

A NOVEL BLOCKCHAIN FRAMEWORK FOR DIGITAL LEARNING

J Bheemeswara Sastry¹

Research Scholar, Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation,
Deemed to be University, Hyderabad, Telangana-500075, India.
shastry.06@klh.edu.in

Barnali Gupta Banik²

Associate Professor, Department of Computer Science & Engineering, Koneru Lakshmaiah Education
Foundation, Deemed to be University, Hyderabad, Telangana-500075, India.
barnali.guptabanik@ieee.org

Abstract

Blockchain is a structure of data blocks arranged in sequential order, including reliability, data sharing, decentralization, security and, extensively used in a smart contract, digital currency, credit encryption, and other fields. Currently, there is a rapid increase in blockchain technology applications, offering opportunities to deal with the limitation in the online education field, e.g., the shortage of a unified e-learning assessment standard, the complication of e-learning assessment, and the concern of digital education certificates. In this paper, a secured blockchain system proposes building an adaptable and safe data delivery facility that interacts with current educational data. The proposed framework improves data security and eliminates trust concerns among users and, between other institutions accessing services and applications.

Keywords: Blockchain, E-Learning, Framework, Online Education, Privacy, Security, Trust.

1. Introduction

Blockchain is the vital technology that generates Bitcoin and cryptocurrency by endorsing the absolute distributed ledgers in several nodes suggested by Satoshi Nakamoto in 2008. Blockchain is considering a part of the fourth industrial revolution since discovering electricity, the steam engine, and information technology [1-3]. In the 21st century, this technology offers a meaningful impact on institutional functions, national governance, education, business operations, and our daily lives [4]. On a global scale, this blockchain technology promotes the progress of the knowledge-based economy quickly, and it is estimated to transform the functioning means of education, business, and commerce. This advanced technology has many potential applications owing to its transparency, immutability, and reliability for all the communications accomplished in a blockchain network [5, 6]. In several fields, this blockchain technology has been applied presently, i.e., as cryptocurrencies in the commercial field, including Ethereum, Zcash (Zerocash), Bitcoin. Bitcoin is the first peer-to-peer payment network in this technology, electronic cash. In a distributed blockchain network, the vital task is to maintain consensus [7-10]. The hash-based Proof-of-Work (PoW) distributed the Bitcoin blockchain network adopts a consensus algorithm. Ethereum is a blockchain-based, public, and open-source distributed computing platform using a Proof-of-Stake (PoS) consensus algorithm including smart contract functionality.

Similar to Bitcoin, Zcash is an open-source, decentralized cryptocurrency. The consensus algorithm utilizes the Proof-of- Zero-Knowledge (PoZK) and suggests a selective and privacy scheme of transactions [11]. On a public blockchain, the Zcash payments publishing, but the recipient, sender, and the transaction volume remain private. Some enterprises and organizations plan to improve the distributed platforms based on blockchain technology [12-15].

Smart contracts and blockchain technologies provide trust worthy processes and ownership which benefit developing countries or markets. E-learning could transform into more mutual recognition's and trustworthy education credentials, including a globalized and border-less higher education sector [16-18]. According to the previously stated principle, blockchain recent applications are still in the 1.0 and 2.0 stages. As per researchers, blockchain belongs to a business related area and discussed applying this technology in education, mainly focusing on several studies [19, 20].

In this paper, the main contribution is developing a secured blockchain-based framework that any educational institution can employ to improve security and privacy and eliminate the trust concerns among users and between

other institutions accessing applications and services. Based on the institution's information security policies, blockchain implements on different learning platforms. The existing network nodes use to study the distributed e-learning framework, and the blockchain ID initializes the fresh users. Every fresh user is registering by the network node, which issues an address wallet and ID.

2. Blockchain Technology

Blockchain is a Peer-to-Peer, decentralized, distributed ledger that records transactions efficiently, and in a verifiable and robust fashion. Blockchain is a transaction where we store the database records that is distributed, validated and maintained around the world by a network of computers. Blockchain Technology is a new generation and innovative internet that is absolute, transparent, dispersed, auditable, determined, and secured. Multiple parties share using this technology in the distributed database, and it is trustable. Each party shares a personal copy of the database in the network transactions. This technology is tamper-proof and has automatic trust with transparent and resilient features.

