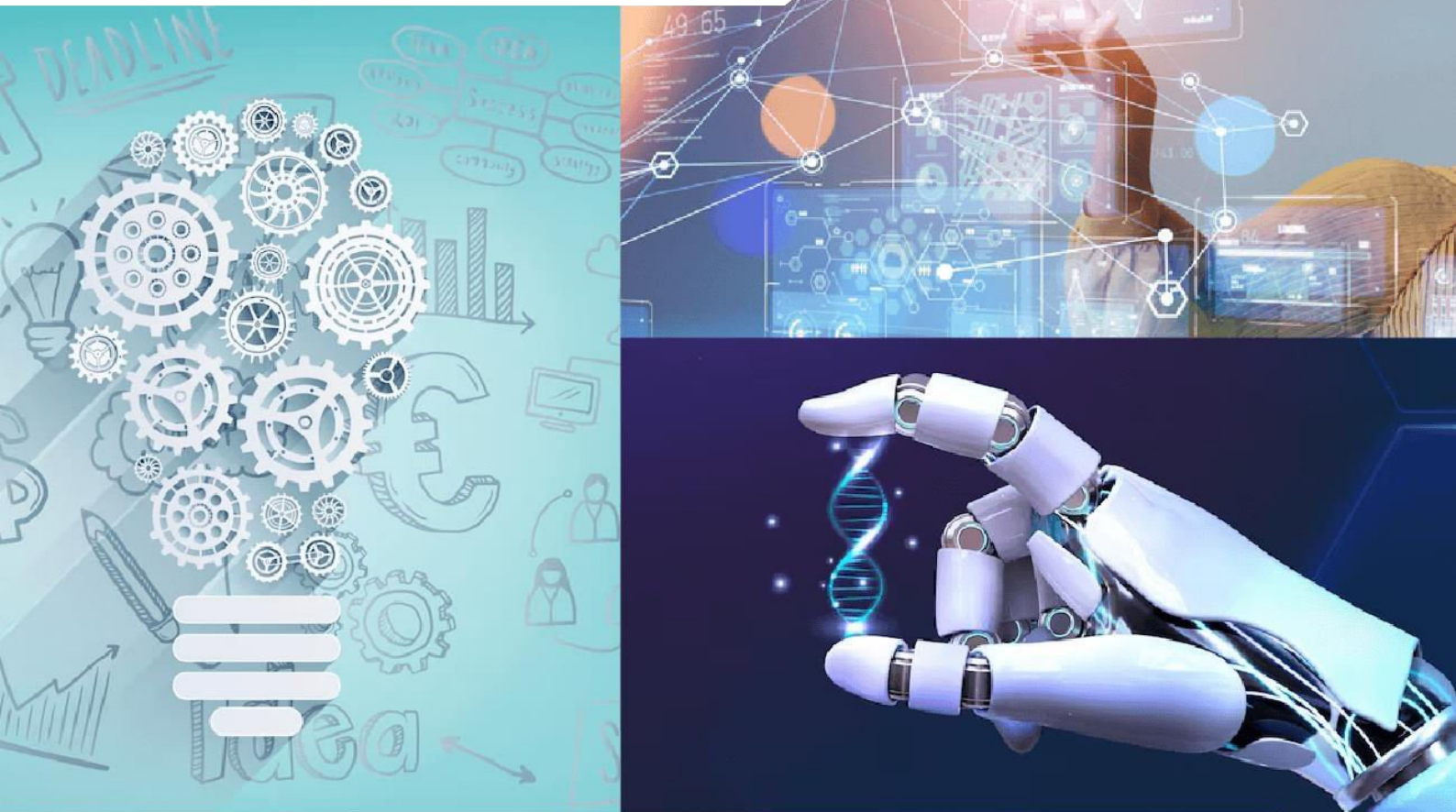




International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 2, March - April 2026

Impact Factor: 8.152



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



A Blockchain-Powered Platform for Secure Management and Verification of Educational Credentials

A.Laksmipathi rao¹, Syed Zaheer Abbas², Pureti Ruthik Sohan³, Mukkula Abhiilashh Vardhan⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India¹

Students, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India^{2,3,4}

ABSTRACT: The increasing incidence of fake academic certificates poses a serious challenge to the credibility of educational institutions and the fairness of recruitment processes. Conventional verification systems are often slow, disjointed, and vulnerable to manipulation, making it difficult to ensure authenticity. To address these issues, blockchain technology offers a reliable alternative due to its decentralized nature, data immutability, and resistance to tampering. This paper presents ElimuChain, an integrated blockchain-based solution aimed at managing and validating educational credentials across all levels and institutions within a nation. Developed as a decentralized application on the Binance Smart Chain, the system utilizes smart contracts to automate certificate issuance and employs distributed storage mechanisms for secure document handling. By providing a transparent and efficient verification process, the proposed platform minimizes fraud risks and significantly improves the reliability and accessibility of academic records.

