International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 02 | Feb - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

A Blockchain Application for Authenticating Certificates

SAYED MAJID ALI
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India.
sayedmajidalicse@gmail.com

RHUJITHO KAJIRI
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India.
ruru12kajiri@gmail.com

NEITHONGULIE YASHU
Department of Computer Science and Engineering,
Dr.M.G.Reducational and Research Institute, Chennai, India.
neithongulieyash@gmail.com

S.DIVYA
Assistant Professor
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India.
divya.cse@drmgrdu.ac.in

Dr.M.NISHA
Assistant Professor
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India.
nisha.cse@drmgrdu.ac.in

Dr.M.SUJITHA
Assistant Professor
Department of Computer Science and Engineering,
Dr.M.G.R Educational and Research Institute, Chennai, India.
sujitha.ece@drmgrdu.ac.in

Abstract - The present processes frequently experience inefficiencies and fraud susceptibility in a society where educational credentials are crucial. This study explores the idea of using blockchain as a decentralized,secure database for storing and verifying academic credentials. The study addresses how blockchain technology can provide a tamper-proof, transparent, and effective means for certifying educational credentials by using its immutability and consensus mechanisms. The study explores how blockchain implementation may affect students, educational institutions, and employers, stressing the potential for streamlined verification procedures, cost savings, and improved overall academic record integrity. This article clarifies the tremendous prospects of blockchain in altering the certificate authentication environment through a thorough examination. This problem is solved using blockchain technology. Changes made to blockchain data must be approved unanimously by all parties responsible for maintaining the records. This makes the system encrypted and non-transparent, improving data integrity.

Keywords— Blockchain, Certificate validation, Fake certificates, Metamask.

II. INTRODUCTION

Currently, each institution has its own method for publishing and storing academic data that is essentially independent of other organizations' record-keeping procedures. This problem directly affects how academic accomplishment data are evaluated. This is because, in some cases, the human confirmation of transcript and documents may prove rather time-consuming and expensive. The blockchain age has created potential for the implementation of novel business models in sizable, established sectors. The damage caused by blockchain technology for educational institutions represents one of among the most difficult sectors.,and its effects are generally distributed over the long term and into the future. The following conditions make it easier to produce phony diplomas from five v arious sources inorder to prove one's knowledge and talents in a society where competition is growing. (1) "Degree-holder" who prepare false witness statements and sell them to consumers [1]. (2) Fake entries for insufficient educational institutions [2]. (3) Records that have been manipulated by inserting bogus dates, instruction, disciplines, and so on into authentic records.(4)"In-house"documents are copies of a cademic transcripts that are protected,publicized,and generated by respected organizations but were really made by unapproved collaborators.[4].This technology eliminates fake credentials and establishes a verified, trusted system.

In our increasingly interconnected world, the proliferation of false academic qualifications and certificates represents a serious problem that has to be addressed and eliminated. There aren't any centralized databases or acknowledged guidelines for presenting scholarly data, nevertheless. Furthermore, it is challenging to evaluate how people in other nations get their degrees without a worldwide platform for openly accessible academic material.

Academic resources can be tamper-proof registered, allowing for simple external verification. Reliable blockchain-based solutions may be the solution to these issues. It requires being adaptive as well as effective in maintaining all important academic information while maintaining the confidentiality of any private information, along with comply with every major regulatory standards. In various industrial industries, as a test tool. Blockchain provides a fast and reliable solution to transparently, reliably and cost-effectively verify real-world documents such as:-school performance. To get the most out of your real estate business model in this context, you need to embrace the most user-friendly, adaptable, and cost- effective technology. Blockchain technology can reduce the risk of certificate fraud while

ensuring the safety, validity, and confidentiality of transactions. Non- repudiation, uniqueness, and confidentiality of electronic information can be achieved through the use of related domain name technologies such as digital signatures. However, e-qualification certificates must have a certain set of major security and functional flaws.

For instance, this value is used to authenticate report updates, but does not initiate authenticity verification ofall public certificates. If keys are compromised, frequent counterfeiting may result.

The innovative "Certificate Authentication System using Blockchain" project aims to fundamentally alter how we authenticate digital certificates across a range of industries, including education, professional credentials.

