iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IX Month of publication: September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74405

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Secure Academic Credential Management using Blockchain-Based Self-Sovereign Identity

Rehna R S[1], Aswathy L[2], Nandana B S[3], Mariam Susan Lal[4], Rithu S Raj[5]
[1]*Department of Computer Science & Engineering, LBS Institute of Technology for women, Thiruvananthapuram,*
[2, 3, 4, 5]*Department of Information Technology, LBS Institute of Technology for women, Thiruvananthapuram*

Abstract: Digital identity management and verification of educational credentials have grown increasingly difficult in today's times. Conventional practices tend to include centralized systems that are vulnerable to breaches and inefficiencies. Realizing the existing difficulties in identity management, we suggest a decentralized SSI-enabled model to overcome these difficulties. The model facilitates SSI-enabled operations such as user sign-up, issuing decentralized identifiers (DIDs) with public/private keys created upon sign-up, issuing and creation of verifiable credentials (VCs) in the form of digital certificates of student information, academic records, and issuer signatures and credential validation facilitated by decentralized blockchain-based ledger. Educational institutions issue and create verifiable credentials associated with students ID. The system enables learners to obtain and hold verifiable credentials (VCs) for their digital proof of certificate. The issued credentials would be retained off-chain and hash value of the credential would be maintained in blockchain ledger. The model uses cryptography such as hashing and digital signature to check data integrity and authenticity and issuance of the credential, storing and verifying will be handled by Smart Contract. An easy-to-use interface that provides management, request, and document verification. An integrated system based on blockchain, decentralized storage, and cryptographic algorithms ensures a privacy-oriented and consistent system for handling academic documents.

Keywords: Blockchain, Self-Sovereign Identity (SSI), Decentralized identifiers (DIDs), Verifiable Credential (VC), SmartContract(SC).

I. INTRODUCTION

With the growth in online education, telecommuting, and worldwide exchanges of educational credentials, credential management and the verification of the same have increasingly become complicated with the advent of the digital age. Traditional credential management systems generally rely on centralized repositories kept by employers, educational institutions and universities, and third-party verification agencies. The traditional systems have many issues like security threats, inefficiency, non-transparency, and susceptibility to credential forgery. With the advancement in digital technology, the demand for a safer, decentralized, and privacy-protecting identity management system has rendered its inevitability. A self-sovereign identity (SSI) management system based on blockchain offers solution to such problems by enabling users to control and manage their own digital identities.Self-Sovereign Identity (SSI) makes individuals fully capable of controlling their identity information, without any central system. This system offers a secure, transparent, and efficient way of handling academic credentials through blockchain technology, decentralized identifiers (DIDs), and verifiable credentials (VCs). Universities and employers can verify digital credentials of the students' without relying on a central authority. This work intends to take advantage of the principles of self-sovereign identity and blockchain technology to build a secure, efficient, and privacy-focused academic credential management system. The intended solution is meant to remove fraud from credentials, significantly reliance on external verifiers, and make overall effectiveness of digital identity management in education more improved.

II. BACKGROUND

Colleges have been giving out paper certificates and maintaining electronic records in large centralized repositories for decades. The system has been working well enough, but it is with some severe problems:

1) *Security and Privacy Risks*: Decentralized credential storage systems are exposed to cyberattacks, abuse, and data disclosure. Sensitive educational information are likely to be stored in plaintext databases, which are thus prime targets for the hackers.
2) *Credential Forgery and Fraud:* Employment trust to this point has been undermined by the widespread issue of phony degrees, diploma mills, and falsified credentials. It becomes progressively harder to ascertain valid as opposed to worthless scholarly documents.

3) *Inefficient and Uninteresting Authentication Processes:* The process of authenticating credentials is sometimes lengthy and has a number of steps, including the calling of issuing institutions or third-party authentication providers. The processes are likely to be cumbersome, costly, and inefficient to graduates and employers.
4) *Dependence on Centralized Organizations:* Professionals and students depend on organizations to store and verify their credentials securely. Individuals cannot easily verify their academic credentials when an organization is compromised, closed, or papers are misplaced.
5) Lack of Interoperability Worldwide: Various organizations and nations apply varied credential standards, resulting in interoperability. One universal credential verification system acceptable across the globe is necessary.