2.1 Blockchain Overview

Blockchain is a chain of data blocks. Each block can be a page in a shared ledger. The individual blocks are composed of several components roughly these can be differentiated into block header and its block body. Block header is divided into six components as shown in Fig. 1. like version number of the block, the Merkle tree root hash, the previous block hash, nBits, Nounce and Timestamp. The version number of block does not matter in most cases however a miner with a particular version number can signal which protocol decisions mainly supports. The hash of previous block is the chain of blockchain because the hash of the previous block is contained in the hash of the new block. The blocks of the blockchain all build on each other without this component there would be no connection.

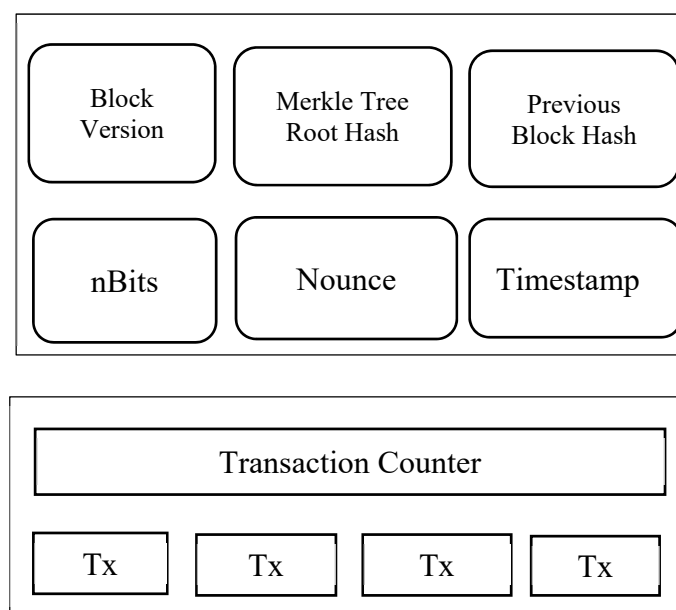


Fig. 1. Block Overview

The Merkle tree root hash encodes the blockchain data in an efficient and secure manner. It enables the quick verification of blockchain data as well as quick movement of large amount of data from one computer node to the other in a peer-to-peer blockchain network. The data itself is first hashed then hashes are hashed again and merged. Finally, the Merkle tree is merged into single hash is called as root hash. It represents all the information of its leafs that is the individual transactions and branches which represents the hashes of the leafs in a relatively short stream. Each transaction occurring on the blockchain network has a hash associated with it however these hashes are not stored in a sequential order on the block rather in the form of tree like structure such that each hash is linked to its parent following a parent-child tree like relation. nBits is the encoded form of block header. Nounce is the variable incremented by the Proof-of-Work in this way a miner guesses a valid hash. Each block contains a unique timestamp in addition to serving as a source of variation for the block hash and, also make it more difficult

for an adversary to manipulate the blockchain. A Timestamp is accepted as valid if it is greater than the median of timestamp of previous of eleven blocks or the network adjusted time means the median of timestamps returned by all nodes connected to the blockchain.

2.2 Types of Blockchain

Blockchain Technology is classified into mainly three categories mentioned in Table. 1. as Public blockchain, Private blockchain and Federated blockchain.

TABLE 1. SUMMARY OF DIFFERENT TYPES OF BLOCKCHAIN

Types of blockchain	Public	Private	Federated/ Consortium
Access	Anyone	Single Organization	Multiple Selected Organizations
Participants	Permissionless and Anonymous	Permissioned and Known Identities	Permissioned and Known Identities
Security	Consensus Proof-of-Work Proof-of-Stake	Pre-approved Participants Voting-Bases Consensus	Pre-approved Participants Voting-Bases Consensus
Transaction Speed	Slow	Lighter and Faster	Lighter and Faster

A Public blockchain is the standard blockchain Network that is open to all and there is no centralized management. Here anyone can access the network and participate in reading, writing and audit the blockchain. It is a fully decentralized permissionless and open source system means anyone create, validate and view transactions at a given point of time. To validate transactions decision making happen by consensus algorithms like Proof-of-Work or Proof-of-Stake. Bitcoin and Ethereum are the well-known examples of a Public blockchain.

