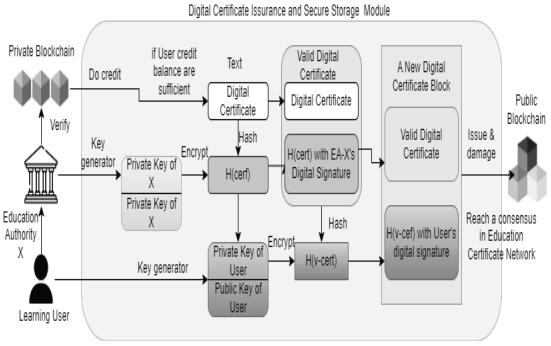

Fig. 3. Block Diagram for a secure storage and certifcate issuance

- Settlement of the course credits is the first step.
- The education authority's digital signature
- The learning user's digital signature
- Storage of the digital certificate block is the fourth step.

C. Protection against Attacks

Given a sharding-based blockchain protocol, the probability of a successful attack (assumed by an adversary) can be computed as follows:

$$\mathcal{P}'' = \sum_{s=m}^{\mathcal{K}} \frac{\binom{\mathcal{M}}{s}\binom{\mathcal{N}-1}{\mathcal{K}-s}}{\binom{\mathcal{N}-1+\mathcal{M}}{\mathcal{K}}} \left(1 - \frac{[x^m]\,\Psi(x)}{\binom{\mathcal{N}}{m}}\right). \quad (1)$$

The probability of successful attack is given by:

$$\begin{aligned}\mathcal{P}'' &= P(\mathcal{X} = nr)\mathcal{P}' + \cdots + P(\mathcal{X} = \mathcal{K})\mathcal{P}' \\ &= (P(\mathcal{X} = nr) + \cdots + P(\mathcal{X} = \mathcal{K}))\mathcal{P}' \\ &= \sum_{k=nr}^{\mathcal{K}} P(\mathcal{X} \geq k)\mathcal{P}'\end{aligned} \tag{2}$$

Implement a proof-of-work or proof-of-stake system to make it difficult for an attacker to insert erroneous blocks into the chain. To guarantee the accuracy of the information in each block, use cryptographic hash functions. Utilize digital signa-tures to verify the parties to each transaction's identification. To defend against network-based assaults, use network security tools like firewalls and secure sockets layer (SSL).Update the system frequently to include the most recent security measures and fixes.To prevent unwanted access to the system, put user authentication and permission controls in place.To identify and stop unwanted access or system tampering, use intrusion detection and prevention systems.

1) Joint Hypergeometric Distribution Approach: In a more recent work, Hafid et al. proposed a novel methodology-based joint hypergeometric distribution to analyze the security of sharded protocols, which can be summarized in below Now, let Yi be a random variable that computes the number of Sybil

Algorithm 1 Protection Against BlockChain Attacks

1: Implement proof-of-work or proof-of-stake mechanism
2: Use cryptographic hash functions
3: Use digital signatures
4: Implement network security measures
5: Regularly update system
6: Implement user authentication and authorization controls
7: Use intrusion detection and prevention systems

IDs in shard i. Theorem 1 computes the probability that at least one shard fails using HDA Theorem 1: In a sharding- based blockchain protocol, the probability that at least one shard fails using JHDA can be expressed as following:

$$\mathcal{P}' = 1 - P\left(\mathcal{Y}_i \leq nr, i \in \{1, 2, \ldots, \lambda\}\right) \tag{3}$$

where,

$$P\left(\mathcal{Y}_i \leq nr, i \in \{1, 2, \ldots, \lambda\}\right) \tag{4}$$

$$= \sum_{m_1=0}^{nr} \sum_{m_2=0}^{nr} \cdots \sum_{m_\lambda=0}^{nr} \prod_{i=1}^{\lambda} \binom{n}{m_i} / \binom{\mathcal{K}}{\mathcal{M}'} \tag{5}$$