Self-Sovereign Identity (SSI) and Blockchain for Managing Digital Credentials Self-Sovereign Identity (SSI) is a paradigm shift in identity management where students have complete control over their academic and personal credentials. In contrast to normal identity management processes, SSI enables users to store and manage credentials without the interference of a centralized authority. Key characteristics of an SSI-based educational credential system are:

a) *Decentralized Identifiers (DIDs):* Blockchain-secured identifiers, which present an immutable and secure way of storing and presenting credentials.
b) *Verifiable Credentials (VCs):* Digitally signed institutional credentials delivered to the student, and cryptographically verifiable.
c) *Decentralized Storage:* Storage of the credential information in securely dispersed storage capsules (SCs) across a blockchain-platform.
d) *Cryptographic Technique:* Implementation of hashing and digital signature ensures the integrity and authenticity of the academic credential.

Blockchain benefits in SSI-Based Credential Management Blockchain technology also has some true benefits for SSI-based identity systems:

- *Immutability:* Preloaded once credentials cannot be altered or amended and therefore confer integrity to information.
- *Decentralization:* Eliminates reliance on a central point of trusting credentials.
- *Transparency:* Every credential transaction gets documented on the blockchain, providing and verifiability.
- *Efficiency:* Every verification process is carried out by technology, and time and money are saved from manual verification.

III.MOTIVATION

The motivation for this research results from the great need for a secure, efficient, and user-centered academic credential verification system.

A. Increased Security and Privacy

Centralized and conventional database-driven identity management systems can be easily hacked, tampered with illegally, and even become victims of data breach. Confidentiality is preserved by the system using Cryptographic Technique such that the credentials may be made secret from unauthorized tampering or access. Blockchain cryptographic attribute provides an assurance that credentials will be stored as well as remembered in an irreversible way.

B. Elimination of Credential Counterfeiting

Mass-scale spurious academic records and fake records have de-valued the sanctity of hiring processes as much as academic admission processes. Irreversible, tamper-evident, and decentralized system of credentials assures resistance to forgery and fraud and assures that credentials are real. Employers are able to authenticate credentials on the fly without having to pursue third-party validation.

C. Maximizing Efficiency and Reducing Costs

It is costly, time-consuming, and involves enormous man-hours via conventional manual verification processes. Blockchain-based smart contracts automate and perform issuance and verification of credentials in real-time. This eliminates the administrative burden from employers and institutions to achieve ease of verification processes.

D. Sovereignty of the User over Their Own Credentials

Current systems use third parties to play the role of brokers in issuing and verifying credentials. SSI gives individuals, professionals, and students complete control over their education credentials. Users are completely responsible for controlling their credentials on their own terms, deciding at their own will whether or not to share or revoke access.

E. Leveraging Blockchain's Decentralized and Transparent Nature

Centralized infrastructures are by nature opaque and central authority-reliant. Blockchain offers a transparent, auditable, and immutable record-keeping system where data can be accessed directly by the concerned parties without the assistance of intermediaries.

IV. OBJECTIVE

The core agenda of the research is to offer an identity management system that is decentralized where learners are custodians, owners, and sharers of academic credentials securely either with or without third parties. Rooted in the foundation of self-sovereign identity (SSI) in its design, the system provides that credentials are always owned and controlled by users entirely themselves at all times, thus mitigating risks of third-party authentications. It combines decentralized identifiers (DIDs) and verifiable credentials (VCs), and this allows institutions to issue institutionally cryptographically signed, tamper-evident credentials. The security model allows students to store and transfer their credentials securely with employers and institutions in a way not involving intermediaries. For locking credentials, cryptographic methods such as hashing algorithm, digital signature, are applied, these strategies protect credentials against unauthorized tampering while making it simple to check without revealing confidential data. Blockchain technology also contributes to the genuineness of the information since issued credentials turn out to be unalterable, and forgery or deleting them is not easy. This enhances trust, transparency, and security among institutions, employers, and students. The system further includes decentralized storage to increase efficiency with credentials spread out in storage capsules (SCs) and therefore preventing centralized loss or corruption of data risk.

V. PROPOSED SYSTEM

A. System Overview

In this system, schools and universities issue credentials. When a student finishes a course or program, the school creates a Verifiable Credential (VC) for the academic certificate. The VC includes details like the student's name, degree, issue date, and other school-related information. The school signs the credential using its private key, so it can't be changed without authorization. To enhance security and transparency, the system also stores the hash of the VC on the blockchain so that it cannot be altered.