A Private blockchain is a type of blockchain where an incharge of the network can read, write and audit the blockchain. The central incharge can also provide permissioned access to selected nodes to make validate and view transactions at specified point of time only. As it is an essential Private consensus is a achieved at the discretion of the central incharge go through a voting and multi party consensus algorithm. Hyperledger Fabric is the well-known example of a Private blockchain.

A Consortium or Federated blockchain is a group owned system and Permissioned blockchain where an autonomy is removed. In this type of blockchain, there is more than one central incharge who will provide access to pre-selected nodes to read, write and audit the blockchain. Consensus is achieved by members of the consortium through a voting and multi party consensus algorithm based on the agreement of the participants. R3's and Corda blockchain are the well-known examples of a Consortium or Federated blockchain.

3. Literature Review

Satoshi Nakamoto proposed the blockchain in his paper and named it Bitcoin, which considers as a Peer-to-Peer electronic cash system, in 2008. The Bitcoin social network was found in 2009 by Nakamoto and established the Genesis block, which was its first block. Blockchain holds a broad list of transaction records with a consecutive sequence of blocks. Each blockchain's block contains typical contents: previous blocks, Cryptographic hash values, transaction data, and timestamps. Cryptographic algorithms secure all the blocks from being tampered with or falsified.

The primary technical principles and the application features of blockchain technology have been presented by Sun et al. [21]. The main aim of this study was to provide a solution to the online education problems. In a trusted distributed manner, blockchain technology can store learning records, realize smart contract based learning resource sharing, offer credible digital certificates, and utilize data encryption to protect intellectual property. This study presents that the development of online education is possible by incorporating blockchain technology.

The Deepcoin based novel deep learning and the blockchain based energy framework were proposed by Ferrag and Maglaras [22] for Smart Grids. There are five phases in this system, i.e., agreement phase, setup phase, consensus building phase, developing a block phase, and view change phase. The Byzantine fault tolerance

algorithm employed in this study and achieves high throughput. Hash functions and Short signatures are employed in this study to prevent smart grid attacks.

A Digital Twin Wireless Networks (DTWN) present by Yunlong Lu et al. [23] for migrating real-time data processing and computation. For collaborative computing, this study presents a DTWN based federated learning framework that enhances data privacy and develops reliability and security. An optimization problem is framing to equalize the time cost and the learning accuracy of the proposed approach. To attain the optimal solution a multi-agent reinforcement learning is employed. The experimental outcomes revealed the efficiency of the proposed approach compared to the standard learning method.

A secure computing framework was presented by Zhou et al. [24] based on a novel approach named PIRATE. A case study validates the contribution of the proposed approach to the distributed learning. The zantiner salient learning framework envisages some challenges and open issues of numerous devices enabled by the 5G technologies to participate in distributed-learning tasks with ample network bandwidth.

Chen et al. [25] presented the consensus algorithms and cryptography techniques to create features, for instance, decentralization, immutability, traceability, and currency properties. Students are encouraged by blockchain technology as a motivation for learning. Additionally, it stores a set of records comprised of educational actions and results in learning environments that are formal and informal. Besides, the faculty's teaching behaviors and the performance records offer a reference suggestion for teaching evaluation. Blockchain has great potential applications for learners and teachers in instructional design, evaluation, behavior recording, and analysis.

4. Proposed Model

Blockchain enabled framework presents in this section will address the security issue and better understand the E- Learning system designer in aids for the development of secure E-Learning platforms. Because of plenty of users involved in E-Learning, the only solution is the cloud, where E-Learning providers can host their software shown in the Fig. 2. depicts the proposed blockchain based E-Learning framework.

