ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1597

Academic Credential Verification System Using Blockchain

G Harika; Hareesh; Harshitha B H; Akash G A; Dr Hema N
Department of Information Science RNS Institute of Technology, Bengaluru

Abstract:- Despite their increased security, current centralized systems still have privacy, transparency, and service digitalization problems in higher education. This paper investigates how blockchain systems could be able to overcome these difficulties. It contrasts blockchain with centralized systems, emphasizing the challenges of platform adaption and data transport. Smart contracts are essential to the suggested blockchain architecture, which places an emphasis on the creation and verification of academic credentials. In order to show how the system may be used practically through testing in real-world situations, the paper describes the conceptual framework, architecture, and smart contract design.

Keywords:- *Blockchain Platforms, Smart Contracts, Conceptual Model, System Process Architecture, Decentralized System, Data Management, Higher Education Institution, Survey Paper.*

I. INTRODUCTION

In the digital age of today, confirming academic credentials is frequently a laborious, expensive, and ineffective procedure. Forgery, verification delays, and a lack of a centralized system are problems with traditional systems for storing, issuing, and confirming academic credentials. These issues can be resolved by blockchain technology, which is decentralized, unchangeable, and transparent. By storing academic credentials on a blockchain, this project suggests creating a Blockchain-based Academic Credentials Verification System that guarantees immediate verifiability, validity, and integrity.

Blockchain guarantees that, once being granted, a credential is permanently entered into a decentralized ledger that can be accessed by everyone for verification without the need for a central authority. This approach benefits companies, students, and educational institutions by offering a more efficient, transparent, and safe method of issuing and confirming academic credentials.

II. LITERATURE SURVEY

A review of the literature is essential because it looks at different analyses and studies that have been done in the area of interest. It explores the results that have previously been released, taking into account various project characteristics and the project's scope. A literature review's main goal is to examine the project's history in detail, pointing out flaws in the current setup and highlighting concerns that still need to be addressed. The subjects addressed not only shed light on the project's history but also highlight the issues and shortcomings that motivated the project's conception and remedy proposals.

- *Verifying Certificate with Public Key Infrastructure:*

This study looks into Blockcerts, a blockchain-based protocol that verifies digital academic credentials in accordance with the Open Badges standard. The study outlines the protocol's weaknesses with respect to Blockcerts, particularly attacks involving impersonation. It was demonstrated that an attacker might generate a fake certificate that could not be distinguished from the authentic ones by the present validation process by issuing a false issuer profile. To address the same issue with relation to the security of academic credential certification, the authors propose countermeasures such the use of a Public Key Infrastructure (PKI) or decentralized identification system.

- *Hyperledger Fabric for Student Certificate Management:*

In order to facilitate the issue, verification, and exchange of academic records, this study examines a blockchain-based architecture for managing and exchanging student certifications. It makes use of Hyperledger Fabric to address current concerns about immutability, privacy, and decentralization. It does, in fact, automate conventional, laborious procedures when certifications are being issued or verified. With an average issuance time of 1.9 seconds and a latency of 1.4 seconds, the system's performance is based on how long it takes to issue and validate the e-certificates. Compared to conventional techniques, smart contracts will provide secure and regulated data transfer, increasing efficiency.

- *Blockchain-based solutions for Higher Education using EduCTX:*

This study is on blockchain-based solutions in HE, with an emphasis on changing current procedures like student credential management and diploma verification. In order to do this, it divides solutions into two categories: institution-centric and student-centric. The majority of the efforts are geared toward the former. EduCTX is one of the primary options discussed. This mechanism for handling student credentials is built on blockchain technology. Nevertheless, the report also points out several drawbacks, such privacy issues and difficulties integrating blockchain technology with current systems. In this regard, the authors provide a concept for using decentralized systems, such as EduCTX, to guarantee more efficient and safe educational credentialing, preventing certificate forgeries using transparent and immutable blockchain.