This blockchain entry gives an immutable list of all the issued credentials so that no one can alter the data without being detected. Students get a Self-Sovereign Identity (SSI), which lets them control a unique Decentralized Identifier (DID) stored on the blockchain. A DID is a special decentralized identifier that doesn't need a central authority to issue certificates. It allows students to manage their credentials on their own, without depending on anyone else.

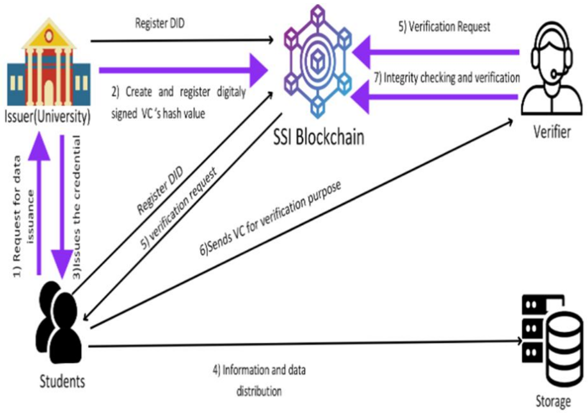
Register DID
Issuer(University)
2) Create and register digitaly signed VC's hash value
5) Verification Request
7) Integrity checking and verification
SSI Blockchain
Verifier
1) Request for data issuance
3)Issues the credential
Register DID
5) verification request
6)Sends VC for verification purpose
Students
4) Information and data distribution
Storage

Fig. 1 System Architecture

Verifiable Credentials (VCs) link to the student's DID giving them full control over their data and when they share their credentials. When a student needs to prove they have an academic certificate, they can show their credentials in a safe way that protects their privacy.

Third parties like employers, institutions or government organizations can validate student certificates. They do this by requesting the student to present their VC and compare the hash value with the saved hash value in the blockchain. If the two hashes are the same, it is a guarantee that the VC is original, and the third party is certain no one has tampered with the certificate. In this way, there is no third party, which facilitates easy certificates and time and authentication of money saved.

B. Technology Stack

1) *Blockchain*: Blockchain is the backbone of our system, it provides an immutable, secure, and mostly utilizes Hyperledger Fabric, which is a permissioned blockchain system centralized system to maintain hash value of credentials. Utilizing blockchain, we avoid having a centralized party, giving data transparency, integrity, and trust. Because it is decentralized, it avoids tampering or illegal accessing, thus presenting itself as a reliable way of dealing with academic credentials. Our platform is designed to be effective and secure for credential management. Only authorized parties like verifiers and universities are allowed to access the blockchain network through permissioned access, guaranteeing that secret academic data does not fall into the wrong hands. The Hyperledger Fabric architecture also allows it to scale and handle a high volume of transactions in institutions. Private channels and data partitioning features offer secure data sharing, making it the ideal blockchain solution for our system.
2) *Smart Contract*: Smart contracts have a key role in making the system's operations automatic. These contracts let universities give out Verifiable Credentials (VCs) to students. The smart contract also checks if the credentials are real before giving them out to make sure they meet set standards. After a credential is given, the blockchain stores a cryptographic hash of the VC, which third parties can use to check it.
3) *SHA-256*: The system adopts SHA-256 for hashing Verifiable Credentials for improved security and integrity. A unique hash value is generated for each VC so as to ensure drastically different hash values when a minimal change on the original credential is affected. Any form of tampering would be unmasked since the hash is stored on the blockchain. SHA-256 facilitates lightweight verification where third parties are able to confirm the authenticity of credentials without only accessing the VC, thereby preserving the privacy and efficiency.
4) *Docker*: For consistency of the network in various environments, the blockchain network is containerized and executed on Docker. Deployment of Hyperledger Fabric components such as peers, orderers, and certificate authorities (CAs) is simplified through Docker. With Docker, the network's behaviour is exactly the same across development, test, and production environments, decreases unexpected errors, and simplify development.
5) *DID Creation*: The system employs Decentralized Identifiers (DIDs) as a key component of its Self-Sovereign Identity (SSI) system. Fabric CA on the Hyperledger Fabric network is used to create and register DIDs, allowing authorized parties, like university and students, to register and generate public and private keys. These decentralised ID are used as a unique identifier that securely connect students to their Verifiable Credentials without compromising privacy. Using DIDs, the system guarantees that students have complete ownership of their credentials so that they can choose to share their information at will and with whom they wish.

