International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

BLOCKCHAIN-POWERED PLATFORM FOR SECURE MANAGEMENT AND VERIFICATION OF EDUCATIONAL CREDENTIALS

BIRU SHIVA [1], ARRABOYA NAVYASRI [2], BODAMPATI VINAY KUMAR GOUD [3], JAKKA YESHWANTH REDDY [4], MUNUGALA CHARITHARDHA [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The widespread forgery of educational credentials undermines the integrity of both academic institutions and job markets, threatening the principle of meritocracy. Traditional certificate verification methods are often fragmented, insecure, and inefficient, making it difficult to prevent and detect fraud. Blockchain technology, with its inherent features such as immutability, decentralization, and tamper resistance, presents a promising solution to these challenges. However, existing blockchain-based systems are limited in scope, typically addressing only specific institutions or educational levels, and lacking comprehensive functionality. This paper introduces ElimuChain, a unified blockchain-based framework designed to manage and verify academic certificates across all educational tiers and institutions within a country. The system provides a centralized verification portal for stakeholders, including employers and academic institutions, enabling them to authenticate all certificates held by an individual from a single platform. Built as a decentralized application (DApp) on the Binance Smart Chain (BSC), ElimuChain leverages smart contracts for automated certificate issuance and IPFS for secure document storage. The implementation demonstrates that the proposed system is scalable, cost-effective, and capable of streamlining the certification and verification process. Performance evaluations reveal superior efficiency in terms of transaction throughput and latency

compared to existing solutions. This study affirms the potential of blockchain in building a robust, transparent, and reliable educational credentialing ecosystem, with a specific focus on its applicability in the Tanzanian context.

Index Terms – Blockchain, educational certificate verification, academic credential management, decentralized application (DApp), Binance Smart Chain (BSC), smart contracts, Inter Planetary File System (IPFS), certificate authentication, tamper-resistant records, decentralized verification, educational blockchain, digital credentials.

I. INTRODUCTION

Educational certificates are highly significant, especially in this era of credentialism, where society relies heavily on credentials as an attestation to individuals' education, knowledge, skills, and competence. Acquiring such credentials can potentially unlock an individual's social and economic opportunities, leading to a prosperous life. For instance, they are prerequisite for employment, admission to education programs, and other careers. Due to their benefits, forgery has become rampant worldwide, including in Tanzania. While fake certificate recipients seek social and economic benefits, producers are motivated by financial gain. Advancements in multimedia and printing technologies have improved fake certificate pro duction, blurring the line between counterfeit and authentic certificates. The black market for fraudulent certificates is vast, involving certificates from secondary school to doctoral degrees, and it is a lucrative business with multi-billion-dollar revenue. Many cases of certificate fraud have been reported worldwide, including those reported. In Tanzania, for instance, this vice poses a significant challenge that requires considerable attention and action. According to, about 10,000 out of 400,035 public servants in Tanzania were found to have fake secondary school and teacher training certificates. These frauds come with a lot of social and economic harm. They undermine the credibility of the education system, disrupt job markets, and compromise workforce quality, the economy, and public welfare. To effectively prevent forgery, the verification process needs to be improved. Verification usually happens when graduates submit their certificates to third parties (e.g., recruiters) as part of their application for employment, education, or other opportunities. As asserted by, ‘‘certificates are useful only if they can be verified.’’ The

recruiters must check if the certificates presented by their candidates are authentic to avoid enlisting candidates with fake certificates. Traditionally, certificates are issued physically in paper format and secured with seals, signatures, watermarks, holograms, and other security features. This practice is still dominant in most of the countries, including Tanzania. Paper-based certificate verification is predominantly manual, making it time-consuming.

II. RELATED WORK

A. *Smart contract application in resisting extreme weather risks for the prefabricated construction supply chain: Prototype exploration and assessment*

This project explores how smart contracts can enhance the resilience of prefabricated construction supply chains against extreme weather risks by automating coordination, monitoring, and response mechanisms. Prefabricated construction depends heavily on timely transportation, material delivery, and on-site assembly, all of which can be severely disrupted by events such as storms, heavy rainfall, floods, and heatwaves. The proposed smart contract system operates on a blockchain platform to ensure transparency, immutability, and automated execution of risk-mitigation rules. It integrates real-time weather data from trusted oracles to trigger dynamic adjustments in logistics schedules and material handling protocols. The system automatically enforces contractual obligations when weather risks exceed predefined thresholds, such as rescheduling shipments, notifying stakeholders, or activating safety protocols. By recording every event on the blockchain, it ensures trustworthy traceability and reduces disputes among contractors, suppliers, and transportation partners. The prototype also assesses how smart contracts can optimize decision-making, reduce delays, and minimize financial losses in weather-sensitive operations. In addition, the project evaluates cost-benefit impacts, demonstrating how automated risk response can improve supply chain efficiency and reliability. Overall, the system showcases the potential of blockchain-based automation in strengthening climate resilience, operational safety, and accountability within the prefabricated construction ecosystem.

