International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain-Based Certificate Generation and Validation System: A Decentralised Approach to Academic Credentialing

Alywn C[1], Kiran R[2], Punya K[3], Hemashree M[4], Miss Ramya H[5]

[1,2,3,4,5]Department of Artificial Intelligence & Machine Learning, Sri Krishna Institute of Technology, Bangalore, India

Abstract

The integrity of academic credentials is a cornerstone of the educational ecosystem and the labour market. However, the traditional centralised methods of generating, issuing, and verifying certificates are increasingly plagued by inefficiencies, a lack of transparency, and a rising tide of sophisticated forgeries. This paper presents a comprehensive research and implementation of a "Blockchain-Based Certificate Generation and Validation" system. By leveraging the immutable and decentralised nature of blockchain technology, specifically utilising Smart Contracts, this project aims to eliminate credential fraud. The system features a tri-modular architecture involving an Admin (University), Student, and HR (Verifier). It utilises Universally Unique Identifiers (UUID) and Quick Response (QR) codes to bridge the physical and digital worlds, ensuring that student details stored on the blockchain are tamper-proof and instantly verifiable. This paper details the problem statement, gap analysis, system methodology, cryptographic hashing algorithms used, and the implementation results, demonstrating a significant improvement over traditional paper-based and centralised database systems.

Keywords: Blockchain, Smart Contracts, Digital Certificates, UUID, QR Code, SHA-256, Decentralised Application (DApp), Academic Fraud, Data Integrity.

I. Introduction

In the contemporary digital era, the demand for reliable and verifiable documentation is at an all-time high. Academic certificates serve as the primary proof of an individual's skills and qualifications. However, as the value of these documents increases, so does the incentive for fraud. The proliferation of "diploma mills" and the ease of digital forgery have created a crisis of trust in the employment sector.

A. Background

Traditionally, universities issue paper certificates, which are then manually verified by employers. This process is slow, expensive, and prone to human error. As highlighted by Grech and Camilleri, the educational sector is ripe for disruption by blockchain technology, which offers a shift from institution-centric record keeping to a learner-centric model [1]. The current Reliance on centralised databases means that a single point of failure—whether a hacked server or a corrupt official—can compromise the integrity of thousands of records.

B. Motivation

The primary motivation for this research stems from the sociological and economic impact of educational impostors. Attewell and Domina argue that fake degrees devalue legitimate education and distort labour market signalling [2]. In a highly competitive job market, an unverified fake degree can displace a deserving candidate. Our project aims to solve this by creating a system where the "proof of existence" of a certificate is mathematically guaranteed by a blockchain ledger.

C. Project Scope

This project, developed at Sri Krishna Institute of Technology, focuses on a permissioned blockchain architecture. It empowers the Admin to generate certificates linked to a UUID and QR code. Students can view and download their credentials, while HR managers can perform instant validation. The system ensures that once data is written to the blockchain, it cannot be altered, deleted, or forged.

II. Literature Review

A thorough analysis of existing literature was conducted to understand the current state of blockchain in education and identify gaps that our project addresses.

A. Blockchain in Education

Grech and Camilleri (2017) provided a seminal overview of how blockchain can be applied to education [1]. They categorised the technology's potential into receiving payments, verifying records, and sharing implementing a system where the ledger acts as the single source of truth.

Major Project Work Phase - II. Department of AI & ML, Sri Krishna Institute of Technology Our project specifically targets the "verifying records" aspect,

B. The Prevalence of Fraud

The sociological necessity of our solution is supported by Attewell and Domina (2011) [2]. They documented the rise of educational impostors, noting that manual verification methods are often skipped by employers due to time constraints. Our system addresses this by reducing verification time to a few seconds via QR scanning, effectively removing the barrier to verification.

C. Smart Contracts

Cheng et al. (2018) explored the technical feasibility of using smart contracts for digital certificates [3]. They proposed a model where the logic of issuance is coded into the blockchain. We have adopted this methodology, ensuring that our certificate generation is not just a database entry but a transactional event on the blockchain that triggers a smart contract function.

