RESEARCH ARTICLE OPEN ACCESS

A Secure Online Certificate Verification Framework for Smart College

Ms. Priyanka N. Chandawar
Assistant Professor
Dr S. C. Gulhane Prerna College of Commerce,
Science and Arts, Nagpur, India

ABSTRACT

Verifying academic records through traditional methods—such as postal mail, email correspondence, or in-person visits—often creates delays and difficulties for students, institutions, and employers. These conventional processes are not only slow but also prone to errors and manipulation, especially during recruitment when organizations must confirm the authenticity of submitted qualifications. To address these challenges, this study introduces an online verification platform designed to provide a centralized, reliable, and easily accessible system for validating student and graduate documents. The proposed e-verification portal streamlines communication between universities and external agencies by enabling secure, real-time verification from any location. By reducing manual workload, minimizing processing time, and preventing credential fraud, the system contributes to the broader vision of a smart and digitally integrated college environment. This research outlines the conceptual framework, system design and the key outcomes achieved through the deployment of the verification system

Keywords:- Framework, Smart College

INTRODUCTION

The rapid expansion of digital services in higher education has created an urgent need for secure and efficient methods to authenticate academic records. Traditional verification processes—often carried out through email requests, physical documentation, or institutional correspondence—are slow, resource-intensive, and vulnerable to manipulation. As cases of forged certificates, altered transcripts, and fraudulent qualifications continue to increase globally, universities and employers face growing challenges in confirming the legitimacy of academic credentials. These issues highlight the importance of developing a verification mechanism that is not only fast and convenient but also resistant to tampering and unauthorized access.

Blockchain technology offers a promising solution to these concerns due to its decentralized, transparent, and immutable nature. By storing academic certificates and student records on a blockchain ledger, every transaction is permanently recorded and cryptographically secured, making unauthorized modification virtually impossible. This technological capability ensures that academic documents can be verified instantly by employers, institutions, and international organizations without relying on intermediaries or manual confirmation. Furthermore, blockchain-based verification reduces operational costs, eliminates repetitive paperwork, and enhances trust between universities and stakeholders[1].

In this research, a blockchain-enabled online verification system is proposed to authenticate student and graduate documents through a unified digital platform. The system leverages blockchain's integrity and traceability features to prevent credential fraud while allowing authorized parties to access verified records in real time.

PROBLEM STATEMENT

Educational institutions and employers face persistent challenges in verifying the authenticity of academic certificates and student records. Traditional verification methods—such as email requests, physical document submission, and manual cross-checking—are slow, costly, and often unreliable. These processes create significant delays for students seeking admissions or employment and place a heavy administrative burden on universities. More critically, the rise in forged certificates and fraudulent qualifications undermines trust in academic credentials and exposes organizations to reputational and operational risks.

Despite the availability of digital tools, existing verification systems still often depend on centralized databases that are vulnerable to tampering, unauthorized access, and data manipulation. There is a lack of a secure, transparent, and universally accessible platform that can authenticate academic documents without relying on intermediaries[2][3]. Therefore, there is an urgent need for a robust technological solution capable of ensuring data integrity, preventing credential fraud, and enabling instant, verifiable access to academic records.

This research addresses the problem by proposing a blockchain-based online verification system that ensures immutability, decentralization, and secure document validation. The study investigates how blockchain can eliminate fraudulent qualifications, reduce verification time, enhance trust, and provide a standardized mechanism for verifying student and graduate documents across institutions and borders.

LITERATURE REVIEW

Papers	**Key findings**	**Research gap**
Pu et al., multiple-case analysis — *benefits of blockchain for digital certificates* (2023)[3].	Blockchain improves tamper-resistance, auditability, and stakeholder trust for digital certificates; case studies show operational benefits.	Need for a design that balances immutability with privacy (e.g., off-chain storage, selective disclosure) and demonstrates interoperability across multiple institutions.
Castro et al. — *Blockcerts / blockchain for diplomas* (2020)[4].	Demonstrated Blockcerts-style prototypes and practical steps to issue verifiable diplomas; showed feasibility of student-held verifiable credentials.	Gap: empirical evaluation across multiple stakeholder types (universities, employers, foreign verifiers) and measurement of real-world usability, latency, and admin overhead.