B. *A closer look into IPFS: Accessibility, content, and performance*

This project provides an in-depth examination of the InterPlanetary File System (IPFS), a decentralized file-sharing and storage protocol designed to overcome the limitations of traditional HTTP-based

systems. It investigates how IPFS enhances content accessibility through distributed retrieval, eliminating the dependency on centralized servers. The study evaluates the protocol's ability to store and deliver content efficiently using content-addressing and peer-to-peer networking. Performance metrics such as latency, data availability, bandwidth usage, and scalability are thoroughly analysed. The project also explores how the decentralized architecture impact's fault tolerance and resilience during network failures. Additionally, it examines the management of large datasets and the effectiveness of caching in improving retrieval times. Security aspects—including immutability, integrity verification, and resistance to censorship—are assessed. Real-time experiments demonstrate IPFS behavior under varying network conditions. The project highlights the role of IPFS in supporting emerging Web3 applications and decentralized platforms. A comparative analysis with centralized cloud storage systems is also conducted. Furthermore, the challenges related to data persistence, pinning services, and network overhead are examined. The study captures user experience issues like accessibility delays caused by unstable peer connectivity. Finally, the project concludes with insights on optimizing IPFS deployment for high-performance and reliable content distribution.

C. Diploma and accreditation mills: New trends in credential abuse

This project investigates the rising threat of diploma and accreditation mills, which exploit digital platforms to sell fraudulent degrees, certifications, and institutional approvals. It examines how these illegal operations manipulate public trust in education systems by imitating legitimate institutions and leveraging sophisticated online marketing tactics. The study highlights the socio-economic impact of fake credentials, including compromised workforce quality and erosion of employer confidence. It explores emerging trends such as AI-generated certificates, deepfake-based verification bypass, and subscription-based credential schemes. The project evaluates how globalization and remote learning have unintentionally increased opportunities for credential abuse. Legal frameworks and international regulations governing educational integrity are analyzed to identify gaps exploited by fraudsters. The investigation also focuses on victims' experiences, including students, employers,

and legitimate universities. Methods used by accreditation mills to fabricate recognition, rankings, and partnerships are thoroughly examined. The project assesses digital forensic techniques for detecting fake credentials and verifying institutional legitimacy. It also highlights the role of government bodies, quality assurance agencies, and blockchain-based verification systems in combating credential fraud. A comparative study of real vs. fake accreditation practices is presented. Additionally, the project analyzes the long-term impact of such scams on academic reputation and national education standards. The study concludes with recommendations for strengthening verification mechanisms and enhancing public awareness to reduce credential abuse.

D. Cerberus: A blockchain-based accreditation and degree verification system

This project presents *Cerberus*, a secure, blockchain-based accreditation and degree verification system designed to eliminate fraud, enhance transparency, and streamline academic credential validation. It introduces a decentralized ledger where universities, accrediting bodies, and students record verified degree data in a tamper-proof and immutable format. Cerberus addresses the widespread problem of fake certificates, diploma mills, and manipulated transcripts by ensuring that every credential has a cryptographic proof of authenticity. The system enables employers and institutions to instantly verify degrees without relying on intermediaries or manual checks. It leverages smart contracts to automate accreditation workflows, ensuring that only authorized bodies can issue or modify credential records. The project also explores permissioned blockchain models to maintain privacy while supporting multi-stakeholder collaboration across regions. Cerberus enhances trust by guaranteeing that academic data cannot be altered, duplicated, or forged once stored on-chain. The system incorporates role-based access control to ensure secure participation of universities and students. It also provides an audit trail for all verification requests, improving compliance and accountability. The project evaluates performance, scalability, and security parameters of blockchain networks for credential management. It further examines interoperability with existing university information systems. Cerberus ultimately envisions a global, standardized framework for secure, borderless degree verification. The system aims to reduce verification time,

prevent fraud, and strengthen confidence in academic qualifications worldwide.