Transactions are used to stored the information. Bitcoin tracks transactions on blockchain blocks, including who received the money and when it was delivered. Transactions include the timestamp, transaction amount, recipient's address, and the sender's address. Two distinct ransactions took place. Anybody with a copy of the decentralized ledger may view the on-chain transactions since they are preserved there.Everyon- chain transaction updates the blockchain network. Externally records allows for enhanced preservation of systems of various sorts and stages by lowering the quantity of space needed for every blockchain cluster in the network while minimizing blockchain bandwidth. The "TRIE DATA STRUCTURE" is used in cryptocurrency to store information.
Reliability is key. Once data is stored in the blockchain, it can't be modified or changed. Majority techniques are useful to add information, execute multiple transactions, or aggregate nodes. Consensus algorithms are classified into two types: proof-of-workand proof-of stake. The majority method allows all nodes to agree on placing a new block on the blockchain.

EXISTING SYSTEM: Current systems are inaccurate, inefficient in terms of load and implementation times, and do not run in real-time. Current approaches only check a small portion of the certificate content and aren't able to identify similarity across documents. The preciseness of flaws in current approaches merely endanger the dependability of authentication certificates yet also offer significant security threats by omitting vital anomalies. Conventional systems' slowness to cope with diverse workloads and executing patches on time limits their capacity to adapt to fluid safety standards, reducing entire system efficiency.

III.LITERATURE SURVEY

To solve the problem of certificate forgery,blockchain-enabled digital certificate systems arebeing created. The immutability of blockchain enables the creation of verifiable and tamper-proof digital certificates. In the following methods, an digital certificate is created in the manner described below. The connected alternative connectivity information of the paper certificate is first transformed into a digital document, with the digital record's hash value being established. Atlast, a hash keys are kept on chainsystem withinblock.The software will generate a QR code, with a string query's key for certificates that are tied to paper certificates. A online search or a phone scan can yield the information needed to verify the validity of a physical certificate. This action increases the credibility of numerous written information and makes digital certificates less likely to be lost as blockchain is an irreversible technology[1].
Blockchain, commonly referred to as the chain of blocks, is a distributed ledger system that can maintain Certain transactions and procedures cannot be carried out with out the assistance of reputable third-party applications. One important component of blockchain technology is its lack of centralization. The popularity of blockchain has increased since the Bitcoin explosion. Key features of blockchain technology have been sought to be utilized in a number of applications and use cases. This document describes how blockchain technology is being used and some of the ways it is being used to safeguard and demonstrate the reliability of intelligent systems. In particular, anyone who reads this whitepaper will gain a deep understanding of the uses and software of blockchain technology.[2].

Blockchain software had lately grown in popularity due to his decentralized, a peer-to decentralized network, with privacy properties. Technical difficulties and control worries are hidden by blockchain technology. A smart contract is part of the computer programs that is executed, verified, and cannot

be broken. Smart contracts may be traded in real time using blockchain technology, which is cheaper and more secure. This article initially outlines the various components and features of smart contracts. [3].

While widely acknowledged, little is known about the long-term applications of blockchain technology at this point. Blockchain technology improves privacy protection in a number of ways. Nevertheless, the device has a number of design flaws that lead to further issues . The paper investigates the most prevalent blockchain security software, their primary issues, and supplementary blockchain roadblocks that may help future research be more productive [4].

The optimal configuration, durability, and strategy for this open-source project should be simulated using Block SIM, which thoroughly mimics the blockchain system. Blockchain developers are better able to predict how their blockchain network will behave in the future by selecting the simplest or most advantageous system settings that are still functioning during simulations. Blockchain system architects must take into account

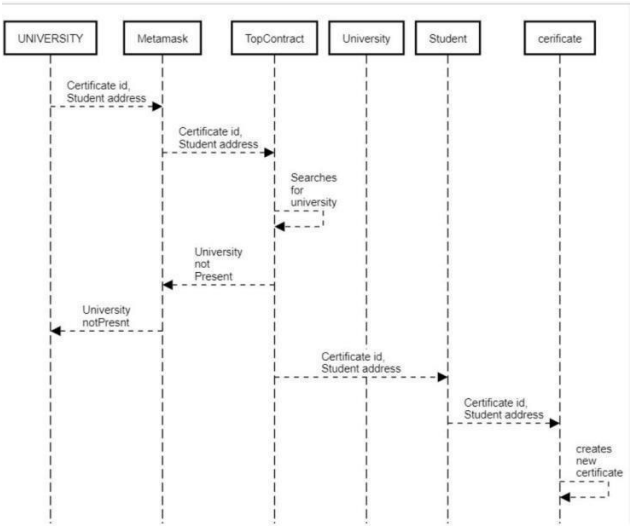
parallels and Simulation findings vs a $64,000 blockchain network in order to guarantee the construction and implementation of a scalable, extensible, reliable and robust blockchain network. Diagrams that depict how actual blockchain systems

may be designed and built using Block SIM are also offered [5].