- *CredSec: A Secure Credential Management System for University Adoption Based on Blockchain Technology:*

The study suggests CredSec, a Blockchain-based solution for safe credential administration and storage in academic institutions. To protect the confidentiality and integrity of student credentials, the system uses a modified two-factor encryption, or m2FE, technology that combines RSA cryptography with DNA encoding. It really uses a decentralized approach utilizing a blockchain server and a local dedicated server to address such important issues as credential manipulation and illegal access. Here, the blockchain's usefulness is utilized to make something impenetrable; the writers will assume that the verification method is safe.

- *A Novel Blockchain-based Education Records Verification Solution:*

This study will make advantage of the blockchain's decentralized and impenetrable features to allow individuals to store and share educational certificates without needing to go via conventional organizations. The foundation for ensuring that records are protected by only those with access and modification permissions will be formed by the smart contract and the SHA-256 hashing algorithm. Its primary goal is to reduce expenses and boost operational efficiency while providing lifetime credential management and assistance for the demands of rapidly expanding online and decentralized learning platforms, such as MOOCs. By doing this, the approach overcomes the conventional privacy and security issues of centralized systems and benefits from scalable safe data sharing.

- *Decentralization of Credential Verification System using Blockchain:*

The study draws attention to the drawbacks of the conventional centralized systems-cumic. As a result, they are subject to modification and forging and are laborious in nature, which gives rise to the world of fraudsters. Instead, the new system will develop a DAPP (decentralized application) using blockchain technology. Digital certificates will be issued, checked, and validated in this safe way. Since the system ensures the integrity and authenticity of certificates, fake versions are difficult to get. It uses smart contracts and cryptography techniques to do this. It may be created with languages like Solidity and technologies like Ethereum or Hyperledger to provide the speed and security required for a method of academic credential verification.

- *Blockchain-Based Certificate Authentication System with Enabling Correction:*

This document differs from Blockcerts in that it lacks the error-correction feature. By utilizing the immutability and decentralization that are intrinsic to blockchain technology, certificate fraud is prevented, and evidence is securely and permanently recorded via quick and transparent authentication methods. Furthermore, the approach makes it possible for authorized organizations to fix errors in certificates, increasing flexibility without sacrificing integrity. Its disadvantage, meanwhile, is the intricacy of managing two separate blockchains—one for accounting adjustments and the other for certificate storage—which raises the bar for processing demands, introduces technological challenges, and may cause scalability problems.

- *Validating Certificate using Bloom Filters:*

In order to store and distribute certificate revocation data, the method combines Bloom filters with the decentralized and unchangeable characteristics of blockchain technology. It is compatible and scalable as it incorporates into the X509 certificate structure without changing the existing web standards. Comparing the aforementioned method to others like Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP), it offers several benefits, including increased security, robustness against single point failure, and quicker revocation checks. The primary drawbacks are the potential for false positives as a result of the Bloom filter and the computational burden associated with managing blockchain data. However, our suggested approach outperforms existing PKI revocation strategies in terms of security and speed.

- *AES Encryption for Validating the Certificate:*

The paper discusses an application on blockchain for academic certificate verification and validation. Smarts contracts in Ethereum, along with AES encryption, would ensure that the certificates are distributed and verified safely. The deployment on blockchain ensures a decentralized, tamper-proof record. Three major applications would be integrated: the verification app, a university interface to issue certificates, and an accreditor interface to check universities' accreditation status. It avails secure certificate storage by encrypting, access via passphrase while delivering on privacy and confidentiality. These benefits include low administrative barriers, instant verification, and security improvements. Some of the downsides of this approach include costs on blockchain transactions; also, it becomes cumbersome for managing keys and loss of data because encryption keys can be easily misplaced.

- *VECefblock-BlockChian Based Solution for Fake Certificate Prevention in Vietnam:*

In order to address the issue of phony certificates in Vietnam, the article will present VECefblock, a blockchain-based certificate authentication system architecture. In this sense, the Hyperledger Fabric-based solution uses smart contracts, anti-forgery methods, and a decentralized architecture to guarantee the security and immutability of educational credentials and verification procedures. As a result, this approach guarantees increased confidence and openness in the certification process as it relates to educational institutions. Better data security, less fraud, effective verification procedures, drawbacks High resource requirements may place restrictions on how well these transactions operate when there are a lot of them.