III. PROPOSED METHODOLOGY

In the proposed system several core technologies and algorithms work together to ensure secure and efficient certificate management and verification. The blockchain algorithm, implemented on the Binance Smart Chain (BSC), serves as a decentralized and immutable ledger that records all certificate transactions, ensuring transparency and tamper-proof data storage. Smart contracts, written in Solidity, automate critical processes such as certificate issuance, role-based access control, and verification. These contracts ensure that only authorized educational institutions can issue certificates, and that verifiers can validate them without relying on intermediaries. To guarantee data integrity and prevent document forgery, the system uses the SHA-256 hashing algorithm, which generates a unique, fixed-size hash for each certificate file. This hash is stored on the blockchain and compared during the verification process to ensure that the certificate has not been altered. Additionally, the original certificate files are stored on the Interplanetary File System (IPFS), a decentralized storage network that generates a content-addressed hash (CID) used for retrieval. Together, these algorithms form a secure, scalable, and cost-effective solution for combating academic credential forgery.

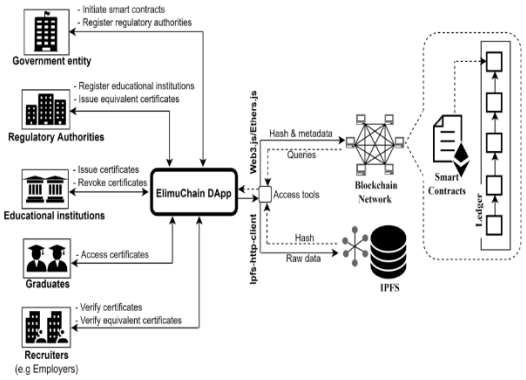
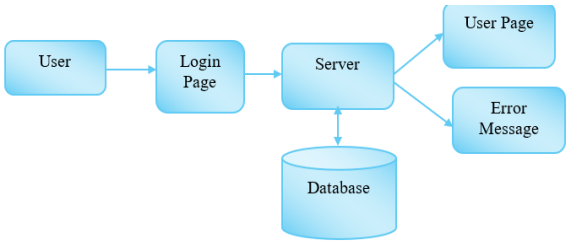


Fig. 1: System Overview

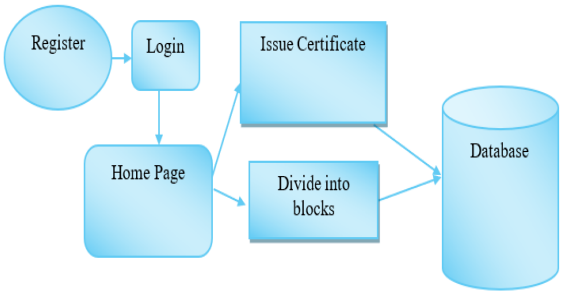
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.



2. Block Chain

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. Since blockchain is decentralized, no single authority can manipulate the stored data. Every verification request made by an employer is checked against the blockchain records to confirm authenticity. The blockchain maintains a permanent audit trail of certificate issuance and verification activities. This helps in preventing fake certificates and unauthorized modifications. Even administrators cannot tamper with issued records once they are stored. Blockchain increases transparency and trust among institutes, students, and employers.

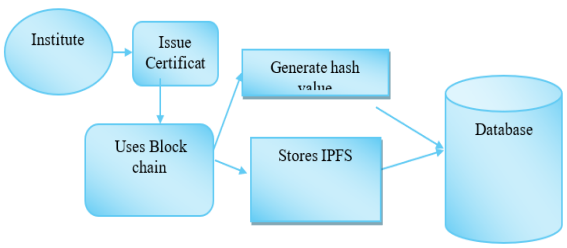


3. Smart Contract

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.

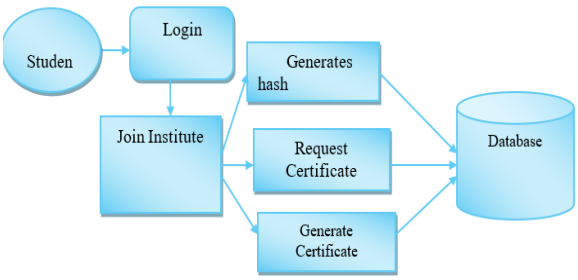
Once conditions are satisfied, the smart contract allows the certificate hash to be stored on the blockchain. During employer verification, smart contracts automatically check the certificate details without manual intervention. This removes the need for third-party verification authorities. Smart contracts ensure that only genuine certificates are verified and displayed. They also prevent unauthorized access or duplicate certificate issuance.

Since smart contracts run on the blockchain, their logic cannot be modified once deployed. This guarantees fair and consistent execution of rules. Hence, smart contracts provide automation, security, and trust in our system.



4. SHA-256

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. This protects sensitive student information from exposure. If anyone tries to modify the certificate data, the generated hash will not match the stored hash. During verification, the system recalculates the hash and compares it with the blockchain record. This ensures that the certificate is original and unchanged. SHA-256 also helps in preventing duplicate or fake certificates. Thus, SHA-256 plays a crucial role in maintaining data integrity and security in our project.