KEYWORDS: Blockchain Technology, Certificate Verification, ElimuChain, Decentralized Application (DApp), Binance Smart Chain (BSC), Smart Contracts, Data Immutability, Fraud Prevention, Fraud Prevention, Digital Certificates.

I. INTRODUCTION

The rise in forged certificates has further weakened trust among institutions, employers, and students, creating a need for a more dependable and transparent solution that can ensure the authenticity of academic achievements. Blockchain technology has emerged as a powerful tool to address these challenges due to its decentralized structure, immutability, and high level of security. By storing data across a distributed network, blockchain ensures that once information is recorded, it cannot be altered or tampered with. This makes it highly suitable for managing sensitive data such as educational certificates. The proposed system, ElimuChain, aims to provide a unified and scalable platform for managing educational credentials across multiple institutions and academic levels.

II. LITERATURE SURVEY

P. Verma, V. Tripathi, and B. Pant (2024) The 2024 study on a blockchain-based system for managing medical interns' credentials proposes a secure and transparent method for handling academic and skill-based records. It introduces stackable micro-credentials, allowing interns to earn and combine verified digital certificates for specific competencies. These records are stored on a decentralized blockchain network, ensuring authenticity and preventing tampering while enabling easy verification by institutions and employers. The system also supports a dynamic digital portfolio, helping interns showcase their achievements in real time and allowing organizations to efficiently monitor and validate their progress, ultimately improving trust and efficiency in medical training and career transition.

Magar et al (2024) This review examines the use of blockchain technology in verifying educational documents by analyzing recent research on credential management, fraud prevention, and system design. A key trend identified is the adoption of a hybrid approach, where document hashes are stored on the blockchain while actual data is kept off-chain, improving both security and efficiency. The study also notes that although many frameworks have been proposed, only a limited number have been implemented in real-world educational settings. While blockchain offers faster and more secure verification, most solutions are still in experimental or early deployment stages.

W. Hong, Y. Weng, and Q. Li (2023) The 2023 paper proposes a secure framework for sharing educational credentials by combining blockchain technology with proxy re-encryption. In this approach, actual credential data is stored in encrypted form in the cloud, while only their hashes are recorded on the blockchain to ensure integrity and transparency. This design protects sensitive information while still enabling reliable verification. The system allows only authorized users to access the encrypted data, ensuring privacy without compromising accessibility. It enables institutions to issue verifiable credentials and allows individuals to share them securely when required.

N.-N. Dao, T. N. Thinh, N. T. Nguyen, and T. V. Pham (2023) The 2023 paper introduces ZUni, a blockchain-based framework aimed at improving the security and privacy of educational credential verification. Built on Ethereum, the system integrates IPFS for decentralized storage, Zero-Knowledge Proofs for privacy-preserving validation, and Decentralized Identifiers for secure identity management. This combination allows credentials to be verified without revealing sensitive personal information.

III. EXISTING SYSTEM

Current methods for managing and verifying educational credentials are mostly centralized and operate in isolation within individual institutions. Certificates are often issued either as physical documents or stored in separate digital systems that do not communicate with one another, resulting in poor interoperability. The verification process is typically manual and slow, involving direct communication with institutions, document checks, or reliance on third-party services, which increases the chances of errors and inefficiencies. This lack of integration and standardization reduces transparency, limits scalability, and weakens overall trust in the credential verification process.

Existing System Disadvantages

- time-consuming
- easy to forge
- Weak access control
- No strong guarantee for file integrity and authentication

Proposed System

The proposed system offers a comprehensive blockchain-based approach for managing and verifying educational certificates across various institutions and academic levels within a country. It replaces traditional manual methods with a secure and transparent digital framework where records are immutable and protected from tampering. The system is built around a decentralized application called ElimuChain, which uses smart contracts to automate certificate issuance and verification, ensuring efficiency and reliability.

