Academic Certificate Authentication System

Keerthana K[#1], Pratiksha Suresh Baddur[#2], Rajeshwari R[#3] , Rohini Bhat M.R[#4],Prashanth Kumar K N[#5]

[#1234]Student , Department of CSE, Bangalore Institute of Technology , Bangalore , India

[#5] Professor , Department of CSE, Bangalore Institute of Technology , Bangalore , India

***Abstract*— The rise in academic credentials fraud poses significant challenges for educational institutions and employers as credentials become more difficult to verify and academic credentials become less trustworthy. Traditional verification methods are typically labor-intensive, expensive, and prone to fraud, highlighting the need for more secure and efficient solutions. This paper presents a blockchain-based approach to academic credentials verification that leverages the decentralized and immutable properties of blockchain technology to create tamper-proof and easily verifiable digital certificates.By leveraging the Ethereum blockchain and cryptographic hashing technology, the proposed system enables universities to issue certificates that can be directly authenticated by employers without the need for an intermediary.This method not only protects against fraud but also minimizes the time and cost of verification, resulting in a transparent and scalable framework for academic documentation. This blockchain framework can be fully deployed across all educational institutions, providing a secure and future-proof solution for verifying digital credentials, thereby strengthening trust in academic credentials.**

***Keywords*:**Academic credentials, Blockchain technology ,Ethereum blockchain , Cryptographic hashing , Digital certificates

I. INTRODUCTION

Academic credentials are crucial for confirming a person's educational accomplishments, skills, and knowledge. They are important in professional environments since employers depend on these documents to make well-informed hiring choices. Nevertheless, the increasing occurrence of fake academic certificates erodes the confidence placed in these qualifications, presenting significant risks for organizations and educational institutions. Studies indicate that millions of counterfeit degrees exist globally, allowing unqualified individuals to obtain jobs that necessitate verified expertise. Conventional methods for credential verification, which usually rely on centralized databases and manual procedures, tend to be expensive, time-consuming, and susceptible to fraud. This lack of efficiency highlights the necessity for a more secure, scalable, and effective solution.

Blockchain technology presents a groundbreaking method for tackling these issues. Originally created to facilitate decentralized cryptocurrencies, blockchain is now acknowledged for its potential in areas that demand secure and transparent data management. The distributed ledger system of blockchain guarantees that every entry is authenticated and maintained across a decentralised network, which significantly increases the data's resistance to tampering. Each transaction recorded on the blockchain is unchangeable, resulting in a durable record that can only be modified with agreement from the entire network. This framework makes blockchain especially well-suited for secure and reliable data storage, rendering it an optimal solution for verifying academic credentials.

This article presents a blockchain-driven framework for validating academics qualifications, employing the Ethereum blockchain along with cryptographic hashing to produce secure digital certificates. In this framework,educational institutions generate digital certificates that are transformed into distinct hashes and recorded on the blockchain. Potential employers can verify these qualifications by checking the blockchain record, thereby removing the necessity for external verification services.As blockchain technology continues to expand across various industries, its use in academic verification offers significant potential for maintaining the integrity and availability of educational credentials

II. RELATED WORKS

The verification of academic credentials has been approached in multiple ways, with blockchain-based solutions gaining traction for their promise of data security and immutability. One prominent model is the study by Huynhet al. (2018), which proposed UniCert, a blockchain-based system designed to issue and verify digital certificates. UniCert demonstrates a practical application of blockchain for counteracting document fraud but is limited by its high verification times, making it less effective for academic settings that require quick validation processes.

Another significant work is EduCTX, introduced by Turkanovic et al. (2018), a platform using blockchain to establish a globally unified higher education credit system. EduCTX leverages blockchain for standardized academic credits, inspired by the European Credit Transfer and Accumulation System (ECTS). However, while it provides an efficient credit management framework, EduCTX does not address the broader need for academic certificate verification.

Electronics Health Records(EHRs) system applies blockchain for privacy preservation and secure data sharing in healthcare, ensuring data integrity. Although EHRs require high levels of privacy, this model is healthcare-specific and lacks adaptability for academic certification. Similarly, Chowdhury et al.(2018) developed a blockchain-based Personal Data Store for secure data sharing, focusing on privacy and access control.