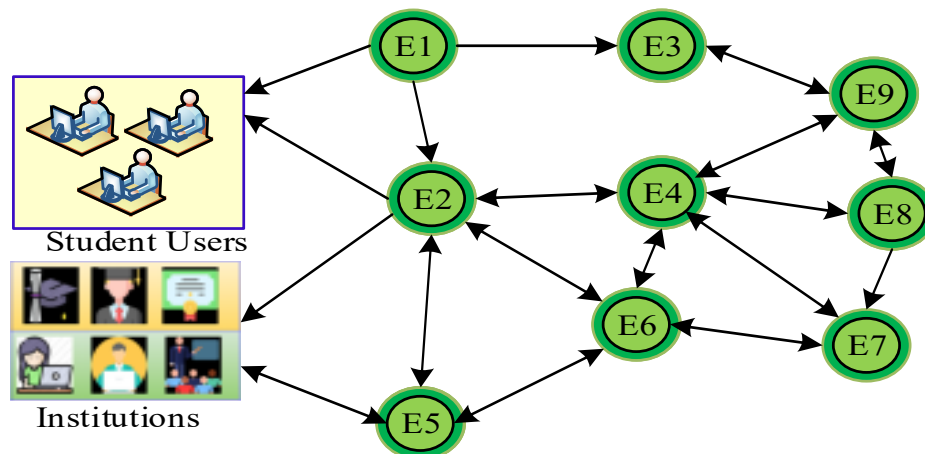


Fig. 2. Blockchain based E-Learning Framework

The cloud is suggesting the rapid and continuous availability of data to its users for hosting E-Learning software. Data tracking is complicated than storing it on a local server since the cloud has its security mechanisms. The E-Learning node is denoted as "E" with its unique node number. Data communication representing as the duple route arrow. In a distributed transmission, the communication takes place amongst the institutions and students. The students access the authentication of data. The duple route arrow represents a learning platform model, and without loss, the data accessing by the users. The network operator authenticates the connection of any new E-Learning (E) node.

Moreover, for arranging a private blockchain service, the E-Learning proofs are rewarded. The total number of records stored by a node in the blockchain network is proportional to the number of E-Learning proof's. The transactions are approved by the entire E-Learning user's node when setting up a node that needs at least 50% consensus. The data security improving by the private blockchain system and eliminates the trust issues of the user. In the literature, the reviews on security are not focusing on other themes. Though, a conclusion attaining in which poor security is provided by the solutions addressing all the five themes discussed in the research. The

solution cases review finds that the credential is open to liability and data security is inadequate. The in the existing solutions for the certificate verification, the gaps found are authentication, confidentiality, authorization, ownership, and privacy.