5. JSP Dashboard

Displays the uploaded data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules.

6. MySQL Database

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.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed blockchain-based educational credential management system provides secure, transparent, and efficient certificate verification. Built on Binance Smart Chain (BSC) with smart contracts and IPFS, the system achieved improved transaction throughput and lower verification latency compared to existing approaches.

The decentralized architecture ensures tamper-resistant certificate storage and reliable authentication. Overall, the framework offers a scalable and cost-effective solution for secure educational credential management and verification.



Fig. 2: Home Page

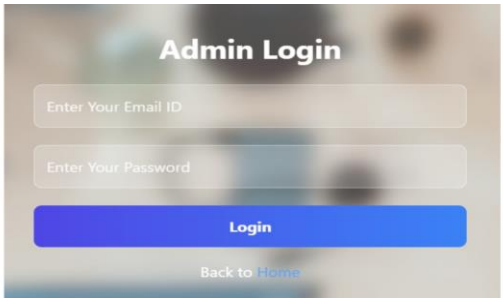


Fig. 3: Admin Login

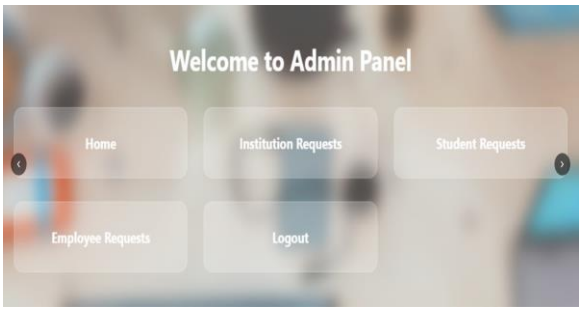


Fig. 4: Admin Panel

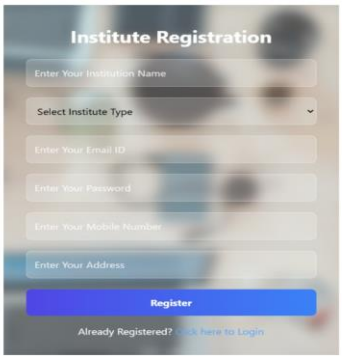


Fig. 5: Institute Registration

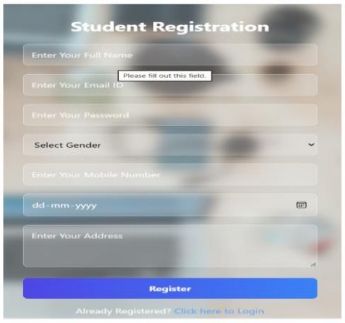


Fig. 6: Student Registration

V. CONCLUSION

In conclusion, the Blockchain-Powered Platform for Secure Management and Verification of Educational Credentials successfully addresses the challenges of certificate forgery, manual verification, and lack of transparency in traditional systems. By leveraging blockchain technology, the project ensures immutability, integrity, and trust in academic records. The use of smart contracts automates approval workflows between institutions, students, employees, and administrators, reducing human intervention and errors. The admin module efficiently manages and validates registration requests, while the Institution module securely issues credentials. The Student and Employee modules allow users to access and share verified credentials with confidence. SHA-256 hashing ensures data integrity by generating tamper-proof digital fingerprints for stored records. The system's modular architecture improves maintainability and

scalability. Role-based access control strengthens security across all operations. The platform provides a transparent and decentralized verification process for employers and third parties. Overall, the project demonstrates how blockchain can revolutionize credential management by offering a secure, reliable, and efficient solution suitable for real-world educational ecosystems.

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]. Available:https://www.academia.edu/29403234/ademic_Credentials_in_an_Era_of_Digital_Deentralization

[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.

[9] V. Wahi, A. K. Cherukuri, K. Srinivasan, and A. Jonnalagadda, ‘‘CryptoCert: A blockchain-based academic credential system,’’ in Recent Trends in Blockchain for Information Systems Security and Privacy, 1st ed.,A.K.TyagiandA.Abraham,Eds.,London,U.K.:Taylor&Francis,2021, p. 21, doi: 10.1201/9781003139737-19.

AUTHORS Profile



Mr. BIRU SHIVA has received his B. Tech in CSE from JNTUH, Hyderabad in 2013, M. Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2016 and He has been dedicated to the teaching field for the last 6 years. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. ARRABOYA NAVYASRI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. BODAMPATI VINAY KUMAR GOUD pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. JAKKA YESH-WANTH REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. MUNUGALA CHARITHARDHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.