2) Probability of a Successful Attack: In this section, computation of the probability of a successful attack (the failure probability of the entire network); this means that consideration of the probability of selecting Sybil IDs from the ID Pool as well as the probability of at least one shard takeover attack.Given a sharding-based blockchain protocol, the probability of a successful attack (assumed by an adversary) can be computed as follows:

$$\mathcal{P}'' = \sum_{s=m}^{\mathcal{K}} \frac{\binom{\mathcal{M}}{s}\binom{\mathcal{N}-1}{\mathcal{K}-s}}{\binom{\mathcal{N}-1+\mathcal{M}}{\mathcal{K}}} \left(1 - \frac{[x^m]\,\Psi(x)}{\binom{\mathcal{N}}{m}}\right). \tag{6}$$

where,

$$\begin{aligned} \mathcal{P}'' &= P(\mathcal{X} = nr)\mathcal{P}' + \cdots + P(\mathcal{X} = \mathcal{K})\mathcal{P}' \\ &= (P(\mathcal{X} = nr) + \cdots + P(\mathcal{X} = \mathcal{K}))\mathcal{P}' \\ &= \sum_{k=nr}^{\mathcal{K}} P(\mathcal{X} \geq k)\mathcal{P}' \end{aligned} \tag{7}$$

IV. Security Analysis

A. Non-Interactive Zero-Knowledge (NIZK)

A type of cryptographic technique called Non-Interactive Zero-Knowledge (NIZK) is used to confirm the veracity of a statement without disclosing any further information about the statement or the individuals taking part in the proof.A prover (the party making the statement) can demonstrate to a verifier (the party receiving the statement) using an NIZK proof that the statement is true without disclosing any personal information about the prover or the statement. This is accomplished through the use of a number of mathematical protocols and algorithms that enable the prover to validate the truth of the statement without disclosing any extra information.

Assume that the relation R = x, w, where x is a public instance and w is a witness, can be computed. Here, the prover uses x and w to calculate a verifiable evidence. The verifier can check a single evidence upon x after getting it from the prover. A trapdoor information td and two PPT simulators S = (S1, S2) are present in such a way that

$$\begin{aligned}
&\Pr\left[\begin{array}{ll} crs \leftarrow G_{crs}(\lambda) & \\ (x,w) \leftarrow \mathcal{A}_1(crs) & : \\ \pi \leftarrow \mathrm{P}(crs,x,w) & \mathcal{A}_2(crs,x,\pi)=1 \end{array}\right] \\
&-\Pr\left[\begin{array}{ll} (crs,td) \leftarrow S_1(\lambda) & \\ (x,w) \leftarrow \mathcal{A}_1(crs) & : \\ \pi \leftarrow S_2(crs,x,td) & \mathcal{A}_2(crs,x,\pi)=1 \end{array}\right]
\end{aligned} \quad \begin{array}{l} (x,w) \in R \\ \\ \\ \\ \\ = \mathrm{negl}(\lambda \\ (8) \end{array}$$

The completeness follows by single message verification and multiple message verification. The first case is between Gen- Proof and VerifyProof referring a single message/signature pair generation and verification. The second case is that a batch of message/signature pairs can be checked by BVerifyProof simultaneously. The completeness property of the scheme can be proven as follows:

$$\begin{aligned}
R_i =& z_i\left(C_i^{1,j}+P\right)+e_iC_i^{2,j} \\
=& \left(r_i-e_isk_i\right)\left(C_i^{1,j}+P\right)+e_i\left(u_jPK_i+PK_i\right) \\
=& r_iC_i^{1,j}-e_iu_jsk_iP+r_iP-e_isk_iP+ \\
& e_iu_jsk_iP+e_isk_iP \\
=& r_iC_i^{1,j}+r_iP \\
=& R_i
\end{aligned} \tag{9}$$

where,

$$\begin{aligned}
\sum_{i=1}^{n}v_iR_i =& \sum_{i=1}^{n}v_iz_iC_i^{1,j}+\left(\sum_{i=1}^{n}v_iz_i\right)P+\sum_{i=1}^{n}v_ie_iC_i^{2,j} \\
=& \sum_{i=1}^{n}v_ir_iC_i^{1,j}-\left(\sum_{i=1}^{n}v_ie_iu_isk_i\right)P+ \\
& \left(\sum_{i=1}^{n}v_ir_i\right)P-\left(\sum_{i=1}^{n}v_ie_isk_i\right)P+ \\
& \left(\sum_{i=1}^{n}v_ie_iu_isk_i\right)P+\left(\sum_{i=1}^{n}v_ie_isk_i\right)P \\
=& \sum_{i=1}^{n}v_i\left(r_iC_i^{1,j}+r_iP\right) \\
=& \sum_{i=1}^{n}v_iR_i
\end{aligned} \tag{10}$$

B. Quantum Blockchain

A quantum blockchain is a sort of blockchain technol- ogy that makes use of quantum computers to boost the network's security and efficiency.A network of nodes makes up a blockchain, a distributed ledger technology that uses a database of shared transactions to store and manage data.