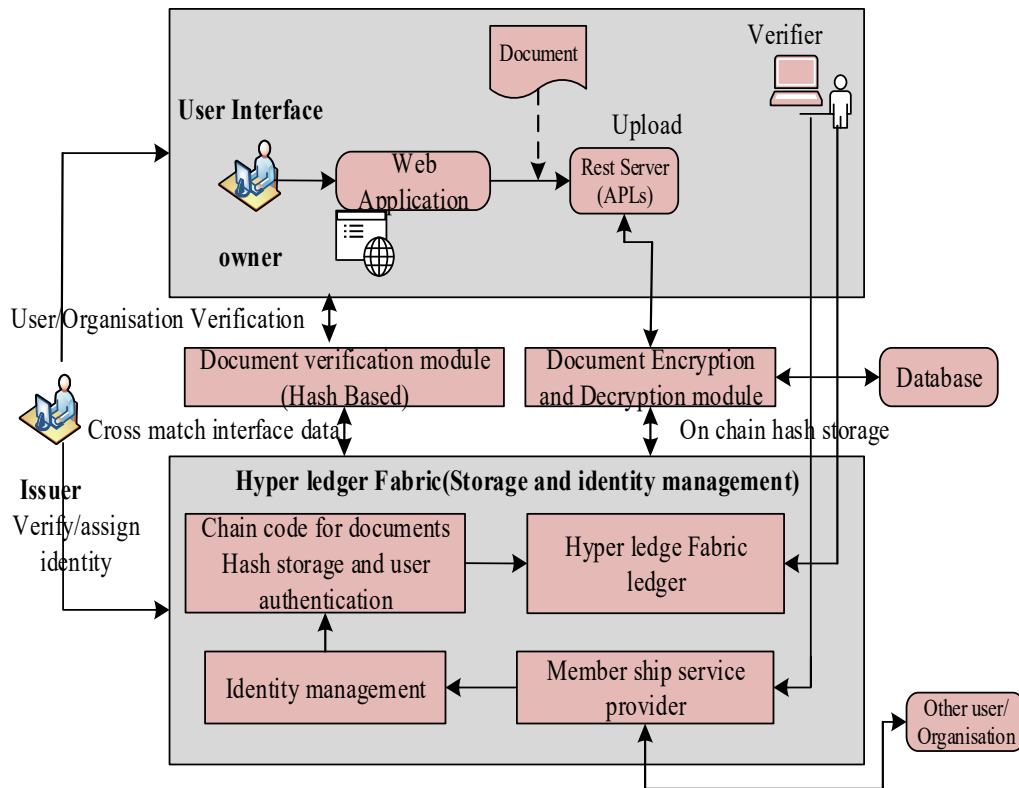


Fig. 3. Blockchain based Hyper Ledger Fabric Framework

Blockchain based framework proposes to verify academic certificates aiming at authentication, confidentiality, authorization, privacy, and ownership themes shown in Fig. 3. depicts the Hyperledger Fabric framework.

4.1 Fresh Node Creation

Full and lightweight nodes are available in the blockchain network models. Full nodes have access to complete copies of the blockchain and fully permit the network nodes to authenticate transactions and blocks. The light nodes do not have access to the complete copies except the genesis blocks to authenticate the transactions. A full network node can be linked using the E-learning institutions' whereas the students can link to light nodes.

An ID wallet address is created by an efficient node when a new node links the network. After creating the address, an efficient node communicates to the representative authenticating the new registration and allotting some E-Learning proof's in its wallet address. Then the registration of the new node is completed, and the representative announces to the entire network. For setting up a network node, information collects by the new node.

In the subsequent rotation, to authenticate the transactions afresh, the node can be selected as a representative when a network node is set up well and proclaimed by the efficient representative, only adding a new node accomplishes. The encrypted records enhance the data security through spread through the network. Once a traitor node is observed or recorded as an institution node, the data will not change because of the process completely contains undeniable features.

4.2 Operator Registration

To access the E-Learning portals, the users or operators must register using their network devices. An ID will be assigned to the operator and using the public and private keys. A new blockchain address creates as proof of the identity of the owner. The fresh user's blockchain wallet generates, and the node ID address save.

For confirmation, this ID address wallet will be communicated to the user's and used for transactions as its account when a student's data is to be accessed by a third-party institution. Initially, the ID address must be

checked and validated. The institution uses the block web API, and the backup ID keys should be compulsory for every single E-Learning operator to confirm the student's ID address.

A new ID address will create when operators lose their ID keys. The E-Learning user nodes send the transfer data to the freshly created ID address from the old ID address. When the registered operators need to access the network, the user's device and identity will be authenticated and confirmed. The access characterized by E-Learning systems, including weak links and human errors in data storage, will be reduced intensely.

4.3 Fresh Block Creation

One efficient representative creates a new block that is chosen randomly by the efficient members. Another member is to create when a member misses a block, and the block is authenticating to join the blockchain network. It takes five seconds in the Proof-of-stake(PoS). A representative nominates for the blockchain until the representative stops accepting new transactions from the block.

The process will continue to authenticate and generate the transactions. Finally, the new block will be collected by the representative and allocated to the network members for authentication and assessment. The block which is confirmed is reverted to the members then merged to the local blockchain. Although, allocation of the new block in the network is doing by the blockchain. Lastly, the nodes of the E-Learning institution allocate in the network.

5. Application and Future Aspects

Blockchain technology can be used in education apart from achievements assessment and diploma management in many advanced ways. This technology has a boundless ability for extensive application prospects on implementation and learning activities design, creative evaluation, and pursuing the entire learning processes for both teachers and learners. In the field of education, some advanced blockchain technology based applications suggest below. A Smart Contract is fundamentally a computer protocol that functions on Ethereum, a blockchain network that produces a real contract like economic contacts, employment. It can shorten contract terms and negotiation, authenticate the contract's execution state, and implement its execution.