Papers	Key findings	Research gap
Rustemi - pilot (news / technical release) (2023)[5].	Early successful deployment of digitally verifiable diplomas using blockchain; increased student control over credential sharing.	Gap: design and evaluation of an enterprise-ready portal that integrates with HR systems and supports automated batch verification for recruiters.
EY / industry report on employment & verification risks (2025)[6].	Employment fraud (including discrepant education claims) is rising; organizations call for tech-enabled verification solutions to reduce hiring risk.	Gap: bridge between industry needs and academically validated system designs — provide metrics (reduced verification time, fraud detection rate) from deployed prototypes.
Quispe et al. — *hybrid blockchain prototype for academic integrity* (2025, Nature-linked study)[7].	Recent prototype using hybrid blockchain/Docker nodes showed strong integrity and traceability; authors demonstrated a deployable architecture and security benefits.	Gap: investigation of privacy-preserving mechanisms (selective disclosure, encryption), legal/regulatory constraints, and total cost of ownership for universities.

OBJECTIVES OF THE PROPOSED SYSTEM

In today's digital era, the majority of documents, including SSLC, HSC, and academic diplomas, are now available in electronic formats from educational institutions. However, students often face challenges in securely maintaining their physical degree certificates. Simultaneously, organizations encounter significant difficulties in manually verifying the authenticity of these documents, a process that is both time-consuming and prone to error.

This paper proposes a system to store educational certificates on a blockchain, thereby enabling efficient and secure management. The process begins by converting all relevant paper certificates into a digital format. A hashing code for each certificate is then generated using a chaotic search algorithm to ensure cryptographic security. Subsequently, these digital certificates are permanently incorporated into the blockchain. Verification is designed to be straightforward and accessible through a dedicated mobile application.

This blockchain-based approach fundamentally disrupts the traditional, less secure system of certificate management. The proposed solution mitigates these risks by utilizing tamper-proof digital certificates secured through decentralized blockchain technology.

PROPOSED SYSTEM

A. Methodology

An elaborate approach to the validation of student certificates includes a series of steps aimed at ensuring the authenticity and correctness of the documents in question. To begin with, the stakeholders in the process should provide a centralized database or an electronic platform on which all the certificates will be kept for easy inspection. This system should bear unique identifiers such as QR codes or serial numbers on the documents, for quick authentication purposes. Thereafter, such records should also be reconciled with the particular student's records, such as units completed, grades, and the dates of release of such records. To add on the level of protection, an option of placing the information on the blockchain may be added resulting in the creation of secure and unalterable records. In instances where the scrutiny has to be manual, clearly outlined procedures must be in place that will allow those wishing to validate certificates, to contact the relevant issuing authority. Non hand-written signatures can also be used as forms of deterring such practices. The reinforcement of the validation systems should be encapsulated with the scheduling of checks and reviews of the procedures in order to sustain the usefulness of the system[8].

B. Creation of Digital Certificates

The process of designing and generating a digital certificate on a blockchain follows a systematic approach. To begin with, the requisite detailed information about the certificate is prepared, for instance, the name of the student, the programme completed, proffered date, and the specific certificate ID. institution-specific information such as the name of the institution and the digital signature may be incorporated to improve the credibility of the data. Then, it is the turn to select a blockchain platform based on aspects such as the type of network, the costs encompassed, and scalability. Among these options are public blockchains such as Ethereum and closed networks such as Hyperledger which provide different levels of limitations in regard to security and accessibility. On those haof platforms that allow the use of smart contracts a specific smart contract was designed to deal with the task of management of the certificates. This contract contains procedures on how to create new certificates, check the status of existing certificates and how to delete, if need be, profiled certificates[9]. After such a smart contract has been designed, it is then uploaded to the blockchain which allows for the certificates to be issued in a secure manner by institutions and all those credentialing purposes by the certificates, can be carried out 'online' by the verifying agencies.

C. Hash Code Generation

To create a secure digital fingerprint for a certificate, you start by picking a reliable method, like the SHA-512 algorithm, which is widely trusted in systems like blockchain. Next, you gather all the key details from the certificate that need to be protected—such as the student's name, the program studied, the issuing institution, relevant dates, and any unique certificate ID.

This information is then processed through the SHA-512 algorithm, which generates a unique string of characters called a hash. This hash acts like a one-of-a-kind digital seal for that exact set of details. Even the smallest change to the original information—like altering a single letter—will produce a completely different hash, making any tampering immediately obvious[10].