These transactions are organised into blocks and connected to one another by a chain using cryptography. A list of transactions and a cryptographic hash of the block before it are both included in each block. Because it is challenging to cange a block's contents without leaving a trail, this structuremakes blockchains safe and transparent.

Quantum computers are extremely powerful computers that carry out calculations using quantum-mechanical phenomena like superposition and entanglement. They may be beneficial for things like cryptography and data processing since they have the potential to be much faster and more powerful than conventional computers. Quantum computers are utilised in a quantum blockchain to increase the security and performance protection of the network by supplying more cryptographic protection and speeding up transaction processing. By executing calcula- tions that are impossible for classical computers to complete, quantum computers, for instance, could be used to verify the validity of transactions in a quantum blockchain. Attackers may find it more challenging as a result to breach the network or forge transactions.

The proposed quantum is an open and permissionless blockchain that satisfies the following characteristics. It will gothrough the overall structure of the protocol in the following section.

- Decentralized systems
- A shared common quantum database, a quantum system
- with a distributed ledger
- Each node in the network having quantum capabilities including quantum caching and quantum state preparation.

Most of classical voting schemes are based on public- key cryptographic algorithms as in Table 1, which may be cracked by quantum algorithms. But quantum voting schemes based on the principles of quantum mechanics can resist attacks initiated by quantum computers. Recently,[4] proposed a quantum voting protocol by using two special quantum entangled states, which is fair,private, self-tallying, verifiable, and non-reusable.The first m level and n-particle quantum state is described as:

$$|\delta_n\rangle \equiv \frac{1}{m^{\frac{n-1}{2}}} \sum_{\sum_{k=0}^{n-1} j_k \bmod m=0} |j_0\rangle_C |j_1\rangle_C \cdots |j_{n-1}\rangle_C \quad (11)$$

It can be rewritten as

$$|\delta_n\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |j'\rangle_{\mathcal{F}} |j'\rangle_{\mathcal{F}} \cdots |j'\rangle_{\mathcal{F}} \quad (12)$$

where,

$$|j'\rangle_{\mathcal{F}} = \mathcal{F}|j\rangle_C = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{\frac{2\pi i j k}{m}} |k\rangle_C \quad (13)$$

Quantum algorithms and protocols are used in a quantum blockchain to accomplish consensus, encryption, and verifi- cation. Quantum signatures, for instance, enable the verifica- tion of transactions without disclosing their contents, while quantum key distribution (QKD) enables the secure exchange of cryptographic keys between parties.Quantum blockchains may employ consensus protocols like quantum voting or quantum proof-of-stake, which take advantage of the special characteristics of quantum systems to guarantee the objectivity and fairness of the consensus procedure.The genral outline of using quantum blockchain is:

- The act of initiating a transaction: A user adds a trans- action to a pool of unconfirmed transactions.
- Quantum key generation: To encrypt the transaction, the user generates a quantum key using a quantum method like QKD.
- Transaction broadcast: The network receives the en- crypted transaction for verification.
- Quantum verification: The validity and integrity of the transaction are confirmed using quantum methods, such as quantum signatures.
- Consensus: If the transaction is confirmed, it is added to the quantum blockchain, and a consensus mechanism is employed to make sure that all nodes on the network concur on the ledger's current state, such as quantum voting or quantum proof-of-stake.
- Execution of the transaction: Following the achievement of consensus, the transaction is carried out, and the user'saccount is updated appropriately.

Results

A. Comparative Analysis

Contrary to typical blockchain systems, the proposed method reduces the complexity caused by the large node scale of blockchain networks by complementing public and private blockchains. As a result of the private blockchain's fast speed and cheap cost, every education authority's classroom and online procedure is carried out on its individual local area network (LAN) and associated blockchain platform as in Figure 4,5, allowing real-time e-learning evaluation and storage space savings. This assures assessment effectiveness and dynamism. The public ledger and cryptographic technol- ogy of the blockchain also makes it possible to permanently preserve educational achievements and assure that they are reliable, secure, and cannot be faked, in contrast to traditional e-learning platforms. Centralized databases are the foundation of current systems.

