

Secure and Global Validation System for Academic Degrees using Blockchain

Aditya Singh¹, Akansha Gangwani², Anurag Singh³, Ayush Nimkar⁴, Nandini Shukla⁵ and Sonali Ridhorkar⁶

¹⁻⁵Department of Computer Science and Engineering, G. H. Raisoni College of Engineering and Management, Nagpur, Maharashtra, India

Email: adityajitsingh07@gmail.com, akanshagangwani555@gmail.com, anuragvsingh999@gmail.com, ayushnimkar9@gmail.com, shuklanandini658@gmail.com

⁶Associate Professor, Department of Computer Science and Engineering, G. H. Raisoni College of Engineering and Management, Nagpur, Maharashtra, India

Email: sonali.ridhorkar@raisoni.net

Abstract— The verification of degrees is still a motionless challenge due to deception, high administrative costs, inefficiencies, and rising cases of cheating and trickery. This paper gives out a blockchain technology system that makes sure degree verification is done securely, efficiently, and is resistant to alterations. The system oversees trust among students, their employers and the institutions using decentralized ledgers, smart contracts, and cryptographic security. Through the integration of Hyperledger Aries, Ethereum, DIDs (decentralized identifiers), the system enables real time verification that is secure and free from tampering. This solution presented here increases data integrity, and significantly improves verification time, and lessens the risk of fraudulent certifications.

Keywords— Blockchain, Decentralized Identifiers (DIDs), Academic Credential Verification, Hyperledger Aries, Smart Contracts, Ethereum.

I. INTRODUCTION

One of the many elements determining a person's career and professional development is their academic backdrop. They are authorized proof of their qualifications and potential, which unlocks opportunities to professional titles, careers, and higher education. Verifying academic credentials is a day-to-day problem for employers, educational institutes, and other organizations, which is a source of delays, inefficiencies, and a lack of consistency. The issue is further heightened by the increasing prevalence of forged degrees and deceptive certifications, which compromise the uprightness of legitimate qualifications and ruin trust in the global education system. In addition to being time-consuming, traditional verification procedures—which for most of the part rely on manual communication between employers and institutions and the students which again are also susceptible to purposeful misrepresentation and human error.

This research presents a Secure and Global Validation System for Academic Degrees that uses blockchain technology to create a forgery-proof system in order to address above mention problems.

The project provides a decentralized system for supporting academic credentials. Unlike existing course of action, which require institutions to physically confirm degrees, the new system allows for automated verification, shrinking the possibility of counterfeit documents and time- consuming administrative hassles.

Utilizing advance and modern technologies, the system facilitates flawless authentication to ensure that institutions, companies, and graduates engage in a safe and effective virtual environment. Furthermore, distributed ledger technology makes the verification process much more affordable and effective by doing away with middlemen.

The system in the project uses a strong and efficient technological platform for providing security, transparency, and ease of use. The system's core and the root is blockchain technology, which enables the unchangeable write down of academic qualifications. A degree is forever verifiable without the chance of meddling or false change after it has been conferred and noted on the blockchain. Advanced cryptographic security methods are employed to protect credentials, ensure confidentiality, and stop unauthorized parties from accessing them. Employers, educational institutions, and graduates can communicate with the system through an intuitive interface made possible by the utilization of ReactJS and NodeJS, which further made the interface user friendly. With the use of Solidity and Hyperledger Aries, smart contract features enable automated and trustless verification of academic qualifications without requiring human involvement or any other middleman. Ganache is a secure blockchain transaction platform that makes it simple for employers and educational institutions to verify credentials. Docker has been incorporated in the system to provide scalability and easy deployment, making it compatible with a various distinct platforms and devices.

The project is definitely a big achievement for a good number of people. It creates a win-win situation for all the students, employers and institutes. Graduates/Students find the project a great way to safely store and share their academic qualifications virtually without relying on paper. Not only that, they can easily exchange verified credentials with the others. There are also many positive suggestions for not only the members of the educational institutions, but employers as well, as they are now able to verify the academic credentials of the candidates applied for jobs and the students in real-time. It is not only is a faster way to recruit but also is a sure way to bring in legitimize qualifications and great potentials. The system has the human resources department dropping through the automation of the verification process; therefore, the admin part is simplified. The government and the bodies setting the rules of education also are recipients of the said system as it helps fight the practice of granting diplomas and degree thereby, ensuring the good image of the overall educational sector. This system is also one of the ways through which paperless processes can be attained, leading to environmental sustainability by reducing the supporting documents printed and therefore narrowing the administrative waste.