Using the digital way, it grades distinctively, identifies the parties in a transaction precisely, and specifies the obligations and rights mutually by code. The smart contract assures transaction reliability and security, minimizing the third party expenses in traditional dealings. However, some adverse particular or objective factors are present in student's perception, triggering reduced learning results, for example, the lack of financial pressure and motivation. By implementing "Learning is Earning", the students motivate by blockchain.

The smart contract among teachers and students in the educational setup can be applied. The instructors using some simple clicks, can offer Real-time awards to students. According to the smart contract, some digital currencies obtain by the students as rewards. In the education wallet, this kind of money can be stored and used as tuition or even swapped with real currencies. In the education system, evaluation is also a challenging issue. For a long time, creative assessment has been encouraged. Still, every detail of learning and teaching is not easy to track.

Blockchain and smart contracts apply for traceability, reliability, and immutability, signifying that the data recorded on the blockchain is exceptionally reliable, explicit, and anti-theft to deal with this challenge. For example, in "Collaborative Learning", the student's ability to work with others gets improved. The instruction is artistic and sophisticated from the teacher's viewpoint so that it is tough to evaluate.

Based on the student's feedback, the traditional method is partial, in need of subjectivity, and does not support the teacher's improvement. A new valuation system can be constructed based on the smart contract and blockchain network, and pre-planned instructional activities should be submitted to the school's by the teacher as a smart contract. The entire teaching actions record during the teaching process in the blockchain network. The practice and teaching design's reliability will be verified using the smart contract, which plays a vital indicator for instruction evaluations. As a reward, digital currency obtains by the teacher's who meet the standards.

The student's program supervision is conducted on behalf of an academic advisor or a supervisor can help the student schedule the study program and information on the research activities progress. Though these issues check and manage, it will be unsettled to discriminate the responsibilities if something adverse happens in the future. The information asymmetry issues can be solved theoretically by blockchain as of its delegation and immutability. It confirms the legitimacy since the data and value are published and are mutually maintained. It offers a reliable way for talent investment and the user's appreciation and investment gain with more knowledge on digital currencies. In contrast, the blockchain ledger can be an option for a user who wants a vivid employee. The investment bias risk and failure significantly decrease. Generally, the interests of both parties maximize by blockchain.

6. Conclusion

The educational system's needs with huge openness, an online, secure database can be provided by blockchain technology. Educational institutions should deploy this new innovative generation of internet technology. This study focuses on the framework and academic discussion level. In the future, this framework implements additionally explored its ability on an effective E-Learning platform like distance learning the E-Learning systems, mobile learning, classroom learning, online learning, and blended learning platforms. In E-Learning, an appropriate version of blockchain technology should be essential to deal with the structural issues because still, blockchain technology is in its developing stage. For easy communication, blockchain integrates with the voice platform through the voice user interface. An analysis of the concerns in healthcare might also be a part of future research.