C. WorkFlow

1) *DID Creation*: The system utilizes Decentralized Identifiers (DIDs) as one of the major elements of its Self-Sovereign Identity (SSI) framework. Fabric CA on the Hyperledger Fabric network is utilized to create and register DIDs, enabling authorized entities, such as university and students, to register and create public and private keys. These decentralised ID are utilized as a unique identifier that securely link students to their Verifiable Credentials without invading privacy. Through DIDs, the system ensures that students fully own their credentials to be able to make a decision at their will about sharing their information as well as with whom to share.
2) *Verifiable Credential Issuance*: Once the ID is set, the organization issues a Verifiable Credential (VC), for the academic certificate of the student through a smart contract. The VC includes the most critical data, like the name of the student, academic record, issuing institution's name, public key of the student (as a reference to the identity), date of issuance, and the duration for which the credential is valid. For ensuring immutability, a hash value of the VC is safely archived on the blockchain. Once generated, the VC is signed by the institution utilizing their public key, for validation of authenticity. A SHA-256 hash of the VC is then safely deposited on the blockchain. This assures that any form of change made to the VC will cause the hash to vary during verification. As blockchain entries are immutable, the VC is secure, with a tamper-evident means of verification.

3) *DID Creation:* If a third party, such as an employer or some other institution, is required to authenticate a student's credentials, they ask for the VC from the student. The student can share the hash value with the VC. The third party compares the student's hash with the hash saved on the blockchain. Once there is a match of the hashes, the VC is confirmed authentic and ensure not to have been tampered. The verification method ensures trust for students and third parties without going through intermediaries. Since it is decentralized, verification is immediate, secure, and privacy-guarantee. Security and Privacy concerns.
4) *Cryptographic Integrity*: It uses SHA-256 hashing for the integrity and authenticity protection of Verifiable Credentials (VCs). On releasing a VC, it generates a hash by means of SHA-256 so that any change will result in a completely different hash, thereby tampering will be impossible to go undetected. The cryptographically generated hash is stored securely on the blockchain, and provides a tamper-proof repository for future verification. This encryption method ensures that VC data remains safe and confidential, untampered with by any unauthorized person.
5) *Privacy*: The system follows Self-Sovereign Identity (SSI) principles, giving the students full control over their credentials. They have the option of when and to whom they would like to share their Verifiable Credentials, thereby not exposing anything without their clear consent. The decentralized operation reduces unwanted exposure of user data.
6) *Immutability*: The blockchain ensures the immutability of the VC hash by placing it in an immutable ledger. The stored VC hash cannot be altered. Any alteration of the original information will cause a discrepancy in the hash upon verification, and it is not possible to tamper with it, ensuring the integrity of the credential in the long run.

VI. RESULT

The model of the self-sovereign identity (SSI) system based on blockchain is used to test efficiency in issuing academic credentials Generation and pamphlet signs were about 2.3 seconds in average time. This issuance time was constant through many test cases that contained all other institutional setups by that time proving the scalability of the said system. Verification speed was analysed under different conditions, single and batch certificate verification. Concerning a single credential, it took about 1.2 seconds to verify, and for ten certificates. The results proved faster verification processes from what blockchain offers, compared to traditional if batch verification was applied; it would take 3.5 seconds manual-based verification, which lasts several hours or days.

A. System Overview

To secure academic credentials, SHA-256 hashing was implemented to immutably store credential proofs on the blockchain. Tests indicated that nobody can execute any alterations due to immutability on the block. Forgery attempts showed failure; the hash of each certificate was verified against the recorded blockchain ledger.

B. Scalability and transaction throughput

Performance evaluation with Hyperledger-Fabric blockchain was conducted. The network supports up to 500 transactions per second (TPS); these imply that the system can efficiently cater to a large number of concurrent certificate issuance and verification requests. These results also suggest that the system could scale up efficiently with no waiting time or any knockdown in performance.
A user survey assessed the efficacy of the web-based credentialing management platform. 95% of the participants found the interface intuitive and easy to use. The possibility provided to share credentials with third parties securely, leveraged by blockchain-based identity management, improved user satisfaction. In addition, students were able to retrieve and show their credentials to employers via a presentation of 2 seconds, thus enhancing the speed of job applications through efficiency.