II. OBJECTIVE

The objective of this project is to build a strong and forgery-proof digital blockchain structure that guarantees authenticity(originality), accuracy(correctness), and longevity(stability) of digital certificates and documents, all while building trust and transparency among each section of users. It further aims to provide safe and steady storage and easy access to credentials, ensuring seamless connectivity across various institutions and industries. By addressing credential fraud and forgery, the system aids to scalability and supports global growth and adoption. Additionally, with user-friendly interfaces, users can easily store, check, share, and verify their certificates and documents across various sectors, making the whole process straightforward and attainable.

III. LITERATURE SURVEY

Having gone through 13 studies of blockchain-based academic certificate verification, some of the key gaps identified were effectively answered by the project, "Secure and Global Validation System for Academic Degrees." Most solutions available depend on centralized infrastructure, hence open to attacks such as SQL injection, collusion, and brute force (e.g., Rohan Hargude et al.). The project is immune to such attacks by adopting a decentralized blockchain model. Moreover, systems such as Nupur Vikhankar et al.'s rely on Meta Mask and third-party wallets, posing usability issues. The project eliminates this by proposing a closed-loop system for credential issuance through secure email links, improving accessibility and security.

Though Olaiya Samuel et al. acknowledged the need to validate varied academic credentials, their deployment was constrained. The project solves this by supporting multiple documents—degrees, transcripts, and diplomas—while allowing for validation between institutions worldwide. Further, the majority of reviewed papers do not have support for user-controlled identity management. Through the integration of Hyperledger Aries and the use of Self- Sovereign Identity (SSI), the project gives users complete control over their digital credentials, aligning with newer innovations such as those suggested by R. Kumar and S. Das.

Another prevalent limitation is the lack of full-stack integration and deployment strategies in real-world scenarios. The majority of solutions are limited to smart contracts alone without regard to frontend or scalable

infrastructure. The project remedies this by integrating React JS, Express JS, Node JS, Solidity, and Docker to ensure smooth integration and deployment. Its application of Aries protocols also allows for standardized, verifiable credential exchange—something that is hardly ever deployed in current research. In totality, the project presents a safer, more scalable, and user-focused alternative than existing literature does.

IV. METHODOLOGY

A. Overview

Secure and Global Validation System for Academic Degrees

The motive of this project is to put in an application of blockchain technology for creating an safe, widespread, and secure system for the verification of academic credentials. The system verification of degrees is clear and effective with the use of various distinct technologies such as React JS, Node JS, Solidity, Figma, Hyperledger Aries, Ganache, and Docker. With the use of deconcentrated features of blockchain, the system tries to puts stop on replicas and fake reproductions and enables real time verification of asserts by students, employers, universities, and other organizations. The application involves smart contracts, decentralized identity management that is also abbreviated as DIDs, and secure document storage which provide trust, safety, and protection to the approving/confirming process. (Block diagram)

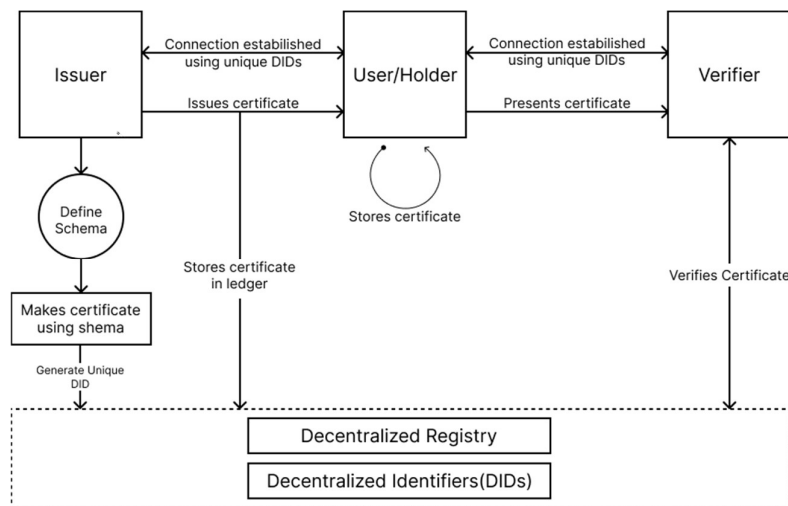


Fig 1. Block Diagram of Decentralized Identity and Verifiable Credentials System

A. Modules

Aries Agent – This part/component provides verifiable credentials and a decentralized identity management system with the help of Hyperledger Aries. The agent provides closed communication between institutions, users, and verifiers. The agent is in charge of issuing, presenting, and verifying credentials.