The technology presented in this article is based on the Ethereum principle that software systems should only exist in the layers in which they are used; however, extending a idea byincluding the relevant section in a newtransaction. This gets rid of the necessity to transmit the blockchain in its entirety initially and enables different participants tosee incoming transactions. These concepts will lead to the development of scalable blockchain technology for use-cases that don't necessarily need for unending or comprehensive origins of the group actions [6].

During this work, used as a platform for blockchain technology to choose, verify, and manage an authoritative knowledge base during this work. An immutable knowledge path is efficiently recorded in the constructed system using smart contracts and an open cradle concept. Study demonstrates that, assuming most participants are telling the truth, recommended approach efficiently and safely draws, validates, or validates basic knowledge while guarding

toward mistakenly harmful modifications to the



information obtained. Demonstrates. Because of this, it might be easier to audit and assess the integrity and history of the knowledge cradle over time [7].

The system should only exist at the level currently in use, but adding appropriate sections for new transactions expands the idea. It avoids having to the first broadcast full network, allowing many participants to access incoming transactions. Considering those concepts, resilient blockchain technology becomes accessible to applications which may not necessarily demand an endless and detailed record of teamwork.[8].

It utilize blockchain as an interface to create, verify, and manage trustworthy information base for this activity.

System built uses smart contracts and open cradle ideas to effectively record immutable knowledge journeys. If most of those involved are truthful, this research demonstrates that the suggested system can successfully and Carefully gather, verify, and authenticate cradle knowledge while protecting against harmful changes tothe acquired information[9].

IV. Proposed System

Certificates are issued and academic data is managed. This application was further developed To offer a case study for the proposed procedure. Under this scenario, an educational institution provides a diploma, degree, or certificate and maintains its contents on a blockchain to ensure that anauthorized third partycanrecover or verify the data. Performance criteria are being monitored . Results may be turned towards competence assessments provided by universities and certified by approved outside organizations. As a result, awards and degrees aren't the sole option to demonstrate a student's skill. Loan Monitoring: This approach may be used to monitor course credits obtained by learners.. This form of academic data is created by educational institutions using a specified paradigm.

PFS is a system for collecting and delivering information to decentralized network for example, blockchain. This project uses IPFS to save awards. If you push the same certificate to IPFS, you will get the same hash result.

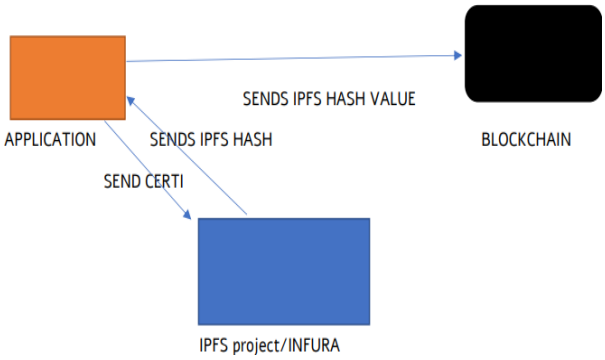


Figure.1 IPFS services

To connect IPFS, the INFURA framework createsan IPFS project and assigns a Project Number and Confidential Identity.

Figure.2 Add Certification

Figure.2 The institution uses the student's MetaMask wallet address to generate unique certificate IDs that are distributed to college students. The parametersused to distribute this certificate to the network include Merkle hash, IPFS value, and access method, and certificate identifier.

Every node maintains data around the technology that acts as each clients and servers. If certain data stored in repository, this database are available in each node like peer-to-peer chain. If the trade has to be done,and then it

has to be changed across every node. All block differs from block chain to blockchain. Each block contains the version number for the block, the hash value of the previous block, transactions, along with time.