A comprehensive overview of prior blockchain-based solutions in the field of academic credential administration and verification is provided in the literature study. This aids in synthesizing the earlier research without taking certain unrelated data into account. Proposals like PKI integration and smart contracts may be made in order to address the critical issues with the current systems, which include processing inefficiencies and vulnerability to impersonation attacks. This review covers a number of frameworks, including Blockcerts, Hyperledger Fabric, EduCTX, and others, providing the reader with an overview of some of the most innovative approaches and technologies in the industry In addition to highlighting the state of the subject, it points out some gaps as though creating opportunities for more research and takes the area in new directions.

III. OBJECTIVES

- By utilizing blockchain technology, the project seeks to establish a decentralized, impenetrable system that guarantees academic credentials are safely kept and incapable of being changed or falsified.
- The system aims to significantly cut down on the time and expense involved in manual or third-party credential checks by automating the verification process, resulting in quicker and more effective verification.
- 3.By including QR codes, the verification process is made simpler and more accessible to users with different levels of technological proficiency, such as employers, educational institutions, and students.

IV. PROPOSED SYSTEM

By smoothly combining the conventional hash address approach with a QR code, the suggested system guarantees an improvement in the academic credential verification procedure. Following issuance, educational institutions generate a distinct hash address along with a QR code that embeds the address. To guarantee imperishability and transparency, all certificate-related data is securely kept on a blockchain ledger. Verifiers may now quickly confirm certificates by using a smartphone to scan QR codes, which instantly connects the device to the blockchain and gets and compares certificate data. The certificate is valid as long as the data that was obtained matches the information included in the QR code. Instead of filling out laborious paper-based information, this new approach allows for faster scanning, which increases usability. This will ensure strong security and efficiency in the verification process and increase levels of trust over academic credentials.

V. ADVANTAGES OF PROPOSED SYSTEM

- The verifiers find validation easier because to that QR code.
- Blockchain storage lowers the risk of fraud and guarantees immutability.
- Verification streamlined for saving time both by the institutions and verifier.
- International recognition of a degree is promoted by the use of blockchain technology and QR codes, which enable verification from any location in the globe.

VI. VI.PROPOSED METHODOLOGY

- *System Architecture Review:*

The process starts with a thorough literature evaluation of the body of research on blockchain technology and its uses in academic accreditation and credential verification. Review of Literature: The literature will concentrate on capturing the subtle differences between different methods, which might include incorporating cryptographic techniques, smart contracts, non-fungible tokens, and QR codes into credential verification systems.

- *System Design and Architecture:*

The proposed system's system architecture will be thoroughly explained, outlining the ways in which smart contracts, NFTs, QR codes, and cryptographic techniques all function together inside the blockchain framework. By doing this, it would be possible to clarify the intended system's functionality and data flow while maintaining the highest standards of security and usability.

- *Analysis of Security:*

An analysis of the system's security features will be conducted. To make sure the system has resisted all kinds of assaults and security flaws, a high-level study is carried out on sophisticated cryptological techniques including public-private key encryption, multi-factor authentication, and SHA-256 hashing.

- *Assessment of Performance:*

Measurements of verification speed, accuracy, and user experience are all part of the proposed system's performance evaluation. Through evaluation, it will demonstrate the viability and effectiveness of blockchain-based credential verification while highlighting areas in need of development.