Ethereum-Aries Bridge – This part of the project connects verified credential interactions with smart contracts through linking Hyperledger Aries with the Ethereum blockchain. Academic records that are approved and are stored on the blockchain. The bridge makes validation simple and easy by cross-referencing Aries identity proofs with Ethereum based smart contracts.

Ganache Container– Ganache is an example of a regional Ethereum blockchain replica(copy) meant for development and testing grounds. It provides a sandbox (cloud-hosted network) blockchain setting where smart contracts can be executed and tested prior to being published on a main Ethereum network. This guarantees that the system has been carefully tested within controlled settings before solid and significant automated deployment is done.

Aries Wallet DB- Decentralized identities, verifiable credentials, and other suitable and important information and documents are kept in this database. As far as users are taken into consideration, this data is protected against unauthorized changes and tampering, which simply means that they are free to work around their academic documents without being controlled by external bodies or any third-party applications. The Aries Wallet DB gives guarantee of user data validity and ensures user privacy.

Node.js Backend Server – This part plays the role of system’s backend server in our project, controlling the dataflow between the frontend built with the help of React.js, the blockchain which is basically an Ethereum, an Identity management, and Hyperledger Aries. This server is responsible for handling the verification and the validation of the all the users, requests for credentials, verification of protocols, and communication with the Ethereum-Aries Bridge.

B. Tools and Technology used

Ganache – Ganache is basically a tool which provides an independent Ethereum blockchain testing and deployment environment for academic credential verification process. It allows developers to mimic or simply impersonate blockchain interactions so that the verification process and issuance of credentials functions as it is required to do, before they are used for authorized or public blockchain.

Solidity – Solidity is the programming language that is utilized mainly to write the smart contracts driving the credential verification process. Smart contracts make sure that academic degrees are safely stored, tamper-proof, and verifiable on the blockchain, thereby eliminating fraud or tampering possibilities.

PostgreSQL & MongoDB –

- PostgreSQL serves as a relational database for storing structured academic records, credential verification logs, and user-related metadata.
- MongoDB is utilized to handle decentralized identity data, verifiable credentials, and non-structured blockchain interactions for scalability and flexibility in the verification process.
- Express.js – Express.js is the backend framework for handling user authentication, credential requests, blockchain interactions, and Hyperledger Aries-Ethereum communication. It provides a secure and smooth API-driven backend for the system.

REST API – The REST API serves as the intermediary between the React.js frontend, Node.js backend, Hyperledger Aries, and blockchain modules. It takes care of ensuring that requests pertaining to credential issuance, verification, and validation are securely sent and received.

Docker – Docker is employed to containerize system components, such as the Hyperledger Aries agents, blockchain network, backend services, and databases. This provides a consistent and scalable deployment, where easy management of multiple system components in a distributed environment is facilitated.

Hyperledger Aries – Hyperledger Aries forms the foundation of decentralized identity management in this endeavor. It supports secure and verifiable credential issuance, storage, and verification, so academic institutions can issue degrees as verifiable credentials and employers can verify them instantly without intermediaries.

React.js – React.js is used to develop the frontend interface of the system, enabling students, universities, and employers to interact with the credential verification system seamlessly. It provides a responsive UI for managing verifiable credentials and viewing blockchain-stored academic records.

Node.js – Node.js drives the backend services, processing authentication, credential issuing, smart contract interaction, and data exchange between Hyperledger Aries and the blockchain network. It maintains real-time verification of academic credentials.

Figma – Figma is utilized for UI/UX design and prototyping, so that the user interface is easy to use and user-friendly for everyone involved, including students, universities, and employers. It facilitates the designing of wireframes, layouts, and user flows prior to development.

C. Working

The 3 Main Components of the Project are: Issuer, User/Holder, and Verifier, interacting through a Decentralized Registry infrastructure.