Proposed System Advantages:

- Reduces verification time
- Strengthens security
- Ensures tamper-proof
- Strong access control
- Secured callback verification

IV. SYSTEM ARCHITECTURE

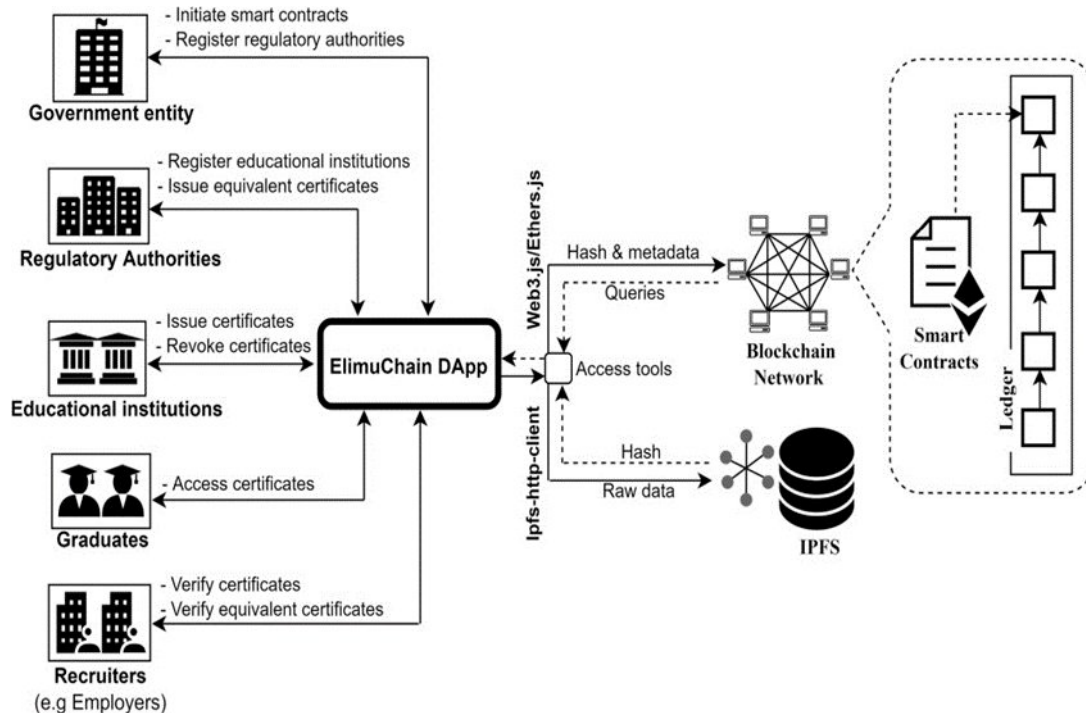


Fig 1.1 System Architecture

This architecture diagram represents the functional flow of the **ElimuChain decentralized certificate system**, showing how different stakeholders interact securely through the DApp. Government entities and regulatory bodies serve as the trust anchors, initializing smart contracts, registering institutions, and issuing equivalent credentials. Educational institutions issue and revoke certificates for students, who can later access and share their verified records.

Methodology

Modules Name:

- Block Chain Module
- Smart Contract Module
- SHA-256 Module
- JSP Dashboard Module
- MySQL Database Module

1) Block Chain Module: In our project, blockchain is used as the core technology to securely manage and verify educational credentials issued by institutes. When an institute generates a certificate for a student, the important verification data such as certificate ID and hash value is recorded on the blockchain. This ensures that certificate records cannot be altered or forged after issuance.

2) Smart Contract Module: Smart contracts are used in our project to automate and control the certificate management and verification process. They define rules for actions such as certificate issuance, approval, and verification access. When an institute uploads a certificate, the smart contract validates whether the institute is authorized.

3) SHA-256 Module: SHA-256 is used in our project to protect the integrity of educational certificates. When a certificate is generated by an institute, the certificate data is converted into a SHA-256 hash value. This hash acts as a digital fingerprint of the certificate. Instead of storing the actual certificate data on the blockchain, only the hash value is stored.

4) JSP Dashboard Module The JSP Dashboard module serves as the central interface of the system, providing users with a clear and interactive view of all essential functionalities. Developed using Java Server Pages (JSP), it enables dynamic content rendering based on user roles such as student, institution, or administrator. This ensures that users can easily access different services such as uploading, requesting, or verifying certificates without confusion.