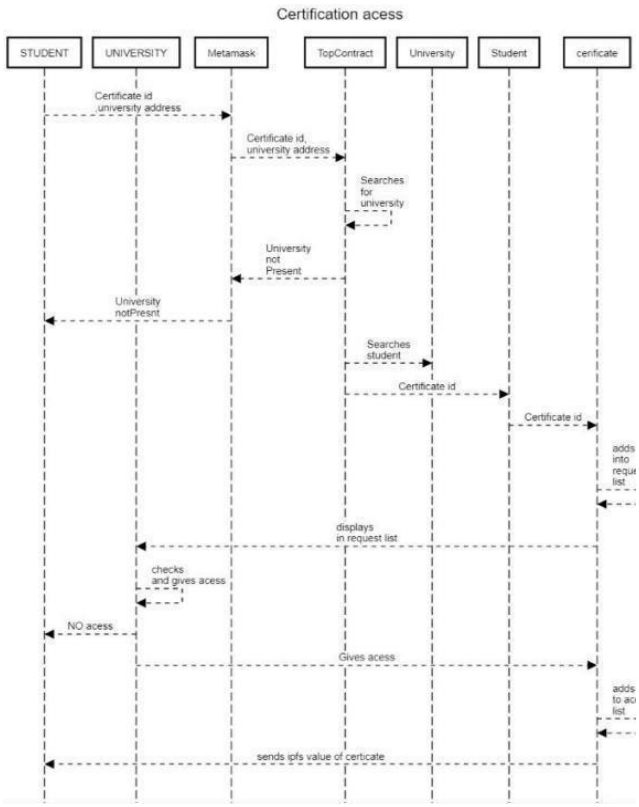


Figure.3 Certification Access

Figure.3 Anyone can apply for a certificate from their institution, but the school will either issue or deny the certificate. Once access is granted, learners can download certificates from the blockchain (IPFS).