VII. SYSTEM ARCHITECTURE

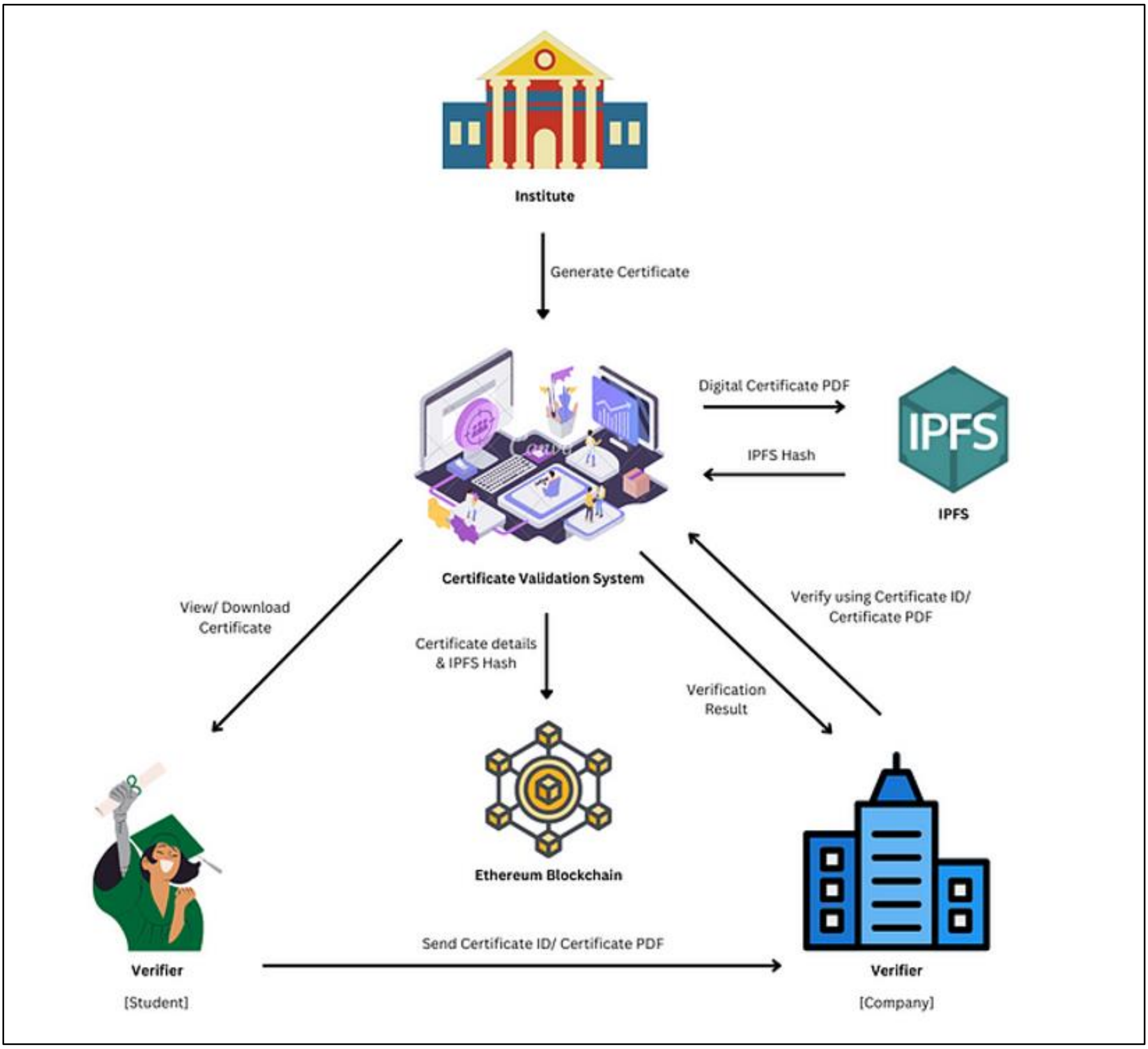
Institute
Generate Certificate
Digital Certificate PDF
IPFS
IPFS Hash
IPFS
Certificate Validation System
View/ Download Certificate
Certificate details & IPFS Hash
Verification Result
Verify using Certificate ID/ Certificate PDF
Ethereum Blockchain
Send Certificate ID/ Certificate PDF
Verifier
[Student]
Verifier
[Company]

Fig 1 System Architecture

VIII. CONCLUSION

According to the survey's findings, the suggested Blockchain-based Academic Credentials Verification System provides a strong, decentralized way to overcome the drawbacks of conventional academic credential verification procedures. Without the need for centralized authority, organizations may safely issue credentials that are instantaneously verifiable, tamper-proof, and accessible worldwide by utilizing blockchain technology. This improves the verification process's speed and security while also fostering confidence between companies, students, and institutions. Adoption of the system might revolutionize the management and verification of academic qualifications, saving money, time, and improving transparency

REFERENCES

[1]. M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, “EduCTX: A Blockchain-Based Higher Education Credit Platform,” IEEE Access, vol. 6, pp. 5112–5127,2018,doi: 10.1109/ACCESS.2018.2789929.