In order to guarantee the dependability and validity of both the credentials, the transparency and openness of the certifica- tion program, and the simplicity and effectiveness of certificate authority verification for business owners and other third parties, certificates are issued and stored using the worldwide network (ECN) as well as the associated public cryptocurrency (EC Public Blockchain) as in Figure 6. The use case that successfully mixes both private and public blockchains encour- ages system structure optimization. Additionally, the smart contracts automatically carry out the production and trading of course credits, and the point accumulation of account Courses Credit Wallet, during the operation of e-learning evaluations.

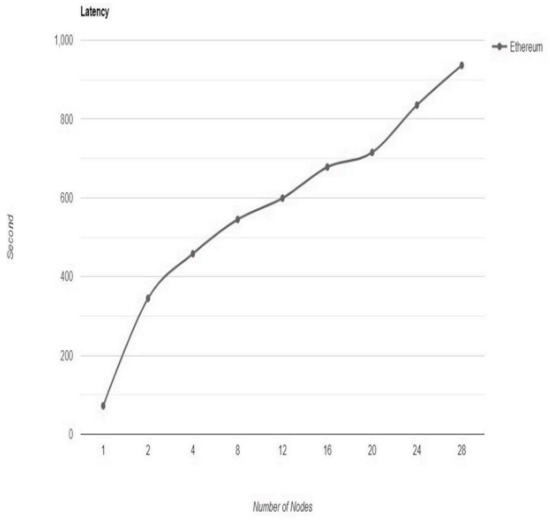

Fig. 4. Latency achieved through ethereum platform for hashing

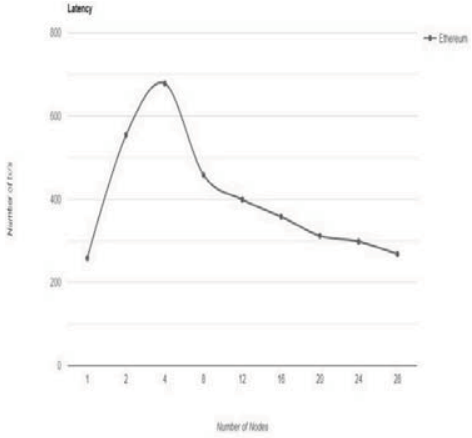

Fig. 5. Latency achieved through ethereum platform for bit wise node growth

VI. Conclusion

The global COVID-19 pandemic has impacted the educa- tional system throughout the world. Due to this latest health catastrophe, billions of students are currently absent from class. The closing of schools has indeed been authorised in more than 100 nations, according to UNESCO. After then,

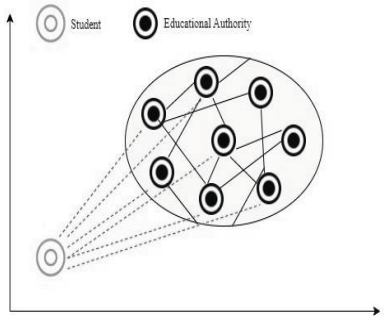

Fig. 6. Visualization of private block

Table I Protection Against Attacks

Technique	Classic Attacks	Quantum Attacks
Liu et al. [6]	No	Yes
Hung N.Q. et al. [11]	No	No
Lakhan et al. [14]	Yes	No
Proposed E-LBC	Yes	Yes

control of the public educational system is transferred to the EL systems, where pupils get interactive online training. However, there are a number of disadvantages to it, including the scarcity of internet-connected devices, particularly in rural regions, the bandwidth problem, connection challenges, etc. To improve the current educational system, two significant issues must be resolved.

Learning providers are unable to select a solution that meets their needs because they are unaware of the options accessible. Additionally, the EL system involves student per- sonal information that needs to be protected from unauthorised access. This paper initially gives a taxonomy of the available remote learning systems in order to solve these problems. The common EL methods are compared in the following section based on crucial requirements imposed by educational systems. the blockchain-based layered architecture, which is promoted as a means to strengthen the security of current EL solutions. The suggested architecture will eventually be put to the test with a real EL system.