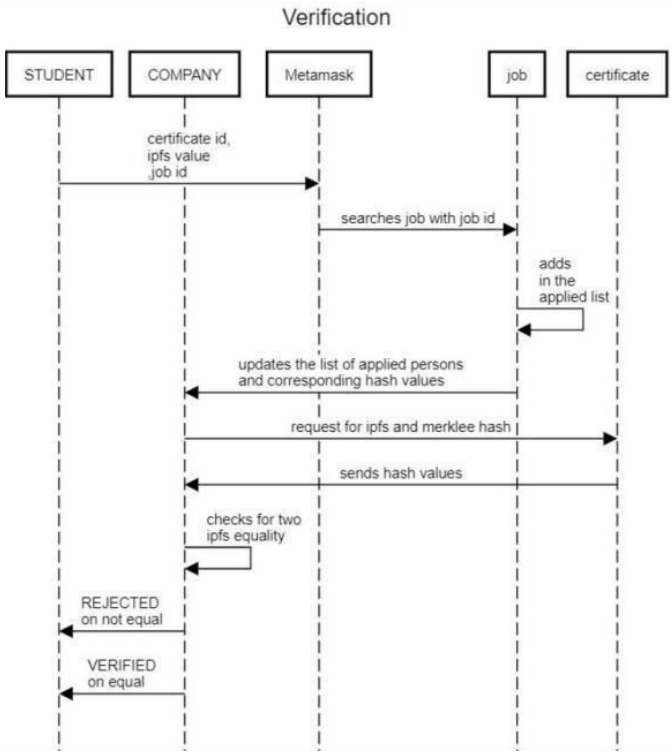


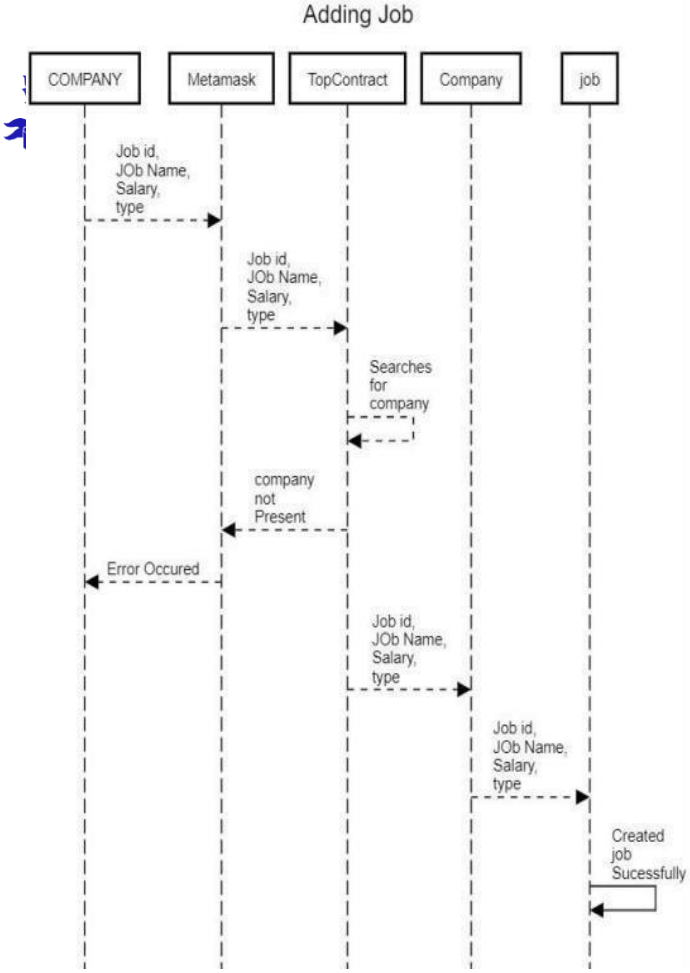
Figure.4 Add Certification

Figure.4 Student's address is added to smart contract's candidate listfor this position. Your organization can then choose to validate the certificate. This includes checking the Merkle hash value and her IPFS numbers and notifying personnel on this exteriorof the organization Unless the document is verified, the company may discontinue it. All decisions Created by the company are interacted to a learner.

Figure.5 Add Job

Figure.5 Any company may post a job advertisement with a particular job ID, title, pay, location, and other details. By using a provider, all of the data is stored, the information is sent over the network, and job who has not yet received approval.

When seeking positions in the private or public fields, students must provide such documents, and each certificate needs to be notarized in person. Students occasionally fabricate certificates, which can lead to issues. Academics have long been concerned about fraudulent degrees. Because these certificates can be created cheaply and verified one at a time, verification methods are especially challenging. Digital certificates can be stored on blockchain, which solves this issue.



V. ARCHITECTURE

Universities must first register in order to generate immutable certifications using blockchain technology. All transactions will be transferred to your university wallet address. Universities can be added by smart contract owners. Once added, the institution can generate a certificate including the data fields with authorization. Each certificate (IPFS) produced is recorded in the interplanetary file system.Next, provide a unique hash created using the SHA-256 method. This serves as a unique identification number for the document. The hash and certificate details are stored on the blockchain and the learner receives a transaction ID. as a consequence.

The certificate details can be viewed by anybody who has access to the initial accreditation duplicate, IPFS has stored within the information, and this transaction code. Furthermore, it is impossible to make or alter phony certificates using the same information. This assists in resolving certificate fraud concerns.

VI. RESULT

The Innovative Certificate and Signature Verification System is a cutting-edge technology that speeds up the authentication of certificates and signatures. With a variety of features and capacities, it assures the dependability and correctness of these critical papers. Using cutting-edge technologies such as blockchain and artificial intelligence, the system successfully combats fraud and ensures the integrity of the verification process.

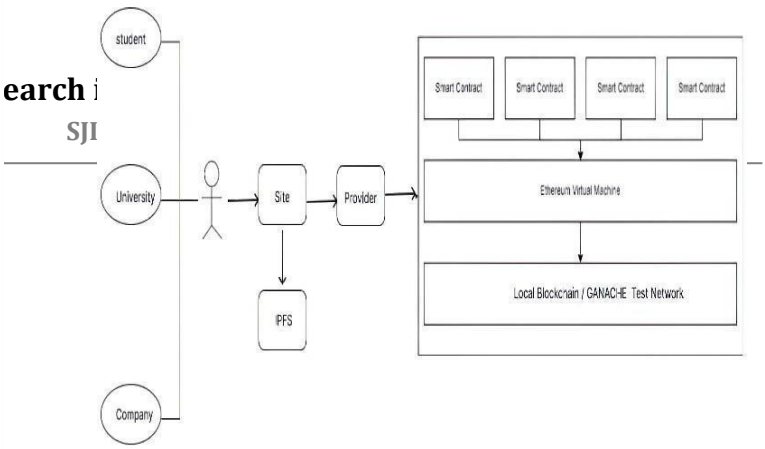


Fig. 6 Architecture of Proposed System

Using blockchain technology, the system securely stores and encrypts certificates andsignatures, making them resistant to manipulation or change. Further more, the use of AI algorithms allows for a thorough inspection and comparison of signatures, which strengthens the verification process. The method's speed and efficiency stand out as main benefits, dramatically shortening the time necessary to validate certificates and signatures and so saving critical time and money for both people and businesses. One of the most significant advantages of this strategy is its speed and efficacy. It significantly reduces the time required to authenticate certificates and signatures, saving people and enterprises considerable time and resources.