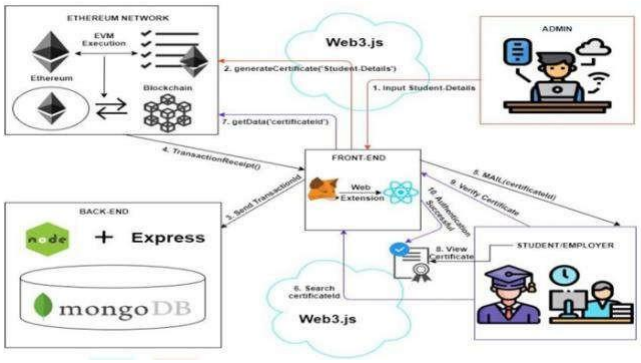
Saleh et al. (2020) proposed a Blockchain-Based Framework for Educational Certificates Verification, which identified security themes essential for document verification but did not provide an end-to-end solution for widespread academic usage. Additionally, Hyperledger Fabric, as described by Androulaki et al. (2018),introduced a flexible permissioned blockchain for secure transactions, though it lacks an optimized approach specifically for academic certificate verification.

III. PROPOSED SYSTEM

The suggested system utilizes blockchain technology to establish a secure, efficient, and tamper-proof approach. This innovative solution overcomes the shortcomings of conventional verification methods by substituting centralized, intermediary-dependent validation with a decentralized framework that promotes transparency and trust. By employing the Ethereum blockchain,educational institutions can issue digitalize certificates that are both immutable and verifiable by external parties,such as employers, without the need for intermediary services. Each certificate is hashed to generate a unique identifier that is recorded on the blockchain, ensuring that any alterations to the certificate are instantly identifiable.

A pivotal aspect of the proposed system is its capacity to enhance the verification process. Students are issued a digital version of their certificate along with a unique certificate ID. When seeking employment, they can provide this ID to potential employers, who can then verify the authentication of the certificate directly on the blockchain. This direct and decentralized verification method eliminates the delays typically associated with manual background checks, thereby serving as a significant asset for both students and employers. Moreover,the system features a user-friendly interface that simplifies access to certificate issuance and verification. The front end, developed using contemporary web technologies, includes distinct portals for students, institutions,and verifiers, each customized to meet the specific requirements of its users.

Regarding privacy, the system employs cryptographic hashing to store only the hash of the certificate on the blockchain, thereby safeguarding the security and integrity of personal data. Additionally, by decentralizing the management of certificates, the system lowers operational costs and improves data protection. Ultimately, this proposed system offers a dependable, accessible, and scalable solution to address the growing issue of academic credential fraud, establishing a new benchmark for secure academic documentation.



IV. EXISITING DRAWBACKS

Scalability: When managing massive volumes of data, both public and private blockchains may experience performance problems that result in sluggish processing times for high transaction volumes.

Integration Challenges: It might be challenging to smoothly integrate blockchain-based solutions into current academic systems since they sometimes require intricate interfaces.

Cost: Transaction fees and storage expenses might result in high operating costs.

Easy to Use: Without an intuitive interface, non-technical users like employers or even the students who are not familiar. They may find it difficult to browse or validate credentials.

Security flaws: Although blockchain is safe, certain attacks, such replay or Sybil, can still affect it.

Legal and Regulatory Concerns: Since the laws governing blockchain uses in education are still developing, there may be regulatory ambiguities surrounding NFTs for certification.

V. ALGORITHM - CERTIFICATE VERIFICATION

Input: The verifier's certificate ID or hash.

Output: "Certificate Verified" or "Invalid Certificate."

Actions to take:

Verifier's Frontend Input:

On the user interface (UI), the verifier displays the certificate ID or a hash of the certificate.
This is the first time that input is sent to the system for validation.

Backend Get Metadata for Certificates:

The back end looks up metadata in the local database or system using the supplied certificate ID or hash. Information like the

hash of the certificate and, if the certificate is saved on IPFS, its unique identifier (CID) may be included in the metadata.
For the certificate to be recognized and matched on the blockchain, this metadata is necessary.

Data from Blockchain-Fetch Certificates:

The blockchain calls a smart contract function, like getCertificate. This function returns the certificate data (hash and other pertinent information) after receiving the issuer's address or another unique identifier.
By taking this step, the backend is guaranteed to have access to the blockchain's official, unchangeable certificate data.

Verification of Hashes:

The hash or certificate ID supplied is compared with the hash that was extracted from the blockchain.
The system stops processing further and returns a "Invalid Certificate" result if the hashes do not match.
The submitted certificate details must match the official record, which is ensured by hash verification.