References

- [1] Sun, Han, Xiaoyue Wang, and Xinge Wang. "Application of blockchain technology in online education." *International Journal of Emerging Technologies in Learning (IJET)* 13, no. 10 (2018): 252-259.
- [2] Alammary, A., Alhazmi, S., Almasri, M. and Gillani, S., 2019. blockchain-based applications in education: A systematic review. *Applied Sciences*, 9(12), p.2400.
- [3] Rivera-Vargas, Pablo, and Carles Lind'in Soriano. "blockchain in the university: a digital technology to design, implement and manage global learning itineraries." *Digital Education Review* 35 (2019): 130-150.
- [4] Lam, Tsz Yiu, and Brijesh Dongol. "A blockchain-enabled e-learning platform." *Interactive Learning Environments* (2020): 1-23.
- [5] Ubaka-Okoye, Millicent N., Ambrose A. Azeta, Aderonke A. Oni, Hilary I. Okagbue, Olanike S. Nicholas-Omoregbe, and Felix Chidozie. "blockchain Framework for Securing E-Learning System." *institutions* 27: 28.
- [6] Chentharu, Shekha, Khandakar Ahmed, Hua Wang, Frank Whittaker, and Zhenxiang Chen. "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology." *Plos One* 15, no. 12 (2020): e0243043.
- [7] Awaji, Bakri, Ellis Solaiman, and Adel Albshri. "blockchain-Based Applications in Higher Education: A Systematic Mapping Study." In *Proceedings of the 5th International Conference on Information and Education Innovations*, pp. 96-104. 2020.
- [8] Zhao, Gang, Bingbing Di, Hui He, and Wenjuan Zhu. "Digital education transaction object authentication service based on blockchain technology." *Internet Technology Letters* 3, no. 2 (2020): e149.
- [9] Nyangaresi, Vincent Omollo, and Slivance Abeka. "blockchain Enabled E-Learning Delivery Model for Enhanced Quality Learning." (2019).
- [10] Bhaskar, Preeti, Chandan Kumar Tiwari, and Amit Joshi. "blockchain in education management: present and future applications." *Interactive Technology and Smart Education* (2020).
- [11] Jirgensons, Merija, and Jānis Kapenieks. "blockchain and the future of digital learning credential assessment and management." *Journal of Teacher Education for Sustainability* 20, no. 1 (2018): 145-156.
- [12] Chen, Guang, Bing Xu, Manli Lu, and Nian-Shing Chen. "Exploring blockchain technology and its potential applications for education." *Smart Learning Environments* 5, no. 1 (2018): 1.
- [13] Ma, Sihua. "Using blockchain to build decentralized access control in a peer-to-peer e-learning platform." Ph.D. diss., University of Saskatchewan, 2018.
- [14] Shuaib, Mohammed, Salwani Mohd Daud, Shadab Alam, and Wazir Zada Khan. "blockchain-based framework for secure and reliable land registry system." *Telkomnika* 18, no. 5 (2020): 2560-2571.
- [15] Ferrag, Mohamed Amine, Makhlof Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. "blockchain technologies for the internet of things: Research issues and challenges." *IEEE Internet of Things Journal* 6, no. 2 (2018): 2188-2204.
- [16] Rojas, Wilson, Víctor Gayoso Martínez, and Araceli Queiruga-Dios. "blockchain in Education: New Challenges." In *Conference on Complex, Intelligent, and Software Intensive Systems*, pp. 380-389. Springer, Cham, 2020.
- [17] Bartolomé, Antonio R. "blockchain in educational methodologies." In *Radical Solutions and eLearning*, pp. 63-79. Springer, Singapore, 2020.
- [18] Sharma, Shallu, and Ranbir Singh Batth. "blockchain Technology for Higher Education System: A Mirror Review." In *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 348-353. IEEE, 2020.
- [19] Zhou, Liming, Ran Lu, and Juan Wang. "Development Status, Trends and Challenges in the Field of "blockchain and Education." In *Journal of Physics: Conference Series*, vol. 1621, no. 1, p. 012112. IOP Publishing, 2020.
- [20] Miah, Muhammed. "blockchain Technology in Peer-to-Peer eLearning: Opportunities and Challenges." In *Proceedings of the EDSIG Conference* ISSN, vol. 2473, p. 4901. 2020.
- [21] Sun, H., Wang, X. and Wang, X., 2018. Application of blockchain technology in online education. *International Journal of Emerging Technologies in Learning (IJET)*, 13(10), pp.252-259.
- [22] Ferrag, M.A. and Maglaras, L., 2019. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Transactions on Engineering Management*.
- [23] Lu, Y., Huang, X., Zhang, K., Maharjan, S. and Zhang, Y., 2020. Low-latency Federated Learning and blockchain for Edge Association in Digital Twin empowered 6G Networks. *IEEE Transactions on Industrial Informatics*.
- [24] Zhou, S., Huang, H., Chen, W., Zhou, P., Zheng, Z., and Guo, S., 2020. Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks. *IEEE Network*.
- [25] Chen, Guang, Xu, Bing Lu, Manli Chen, NianShing. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*. 5. 10.1186/s40561-017-0050-x.