The system is inherently user-friendly, with a simple interface that allows consumers to easily upload and check documents. Furthermore, the system's scalability and interoperability emerge as critical features, enabling for smooth integration across several enterprises and sectors. Its compatibility with current systems and databases enables efficient communication and coordination among the numerous players engaged in the verification process.

Security and data protection are the foundation of the system's operation. Sensitive data is protected against unwanted access and modification while conforming to strict privacy standards. Further more, the system keeps a thorough audit trail, which provides a clear and verifiable record of all certificate and signature verification actions.

In essence, the Innovative Certificate and Signature Verification System transforms document authentication with modern technology and a user- centric design. Its multidimensional strategy, which includes blockchain and AI, not only assures the trust worthiness and correctness of certificates and signatures, but also answers the increasing demand for verification efficiency. This system is a benchmark for certificate and signature verification, focusing on security, user-friendliness, and interoperability. It aims to make document validation faster and more secure in the future. To summarize, the Innovative Certificate and Signature Verification System is cutting-edge technology that revolutionizes certificate and signature verification.

SOFTWARE SPECIFICATION

Ganache: Creates a Local Ethereum test environment.
Truffle: Initialise basic setup for Ethereum Dapp
React js: for frontend implementation
Web3.js: for interacting with Smart Contracts
IPFS: for decentralized file storage
Meta Mask: Wallet for connecting with Ethereum Network
Vscode: code editor

VII. Conclusion

Creative blockchain techniques reduce certificate fraud. The system's automatic certificate issuance process is just and honest. Businesses and organizations can now use this to look up certificate information on their systems. A suggested fix lowers operating expenses, stays away from data manipulation, and provides precise and reliable encrypted information. Data Integrity is among the most crucial aspects of blockchain technology. Every web node acts as a massive public ledger, storing and verifying the same data. Any organization might try this. technique to verify the data contained in a certificate since certificates are generated. honestly and openly. Fake certification is a problem that can be solved with the aid of software.

Acknowledgment

I want to express my gratitude to all of the professors and other staff members in the Department of Computer Science and Engineering for assisting with the project.

References

[1] Cheepurupalli Durga Pradeep, Mulagapaka Ashish, R. Aishwarya, R Yogitha. "A Blockchain Application for the Verification of Academic Information and ScalableCertification",20237th International Conference on Computing Methodologies and Communication (ICCMC), 2023

[2] Pandey, S., Ojha, G., Shrestha, B., & Kumar, R. (2019,May). Block SIM: Apractical simulation tool for optimal network design, stability, and planning. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE.

[3] Ehmke, C., Wessling, F., & Friedrich, C. M. (2018, May). Proof-of-property: a lightweight and scalable blockchain protocol. In Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain.

[4] Caldarelli, G., & Ellul, J. (2021). Trusted academic transcripts on the blockchain: A systematic literature review. Applied Sciences, 11(4), 1842.

[5] Alam, A. (2022). Platform Utilising Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records. In Smart Data Intelligence (pp. 307-320). Springer, Singapore.

[6] Grover, P., Kar, A. K., & Janssen, M. (2019). Diffusion of blockchain technology: Insights from academic literature and social media analytics. Journalof Enterprise Information Management.

[7] Massaro, Maurizio. "Digital transformation in the healthcare sector through blockchain technology. Insights from academic research and business developments." Technovation (2021): 102386.

[8] Zou, Y., Meng, T., Zhang, P., Zhang, W., & Li, H. (2020). Focus on blockchain: A comprehensive survey on academic and application. IEEE Access, 8, 187182- 187201.

[9] Janowicz, K., Regalia, B., Hitzler, P., Mai, G., Delbecque,S.,Fröhlich,M.,...&Lazarus,T.(2018).On the prospects of blockchain and distributed ledger technologies for open science and academic publishing. Semantic web, 9(5), 545-555.