[2]. CredSec: A Blockchain-based Secure Credential Management System for University Adoption by Md. Ahsan Habib Md. Mostafijur Rahman Nieb Hasan Neom.

[3]. Yin et al., “SmartDID: A Novel Privacy-Preserving Identity Based on Blockchain for IoT,” IEEE Internet Things J., vol. 10, no. 8, pp. 6718–6732, Apr. 2023,

doi: 10.1109/JIOT.2022.3145089.

[4]. A Preliminary Review of Blockchain-based Solutions in Higher Education Aida Kamiˇsali´, Muhamed Turkanovi´ Saˇsa Mrdovi´ and Marjan Heriˇcko

[5]. Towards a blockchain-based certificate authentication system in Vietnam Binh Minh Nguyen, Thanh-Chung Dao and Ba-Lam Do

[6]. Blockchain-based student certificate management and system sharing using hyperledger fabric platform Rana F. Ghani , Asia A. Salman , Abdullah B. Khudhair , Laith Aljobouri

[7]. EUNICERT: ETHEREUM BASED DIGITAL CERTIFICATE VERIFICATION SYSTEM Trong Thua Huynh1 , Dang-Khoa Pham

[8]. Blockchain-based Solutions for Education Credentialing System: Comparison and Implications for Future Development Zoey Ziyi Li Joseph K. Liu Jiangshan Yu Dragan Gasevic

[9]. Blockchain-Based Certificate Authentication System with Enabling Correction Md. Mijanur Rahman, Md. Tanzinul Kabir Tonmoy, Saifur Rahman Shihab, Riya Farhana

[10]. Technologies, X. (2017) Blockchain Imperative for Educational Certificates. Xanbell Technologies.

[11]. Haber, S. and Stornetta, W.S. (1991) How to Time-Stamp a Digital Document. Springer Berlin Heidelberg, 437-455.

[12]. Garg, R. (2021) Blockchain Ecosystem for Education & Employment Verification. Proceedings of 13th International Conference on Network & Communication Security (NCS 2021), Toronto, 25-26 September 2021.

[13]. Share, E., Memorable, M. and They, L. (2014) Fifty-Eight Percent of Employers Have Caught a Lie on a Resume.

[14]. Paraide, P., Owens, K., Muke, C., Clarkson, P., Owens, C.: Before and after independence: Community schools, secondary schools and tertiary education, and making curricula our way. In: Mathematics Education in a Neocolonial Country: The Case of Papua New Guinea, pp. 119–148. Springer, ??? (2023)

[15]. Gopal, N., Prakash, V.V.: Survey on blockchain based digital certificate system. International Research Journal of Engineering and Technology (IRJET) 5(11) (2018)

[16]. Monrat, A.A., Schel´en, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 7, 117134–117151 (2019)

[17]. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Computing Surveys (CSUR) 52(3), 1–34 (2019)

[18]. Chatterjee, R., Chatterjee, R.: An overview of the emerging technology: Blockchain. In: 2017 3rd International Conference on Computational Intelligence and Networks (CINE), pp. 126–127 (2017). IEEE

[19]. Benet, J.: Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561 (2014)

[20]. Kumar, R., Tripathi, R.: Implementation of distributed file storage and access framework using ipfs and blockchain. In: 2019 Fifth International Conference on Image Information Processing (ICIIP), pp. 246–251 (2019). IEEE

[21]. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: Blockchain challenges and opportunities: A survey. International journal of web and grid services 14(4), 352–375 (2018)