5) MySQL Database Module: The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs.

V. IMPLEMENTATION

The implementation begins with designing a secure Java-based backend using Spring Boot to manage users, roles, and credential workflows. Institutions, students, and verifiers interact with the system through REST APIs, with authentication handled using JWT and role-based access control. When an institution uploads a certificate, the system processes the data, generates a unique digital fingerprint using a hashing algorithm such as **SHA-256**, and stores the certificate details in a relational database. This ensures efficient data management while keeping sensitive information protected within the application layer. For verification, the platform provides an interface where employers or third parties can validate credentials by uploading a certificate or entering its unique ID.

Algorithm Used

Existing Algorithm

In the storage phase, a collaborator generates a health record for a patient, who stores it in the IPFS network and its metadata in the blockchain in a secure fashion such that another collaborator can later access the record. After this, the designated collaborator can access the health record, in the sharing phase, if she owns the required cryptographic material for this purpose. The emergency access phase occurs when a patient needs emergency medical care and has no physical conditions (e.g., may be unconscious) to give available collaborators access permission to her health record.

Proposed Algorithm

In Proposed system Public key encryption, In a public key (or asymmetric) encryption scheme, a sender u_1 encrypts a message m with a public key pk_{u_2} belonging to a receiver u_2 . The resulting ciphertext $E(m, pk_{u_2})$ can only be decrypted by user u_2 , who owns the corresponding private key sk_{u_2} . To this end, u_2 should compute $D(E(m, pk_{u_2}), sk_{u_2})$, which returns m .

VI. EXPERIMENTAL RESULTS

Home Page:

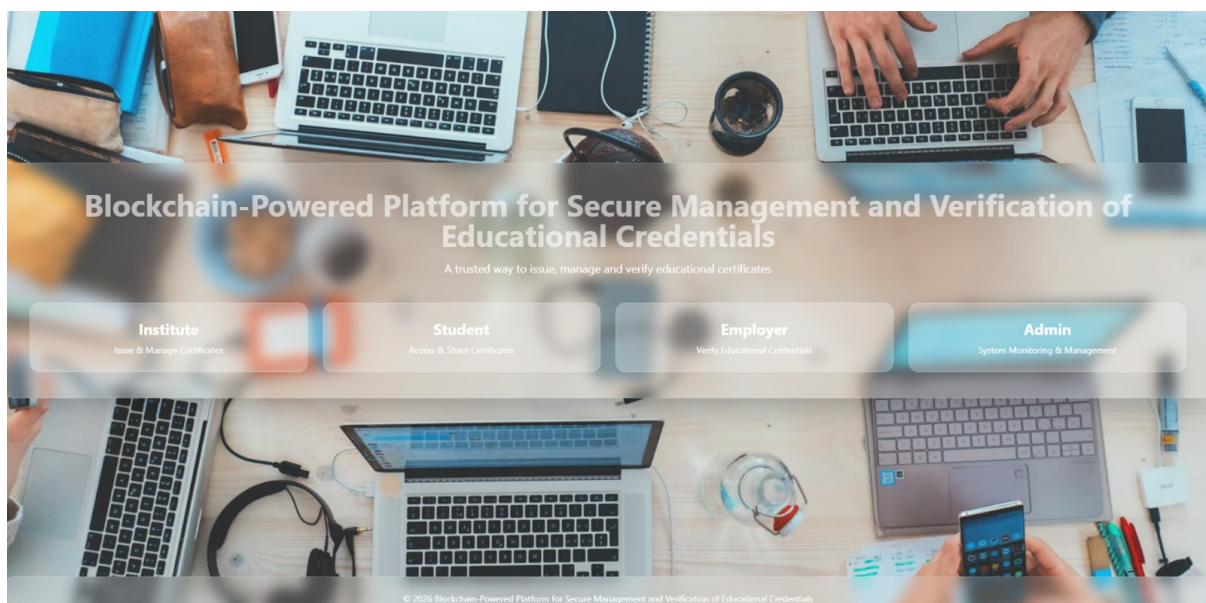


Fig 2: Home Page

The interface represents a centralized entry point for a blockchain-based educational credential system, designed to serve multiple user roles including institutions, students, employers, and administrators. It provides a clean and intuitive dashboard where institutions can issue and manage certificates, students can access and share their credentials, employers can verify authenticity, and admins can monitor overall system activity

Admin login Page:

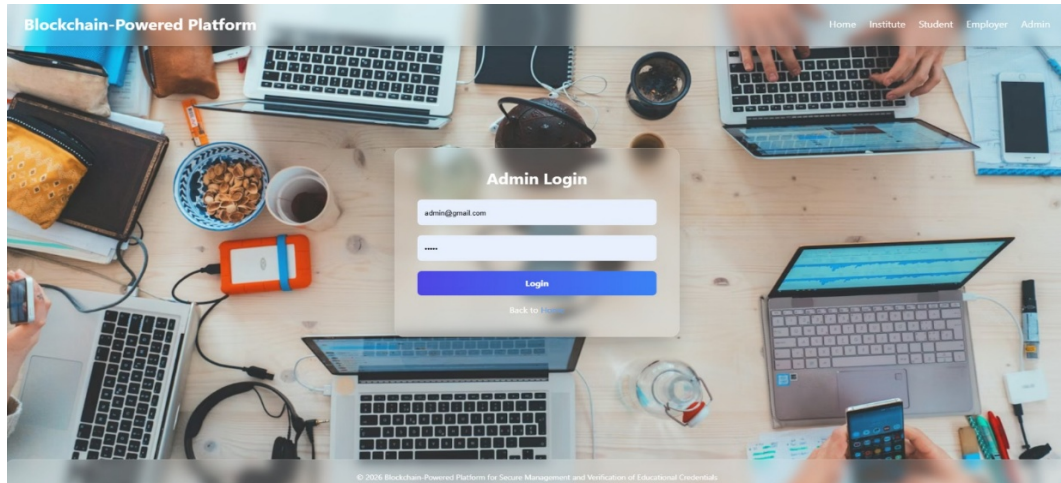


Fig 3: Admin login Page

This screen illustrates the admin login interface of the blockchain-powered credential management platform, designed to provide secure access for system administrators. It features a simple and focused layout with input fields for email and password, allowing authorized users to authenticate and manage system operations.

Student Registration Page:

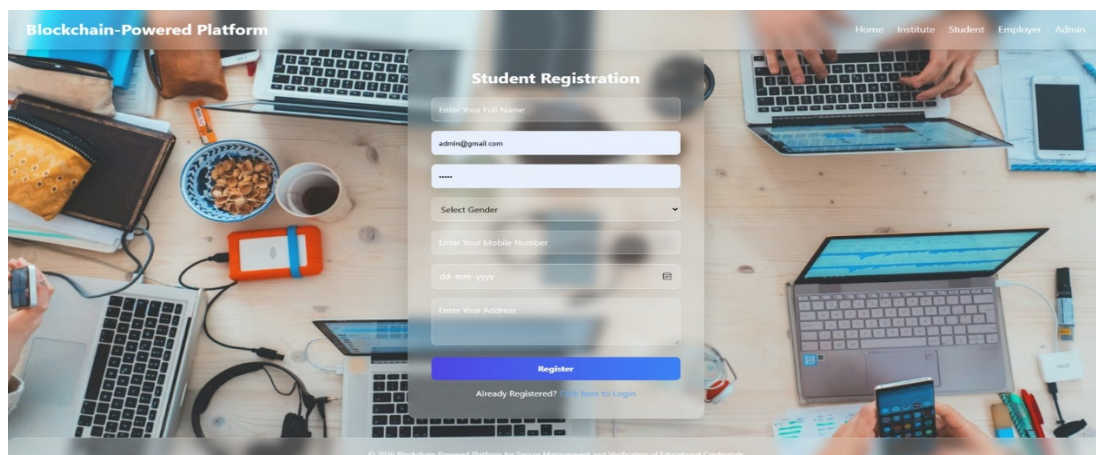


Fig 4: Student Registration Page:

This screen displays the student registration interface of the blockchain-based credential platform, It includes input fields for personal information such as name, email, password, gender, contact number, date of birth, and address, ensuring comprehensive data collection for account creation.

Certificate Requests for Employee



Fig 5: Certificate Requests for Employee

This screen showcases the employer verification interface of the blockchain-based credential platform, designed to simplify and secure the process of validating educational certificates. It displays a structured table containing key details such as student ID, certificate ID, hash value, request time, and verification status.