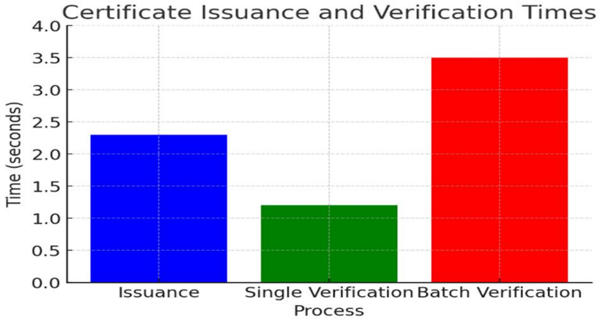

Fig.2. Certificate issuance and verification time chart

During the scalability test, it was found that the performance of the system dipped when the number of concurrent transactions exceeded 10000, thus optimizing execution of the smart contract should be put in place. Also, some institutions without prior blockchain infrastructure had an initial deployment delay of up to five minutes because of blockchain synchronization.

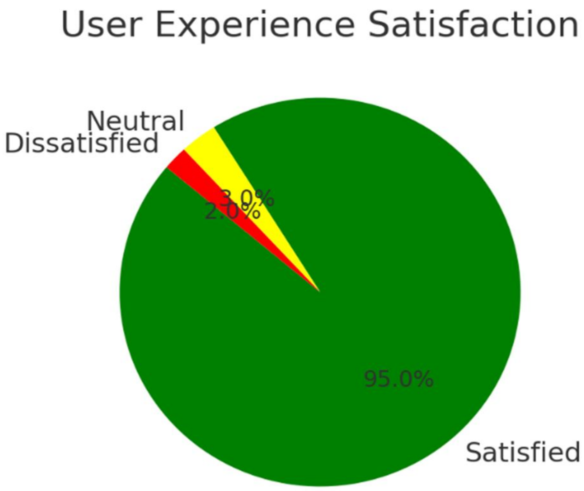

Fig.3. User Experience Chart

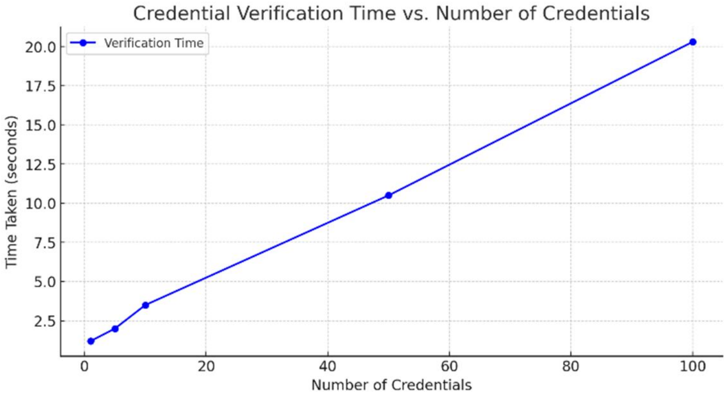

Fig.4. Credential verification time vs. Number of credentials

The findings confirmed that the blockchain-based SSI system seamlessly improves academic credential security, verification efficiency, and control by the end user. It shows the integration of blockchain technology within academic institutions, which counters credential fraud risks.

VII. DISCUSSION

Management of academic credentials is a chronic issue, particularly with respect to security of data, authenticity, and control by users. Conventional systems do not provide solutions to these problems, and opportunities for forgery, inefficiency, and untransparency arise. Blockchain-based Self-Sovereign Identity (SSI) systems present a revolutionary solution to these problems by presenting a decentralized and tamper-evident system for managing credentials. Our research focuses on exploring these capabilities by proposing a blockchain-enabled SSI framework. This system integrates cryptographic techniques such as SHA-256 hashing and decentralized infrastructure to ensure the authenticity and integrity of academic credentials. By enabling universities to issue tamper-proof digital certificates, this model introduces novel, scalable, and user-centric approaches toward credential verification. These findings provide a theoretical basis for building secure, efficient, and transparent systems for academic credentials.

The proposed SSI model addresses core challenges in credential management by leveraging blockchain's decentralized and immutable nature. SHA-256 hashing ensures that credential proofs remain tamper-proof and secure.