Verification of IPFS:

The CID (obtained in Steps 2 or 3) is used to retrieve the certificate document, which is stored on IPFS.
The integrity of the downloaded document is examined to make sure it corresponds with the original certificate information.
This step adds an additional degree of protection by confirming that the document hasn't been updated.

Show Verification Outcome:

If the IPFS verification and hash check are both successful, the system shows "Certificate Verified."
When inconsistencies are detected, the system shows "Invalid Certificate."
Justification:
The system stops processing further and returns a "Invalid Certificate" result if the hashes do not match.
The submitted certificate details must match the official record, which is ensured by hash verification.

VI. CONCLUSION

Although thousands of jobs are created every year, many graduates remain unemployed. One of the reasons is fake certificates, which lead to confidentiality issues such as students being unable to find employment. This system is designed to eliminate the impact of fake certificates by introducing digital certificates and providing a highly secure blockchain based storage architecture to store these certificates. As the data in the blockchain is immutable, academic certificates remain authentic and a web interface has been developed to allow quick access and authentication of certificates. Future improvements: This project implemented only academic certificates, but in the future we may extend it to commercial certificates as well.

VII. REFERENCE

[1]. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data.
[2]. Issuing and Verifying Digital Certificates with Blockchain : 2018 International Conference on Advanced Technologies for Communications - 978-1-5386-6542-8/18/$31.00 ©2018 IEEE.
[3]. Richard Nuetey Nortey , Li Yue, Promise Ricardo Agdedanu, Michael Adjeisah: Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain , 2019 the 4th IEEE International Conference on Big Data Analytics .
[4]. Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han and Paul Sarda: Blockchain as a Notarization Service for Data Sharing with Personal Data Store, 12th IEEE International Conference on Big Data Science And Engineering.
[5]. Block certs A project undertaken at Media Labs MIT, Available at https://www.blockcerts.org.
[6]. National Academic Depository (NAD) a project undertaken by MHRD, India.
[7]. Blockchain Based Framework For Educational Certificates Verification : Journal of critical reviews ISSN- 2394-5125 Vol 7, Issue 3, 2020.
[8]. Certificate validation using blockchain : IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020- 978-1-7281-7223-1/20/$31.00 ©2020 IEEE
[9] "Blockchain-Enhanced Academic Certificate" , Sumaiya Islam Mouno, Tasfia Rahman, IEEE , 2024.
[10] "Blockchain Based Trusted Management of Academic Credentials",Md. Suman Reza, Sujit Biswas, Abdullah Alghamdi,IEEE,2021.
[11] "Adoption of Blockchain Technology in Academic Certificate- Verification Systems" , Mercy Effiong, Alex Norta, Chibuzor Udokwu, Marie Hattingh,IEEE,2022.
[12] "A Blockchain Based Credential Verification System using IPFS" , Swatesh Kumar Ambast, T A Sumesh , IEEE,2022.
[13] "The economics of cryptocurrency and blockchain technology," P. Tasca, T. Kristoufek, and P. Matta, in The Economics of Fintech, Cambridge, MA, 2019, pp. 35-58.
[14] "Blockchain technology: Beyond bitcoin," M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, Applied Innovation, vol. 2, pp. 6-10, Jun 2016.
[15]"An overview of Ethereum and Solidity vulnerabilities",Aicha Bouichou , Soufiane Mezroui,Ahmed El Oualkadi, IEEE,2021
[16]"Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract",Satpal Singh Kushwaha , Sandeep Joshi , Dilbag Singh , Manjit Kaur , Heung-No Lee,IEEE,2022
[17]"Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends",Shuai Wang , Liwei

Ouyang, Yong Yuan , Xiaochun Ni,Xuan Han , Fei-Yue Wang,IEEE,2024
[18]"An Overview of Smart Contract and Use Cases in Blockchain Technology",Bhabendu Kumar Mohanta , Soumyashree S Panda , Debasish Jena,IEEE,2023
[19]"An Overview of Smart Contract: Architecture, Applications, and Future Trends",Shuai Wang , Yong Yuan , Xiao Wang , Juanjuan Li , Rui Qin ,Fei Yue Wang,IEEE,2020
[20]"Blockchain technology: An overview" ,Ramesh Ramadoss,IEEE,2010