References

1. *Hasan, M.K., Akhtaruzzaman, M., Kabir, S.R., Gadekallu, T.R., Islam, S., Magalingam, P., Hassan, R., Alazab, M. and Alazab, M.A., 2022. Evolution of industry and blockchain era: monitoring price hike and corruption using BIoT for smart government and industry 4.0. IEEE Transactions on Industrial Informatics, 18(12), pp.9153-9161.*
2. *Alsamhi, S.H., Shvetsov, A.V., Shvetsova, S.V., Hawbani, A., Guizan, M., Alhartomi, M.A. and Ma, O., 2022. Blockchain-Empowered Secu- rity and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. IEEE Transactions on Green Communications and Net- working.*
3. *Wang, B., Jiawei, S., Wang, W. and Zhao, P., 2022. Image copyright protection based on blockchain and zero-watermark. IEEE Transactions on Network Science and Engineering, 9(4), pp.2188-2199.*
4. *Li, Q., Wu, J., Quan, J., Shi, J. and Zhang, S., 2022. Efficient Quantum Blockchain With a Consensus Mechanism QDPoS. IEEE Transactions on Information Forensics and Security, 17, pp.3264-3276.*
5. *Yang, Z., Salman, T., Jain, R. and Di Pietro, R., 2022. Decentralization Using Quantum Blockchain: A Theoretical Analysis. IEEE Transactions on Quantum Engineering, 3, pp.1-16.*

6. *Liu, J., Zhang, L., Li, C., Bai, J., Lv, H. and Lv, Z., 2022. Blockchain- based secure communication of intelligent transportation digital twins system. IEEE Transactions on Intelligent Transportation Systems, 23(11), pp.22630-22640.*
7. *Yang, T., Cui, Z., Alshehri, A.H., Wang, M., Gao, K. and Yu, K., 2022. Distributed Maritime Transport Communication System With Reliability and Safety Based on Blockchain and Edge Computing. IEEE Transactions on Intelligent Transportation Systems.*
8. *Berg, D.R., Tharunraj, M., Kumar, B.R., Sumalatha, M.R., Palivela, L.H. and Karthikeyaa, P.V.V., 2022, September. WebRTC-based Decentralized Chat Application with Minimal Latency. In 2022 International Confer- ence on Intelligent Innovations in Engineering and Technology (ICIIET) (pp. 210-215). IEEE.*
9. *Ravisankar, S., Mahendran, K., Arulmurugan, S. and Sumalatha, M.R., 2022. Flexible Demand Forecasting in Intelligent Food Supply Chain Management. Available at SSRN 4119151.*
10. *Sumalatha, M.R. and Anbarasi, M., 2019. A Review on Resource Provisioning Algorithms Optimization Techniques in Cloud Computing. International Journal of Electrical and Computer Engineering, 9(1).*
11. *Hung, N.Q., Phung, T.K., Hien, P. and Thanh, D.N.H., 2021. AI and Blockchain: potential and challenge for building a smart E-Learning system in Vietnam. In IOP conference series: Materials Science and Engineering (Vol. 1022, No. 1, p. 012001). IOP Publishing.*
12. *Li, D., Han, D., Zheng, Z., Weng, T.H., Li, H., Liu, H., Castiglione, and Li, K.C., 2022. MOOCsChain: A blockchain-based secure storage and sharing scheme for MOOCs learning. Computer Standards Interfaces, 81, p.103597.*
13. *Wei, D., 2022. Gemiverse: The blockchain-based professional certifi- cation and tourism platform with its own ecosystem in the metaverse. International Journal of Geoheritage and Parks, 10(2), pp.322-336.*
14. *Lakhan, A., Mohammed, M.A., Ibrahim, D.A., Kadry, S. and Abdulka- reem, K.H., 2022. ITS Based on Deep Graph Convolutional Fraud Detection Network Blockchain-Enabled Fog-Cloud. IEEE Transactions on Intelligent Transportation Systems.*
15. *Qureshi, K.N., Jeon, G., Hassan, M.M., Hassan, M.R. and Kaur, K., 2022. Blockchain-based privacy-preserving authentication model intel- ligent transportation systems. IEEE Transactions on Intelligent Trans- portation Systems.*