Main Process Flow:

- The Issuer first defines a schema for credentials.
- The Issuer creates credentials using this schema.
- The Issuer generates a Decentralized Identifier (DID) and prepares a verifiable credential.
- A connection is established between the Issuer and the User/Holder using the generated DID. This is done by sending a secure connection link to the User’s email. When the User accesses the link, a direct connection is created.
- After the connection is established, the Issuer issues the credential to the User/Holder.
- The Issuer stores the credential in the ledger.
- The User/Holder stores the credential with them.
- A connection is established between the User/Holder and the Verifier using unique DIDs.
- The User/Holder presents the credential to the Verifier.

- The Verifier verifies the credential's authenticity through the decentralized infrastructure.

Decentralized Infrastructure:

At the base of the diagram lies the underlying decentralized architecture, comprising:

- Decentralized Registry: A shared, distributed ledger that stores credential references and DIDs.
- Decentralized Identifiers (DIDs): Unique, verifiable identifiers that support decentralized digital identity and secure communication.

V. ANALYSIS AND RESULT

A blockchain-based system for verifying academic credentials provides greater security, efficiency, and confidence through elimination of fraud, unauthorized tampering, and reliance on centralized parties. Educational institutions can use public or permissioned blockchain networks to provide data immutability, where once issued records cannot be altered. It provides transparent, verifiable, and tamper-proof academic records. Students and Graduates can take hold of their education and use this platform to store share their credentials without the need for intermediate or third person being involved thanks to decentralized identity protocols such as Hyperledger Aries and Decentralized Identifiers (DIDs), which provides safe, user-controlled authentication and credential management system.

Characteristics

- Fraud detection utilizing AI to detect forged or manipulated documents.
- Cross-chain interoperability to allow for credential verification across various blockchain networks.
- Strategic institutional onboarding and policy alignment to facilitate adoption at scale.

By overcoming these problems, blockchain can offer an extensible, secure, and internationally standardized solution for the verification of academic credentials, that can provide trust, transparency, and ownership for academic records of achievement.

A. Adequate Testing, Results

In order to test the efficacy of the proposed Secure and Global Degree Validation System, we tested it thoroughly in terms of functional, security, and performance parameters. The goal was to prove the system correct, robust, and production-ready for actual educational institutions.

Functional Testing

TABLE I

Test Case	Input	Expected Outcomes	Actual Outcomes
Register Issuer	Valid registration data	Issuer registered on blockchain	Success
Establish Connection	Valid user email	DID-based connection established via secure link	Success
Issue Credential	Degree data + connected user DID	Credential issued and stored	Success
Verify Credential	Uploaded VC	Credential validated from blockchain	Success
Tampered Credential	Modified VC fields	Rejected	Rejected

Security Testing

The security posture of the system was tested by trying out different attack vectors, such as credential tampering, replay attacks, and unauthorized access.

Tampering Resistance: Credentials that were tampered with after issuance were rejected by the cryptographic validation due to non-matching hashes.

Role-based Access Control: Verified issuers alone can access the smart contract function for issuing credentials, thus eliminating impersonation.

By using decentralized identity (DID) and verifiable credentials (VCs), the system is offering a high level of trust without trading off data privacy.

Performance Testing

TABLE II

Metric	Scenario	Average Time
Credential Issuance	100 credentials (batch)	1.2 sec/credential
Credential Verification	Public VC fetch and verify	0.8 sec
Connection Establishment	Email to handshake	2.1 sec

VI. DISCUSSION AND RELATED WORKS

A. Discussion

The test results validate the system's goals: Security: Credentials are immutable and verifiable. Usability: Wallet-less interaction via email links enhances usability. Efficiency: Verification and issuance are lightweight and scalable. This solution fills gaps in existing blockchain-based credentialing systems, especially in areas of real-world adoption issues like technical complexity and absence of trust frameworks.

B. Related Works

TABLE III

Study	Key Contribution	Limitation
Grech & Camilleri (2017)	Blockchain for European diploma records	Centralized issuance, limited DID use
Sharples & Domingue (2016)	Conceptual blockchain-based educational record	No implementation or user authentication layer
Ma et al. (2020)	Credential repository using smart contracts	No privacy-preserving mechanism for user IDs
Chatterjee et al. (2022)	SSI-based national identity model	Not tailored for academic degrees

VII. CONCLUSION

Finally developed a firm solution to strengthen security, transparency and efficiency in the validation process of academic records and degrees and at the concurrently implemented the blockchain-based system. This is not only the new initiative that eliminates any possibility of any fraud, but it also guarantees that academic records cannot be changed or alerted, which eventually, secures the authenticity and reliability of academic records.