Student certificate access page:

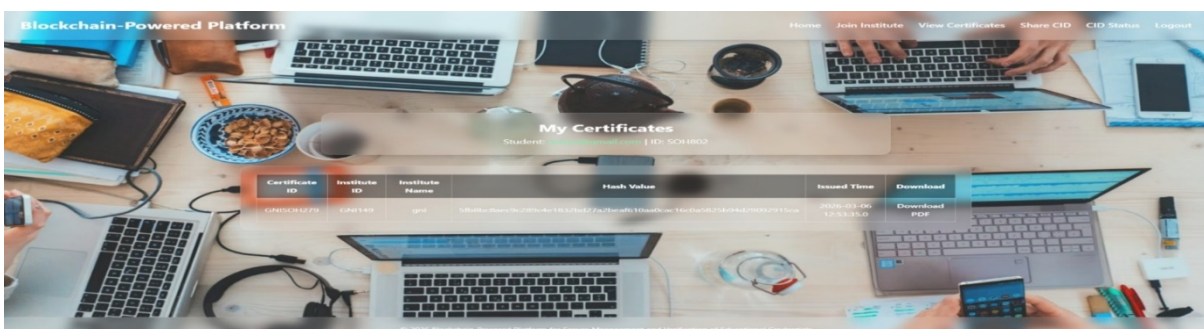


Fig 6: student certificate access page:

This interface represents a personalized certificate dashboard within a blockchain-based system, allowing users to conveniently access and manage their academic records. It displays key information such as certificate ID, issuing institute details, a unique hash value for authenticity, and the issuance date, all organized in a clear and structured format.

Student certificate page:



Fig 7: student certificate page

This document represents a formal certificate of completion, confirming that a student has successfully finished a Bachelor of Technology degree in Computer Science and Engineering from the specified institution. It clearly includes key identifiers such as the student ID and institute ID, ensuring accurate verification and traceability.

VII. CONCLUSION

In conclusion, the proposed system offers a modern and reliable way to handle educational credentials securely and transparently. By using blockchain, IPFS, and smart contracts, it ensures that every certificate is genuine, traceable, and protected from tampering. This not only speeds up verification but also reduces the manual effort required by institutions and employers. Overall, the system creates a trusted digital space where students, universities, and organizations can connect easily, making the management of academic records simpler, safer, and more efficient.

VIII. FUTURE ENHANCEMENT

Future enhancements include improving scalability, usability, and integration while leveraging smart contracts for automation and AI-based techniques for stronger security and analytics.

REFERENCES

- [1] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," 2019, arXiv:1910.04622.
- [2] C.-S. Hsu, S.-F. Tu, and P.-C. Chiu, "Design of an e-diploma system based on consortium blockchain and facial recognition," *Educ. Inf. Technol.*, vol. 27, no. 4, pp. 5495–5519, Jan. 2022, doi: 10.1007/s10639-02110840-5.
- [3] N. Smolenski. (2016). *Academic Credentials in an Era of Digital Decentralization*. Learn. Mach. Res., Anaheim, CA, USA. [Online].
- [4] C. Johnson, "Credentialism and the proliferation of fake degrees: The employer pretends to need a degree; the employee pretends to have one," *Hofstra Labor Employ. Law J.*, vol. 23, no. 2, pp. 1–75, Aug. 2006.
- [5] F. R. Vidal, F. R. Gouveia, and C. Soares, "Blockchain application in higher education diploma management and results analysis," *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 6, pp. 871–882, Dec. 2020, doi:10.25046/aj0506104.
- [6] M. E. Effiong, "A framework for the adoption of blockchain technology in academic certificate-verification systems: A case study in Nigeria," M.S. thesis, Dept. School Information Technology, Tallinn Univ. Technol., Tallinn, Estonia, 2020.
- [7] S. O.Ghazali, O. Rana, and M. Ehsan, "Blockchain based framework for educational certificates verification," *J. Crit. Rev.*, vol. 7, no. 3, pp. 79–84, Mar. 2020, doi: 10.31838/jcr.07.03.13.
- [8] A. Ezell and J. Bear, *Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas*. New York, NY, USA: Prometheus, 2012.
- [11] Citizen. (2017). *Your Bus. is Our Business: Fake Certificates in TZ Economic Equation*. Accessed: Jun. 9, 2022.
- [10] P. Sengati and E. Kitinya, "An inquiry on strategies to mitigate fake certificates: A case of Tanzania," *Int. J. Develop. Res.*, vol. 8, no. 12, pp. 24875–24881, Dec. 2018.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152