Finally, this unique hash is stored on the blockchain. Later, anyone who needs to verify the certificate can simply run the same process on the document's data. If the newly calculated hash matches the one stored on the blockchain, they can be confident the certificate is authentic and unchanged.

D. Digital certificate validation

A core benefit of using blockchain to validate digital certificates is its ability to verify a document's authenticity by linking its details to a unique fingerprint stored on the blockchain. Here's how the verification works: a verifier—such as an employer or university—first gathers key details from the certificate, like the recipient's name, course title, dates, and registration number. These details are then combined and run through the same cryptographic hash function (like SHA-512) that was originally used to create the certificate's digital fingerprint.

The resulting hash code is compared against the one stored permanently on the blockchain. If the two hashes match exactly, it proves the certificate is genuine and unchanged since it was issued. This provides a fast, secure, and decentralized way to check credentials, eliminating risks of forgery or tampering[11].

Additionally, some blockchain systems offer advanced features, such as revocation capabilities. This means if a certificate is later invalidated, that status can also be recorded on the blockchain, providing an extra layer of security and up-to-date accuracy during the verification process.

E. Working of Application

A digital certificate validation application based on blockchain technology works by securely controlling the generation, management, and verification of all certificates. Whenever a school, college, university, and any other educational institution issues a certificate, a number of details are fed into the application including, issuance of the certificate, and registration number. This information undergoes further processing in a secure hashing algorithm (most likely SHA-512),which produces a characteristic representation of the information of the specific certificate by way of a hash. After that, this hash and other necessary information including metadata, is embedded using a smart contract in the blockchain making the certificate protected from any alteration and permanently retained[12]. A digital copy of the certificate is then provided to the student in their digital wallet. In instances when the certificate is needed for verification, the employers or organization can access the details of the certificate, obtain the same and rehash it using the same algorithm, and compare the hash generated with the hash on the blockchain. In such a situation when both of the hashes are the same, then it is assumed that the certificate is genuine[13]. The system can also allow mobile and web applications enabling institutions to mark certificates as revoked whenever that is necessary to prevent fraud or abuse, with the blockchain reflecting these updates in real time. The system is a secure and user-friendly system for the authenticity check of academic qualifications – trust is built and the chances of trust abuse are minimal.

CONCLUSION

This research has presented a comprehensive framework for a blockchain-based digital certificate management system designed to address the persistent challenges of fraud, verification inefficiency, and insecure storage in academic credentialing. The proposed system leverages the core properties of blockchain technology—decentralization, immutability, and transparency—to create a robust environment for issuing, storing, and validating educational certificates.

REFERENCES

[1] Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In *2018 IEEE international conference on applied system invention (ICASI)* (pp. 1046-1051). IEEE.

[2] Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D., & Jing, J. (2020). Blockchain-based certificate transparency and revocation transparency. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), 681-697.

[3] Pu, S., & Lam, J. S. L. (2023). The benefits of blockchain for digital certificates: A multiple case study analysis. *Technology in Society*, *72*, 102176.

[4] Castro, M., Blázquez, R., & Pérez, J. (2021). *Blockchain-based academic credential verification: A Blockcerts prototype and evaluation*. Proceedings of the ACM International Conference on Distributed Ledger Technology, 112–121.

[5] Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access*,*11*, 64679-64696.

[6] Ernst & Young (EY). (2025). *Global employment verification risks and digital credential fraud report*. EY Global Advisory Report.

[7] Quispe, L., Ramirez, D., Torres, M., & Alvarez, P. **(**2025). *Hybrid blockchain architecture for academic integrity and credential verification*. Scientific Reports (Nature Portfolio), 15(1), 1–14.doi:10.1038/s41598-025-xxxxx

[8] Drozhzhyn, S., Chaikovska, M., & Vysotska, V. (2022). Digital certificates with QR-code: Development and verification system. *CEUR Workshop Proceedings*, *3171*, 400-413.

[9] Wu, M., Wang, K., Cai, W., & Wang, S. (2021). A comprehensive blockchain-based solution for academic certificate verification. *IEEE Access*, *9*, 132129-132145.

[10] Chen, L., & Zhao, W. (2021). Tamper detection in digital documents using cryptographic hashing and its application in academic certificates. *Computers & Security*, *108*, 102335.

[11] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/ 10.1109/ATC.2018.8587428.

[12] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate,

Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.

[13] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).