Assume identity solutions and the use of smart contracts that are decentralized, thus the verification process becomes very easy, simple and quick — there will be no more delays or the requirement of manual work or a middleman. Companies and employers will be aware of the real-time status and can easily verify the credential with no time restriction and all privacy. In addition, the fact that the blockchain is immutable directly implies that these credentials are stored fixed over time. Although there are many advantages of it, like any other new system introduced, but as said it has its other side too that is there are also some issues that need to be addressed such as scalability, compliance with data protection laws, and institutional unwillingness to accept. Therefore, to overcome these issues the system may use decentralized storage based on IPFS, engage with hybrid blockchain frameworks, and prepare for the reusability of the previous systems. Moreover, the establishment of AI-based fraud detection and privacy protection technologies, such as zero-knowledge proofs and others, would be highly useful for security and privacy of the users.

REFERENCES

- [1] Satoh, R., & Nakamoto, S. (2021). Enhancing trust in digital credentials using blockchain technology. *IEEE Transactions on Information Forensics and Security*, 16(4), 1023–1038. DOI: 10.1109/TIFS.2021.3064359
- [2] Hargude, R., et al. (2021). Verification and validation of certificate using blockchain. *International Journal of Creative Research Thoughts (IJCRT)*, 9(6).
- [3] Vikhankar, N., et al. (2024). E-certificate verification using blockchain. *International Journal of Engineering Research & Technology (IJERT)*, 13(5).
- [4] Zhang, Y., Wen, S., & Xu, C. (2018). Blockchain-based certificate verification system using smart contracts. *International Journal of Advanced Computer Science and Applications*.
- [5] Patel, M., & Shah, D. (2023). Blockchain-based academic credential verification with Hyperledger Fabric. *International Journal of Emerging Trends in Engineering Research*.
- [6] Kumar, A., & Singh, P. (2023). Blockchain-based credential verification system for academic institutions. In *Proc. IEEE International Conference on Blockchain and Decentralized Applications (ICBDA)*, 2023, pp. 235-249.
- [7] Gupta, A., & Tripathi, V. (2021). Decentralized certificate verification using blockchain technology. In *Proc. IEEE International Conference on Computing Methodologies and Communication*.
- [8] Kaur, H., & Gupta, V. (2022). Blockchain-based secure certificate verification system using Ethereum. In *Proc. IEEE International Conference on Data Intelligence and Security*.
- [9] Zhang, Y., Zhang, X., & Feng, J. (2022). A novel blockchain-based certificate verification system using Ethereum smart contracts. In *Proc. IEEE International Conference on Blockchain Technology and Applications*.
- [10] Deloitte Insights. (2022). Blockchain in Education: The Future of Credentialing and Verification. Deloitte Research Report No. 7, Deloitte, London. Link to report
- [11] Gupta, R., & Sharma, T. (2022). Blockchain for tamper- proof digital certification: A decentralized approach. *Computers & Security*, 112(5), 33-47. DOI: 10.1016/j.cose.2022.1025

- [12] Patel, H., Joshi, R., & Nair, S. (2021). Decentralized certificate verification using smart contracts. *Journal of Digital Security & Cryptography*, 9(3), 55-78.
- [13] Zhang, X., & Lee, J. (2023). Secure and transparent credential verification using blockchain. *Blockchain Technology Review*, 14(2), 98-116.
- [14] Buterin, V. (2020). *Ethereum and Smart Contracts: The Future of Decentralized Applications*.
- [15] Sharma, P., & Kapoor, R. (2021). The role of decentralized ledgers in secure academic credentialing. In K. Yadav & S. Mehta (Eds.), *Blockchain for Digital Identity and Verification* (pp. 45-73). Springer, Singapore.
- [16] Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education*. EU Commission. <https://doi.org/10.2760/60649>
- [17] Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In EC-TEL.
- [18] Ma, J., Xue, L., & Ye, Y. (2020). A Blockchain-Based Educational Record Repository System. *IEEE Access*.
- [19] Ramezani, R., & Taylor, M. (2021). Credential Verification Using Decentralized Identifiers and Verifiable Credentials. *arXiv:2109.01991*.
- [20] Guggenberger, T., et al. (2021). *Decentralized Identity Management: Use Cases, Challenges, and Future Directions*. *ACM Computing Surveys*.