Cryptographic signing of credentials guarantees their authenticity, thereby eliminating risks associated with forgery. Moreover, the append-only structure of blockchain prevents unauthorized modifications, ensuring that all credential records remain immutable and auditable over time. These features collectively enhance the trustworthiness of the credentialing process. A significant focus of this research is on empowering students with complete ownership and control over their credentials. By implementing selective disclosure mechanisms, students can share specific pieces of information, such as degree details or transcripts, with third parties without exposing unrelated personal data. This is to ensure they meet privacy guidelines and deal with increasing data security concerns. This also eliminates the requirement for go-betweens, which facilitates verification in a much simpler and affordable manner for employers and students.

Moreover, it has scalable and accessible aspects. A blockchain-based SSI can handle any size of transaction due to easy integration without causing a loss of performance. The access portal is made available using a friendly web portal which enables students, universities, and employers to make accessibility without in-depth technical skills. Thus, design aspects of this system make the solution for today's problems of modern credential management challenges. This research illustrates the transformative impact blockchain-based SSI systems will bring to address challenging problems in managing academic credentials. The proposed architecture establishes a secure, scalable, and user-centric way forward that significantly benefits the current models used. The conceptual model is far from implementation, providing instead a concrete theoretical basis that subsequent studies must then build upon; these include limiting issues such as investment in initial infrastructure and regulatory alignments.

Future work should focus on piloting the proposed system in real-world academic environments to assess its practical feasibility and performance. Moreover, interoperability with existing credential management frameworks has to be explored as well as refining the system for a broader adoption process. These aspects will help the blockchain-enabled SSI model redefine trust and efficiency within the academic and professional ecosystem.

VIII. CONCLUSION

This paper articulated a self-sovereign identity (SSI) model, built on blockchain technology, to manage academic certificates in a decentralized and secure approach to issuing credentials and verifying them. Using cryptographic techniques and an unalterable blockchain platform, security, authenticity, and control over user data are improved by the application of a proposed system. The model ensured that academic records cannot be tampered with, while students themselves remain the owners of their own credentials. This framework significantly reduces the period for verification, eliminating forgery opportunities, and therefore makes credentialing more transparent and efficient. Various challenges, ranging from initial infrastructure investments to regulatory compliance, exist, but the potential benefit outweighs these constraints. Future work should be focused on real-world deployment, scalability improvement, and interoperability with current existing academic credentialing systems. This model opens the door of solution to revolutionize credential management and build trust while facilitating verification processes in both academic and professional settings.

REFERENCES

[1] A. Rustemi and F. Dalipi, "Academic Certificate Verification: A Practical Comparison between Centralized and Blockchain-Based Systems," 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, 2024

[2] C. N. Butincu and A. Alexandrescu, "Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems," in IEEE Access, vol. 12, pp. 60928-60942, 2024

[3] E. Zeydan et al., "Blockchain-Based Self-Sovereign Identity: Taking Control of Identity in Federated Learning," in IEEE Open Journal of the Communications Society, vol. 5, pp. 5764-5781, 2024

[4] N. V. Toutova, A. P. Gaeva, V. L. Agamirov, L. V. Agamirov and I. A. Andreev, "Blockchain in Education: a New Approach to Storing and Verification of Academic Works," 2024 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED), Moscow, Russian Federation, 2024

[5] K. Tan-Vo et al., "Optimizing Academic Certificate Management With Blockchain and Machine Learning: A Novel Approach Using Optimistic Rollups and Fraud Detection," in IEEE Access, vol. 12, pp. 168135-168159, 2024

[6] E. S. Fathalla, M. Azab, C. Xin and H. Wu, "PT-SSIM: A Proactive, Trustworthy Self-Sovereign Identity Management System," in IEEE Internet of Things Journal, vol. 10, no. 19, pp. 17155-17169, 1 Oct.1, 2023

[7] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in IEEE Access, vol. 11, pp. 64679-64696, 2023

[8] M. Dieye et al., "A Self-Sovereign Identity Based on Zero-Know ledge Proof and Blockchain," in IEEE Access, vol. 11, pp. 49445-49455, 2023

[9] M. R and S. Joshi, "Securing academic certificate verification with blockchain-based algorithmic rules," 2023 IEEE 4th International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2023

[10] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022