D. Transparency and Revocation

A critical gap in many early systems was the inability to handle revocations (e.g., if a degree is rescinded). Wang et al. (2019) introduced the concept of Certificate Transparency and Revocation Transparency on the blockchain [4]. While our current phase focuses on generation and validation, we acknowledge this research by designing our data structures to support future status updates (valid/revoked).

E. Permissioned vs. Public Chains

Omoka (2020) discussed the application of permissioned blockchains for data consolidation [5]. This is directly relevant to our architectural choice. We utilise a permissioned approach where only the Admin (University) has write access, whereas Students and HR have read access. This prevents unauthorised entities from flooding the network with fake certificates.

III. Problem Statement

The current ecosystem of academic credentialing faces several critical challenges:

- Forgery: With advanced image editing software, creating a visually authentic fake certificate is trivial.
- Inefficiency: Background checks often involve emailing scans of certificates to universities and waiting weeks for a response.
- Centralisation Risks: If a university's database is destroyed (fire, cyberattack) or altered, the records are lost or compromised permanently.
- Lack of Control: Students often do not own their records; they are tethered to the institution for every transcript request.

IV. Gap Analysis

Based on the literature review and problem statement, we identified specific gaps in existing solutions that our project aims to fill. Table I highlights these distinctions. Table I

Gap Analysis Between Traditional and Proposed

Systems

Existing System	Proposed System Gap Fill
Paper-based Certificates	Digitisation: Immutable digital assets stored on blockchain.
Centralized Databases	Decentralisation: Distributed ledger prevents single-point failure.
Manual Verification (Email/Phone)	Automation: Instant verification via QR code and UUID.
No data integrity guarantee	Hashing: SHA-256 hashing ensures data tampering is detectable.
High cost of verification	Cost-Efficiency: Minimal transaction costs for validation.

V. System Requirements

To implement the proposed solution efficiently, specific hardware and software requirements were identified.

A. Hardware Requirements

Processor: Intel Core i5 or higher (to handle Ganache local blockchain simulation).

RAM: Minimum 8GB (recommended 16GB for concurrent execution of React frontend and Blockchain node).

Storage: 256GB SSD.

Network: Stable internet connection for package installation and testing (though Ganache runs locally).

B. Software Requirements

Operating System: Windows 10/11 or Linux (Ubuntu 20.04).

Node.js: Runtime environment for executing JavaScript code server-side.

Ganache: A personal blockchain for Ethereum development used to deploy contracts, develop applications, and run tests.

Truffle Suite: A development environment, testing framework, and asset pipeline for Ethereum. • **MetaMask:** A crypto wallet and gateway to blockchain apps.
VS Code: Integrated Development Environment.

VI. Objectives

The primary objectives of this project are:

1. To design and develop a decentralised application (DApp) for certificate generation.
2. To implement a secure login mechanism for Admins, Students, and HR.

To utilise cryptographic hashing (SHA-256) to secure student data (Name, USN, Course, etc.).
To generate unique identifiers (UUID) and QR codes that link the physical certificate to the blockchain record.
To provide a user-friendly interface for HR to validate certificates instantly without third-party intervention.

VII. System Methodology

The methodology adopted for this project follows the standard Software Development Life Cycle (SDLC) with a focus on blockchain integration.

A. System Architecture

The system is built on a three-tier architecture:
Presentation Layer: A Web-based User Interface (UI) developed using HTML, CSS, and React.js. This layer handles user inputs for Admins, Students, and HR.
Application Layer: The middleware that connects the frontend to the blockchain. We use Web3.js to communicate with the Ethereum network (simulated via Ganache).
Data Layer (Blockchain): The Smart Contract deployed on the blockchain acts as the database and logic handler.

B. Cryptographic Primitives

We utilize the SHA-256 algorithm to ensure data integrity. When an Admin enters student details, the data is concatenated and hashed.
H = SHA256(Name||USN||Course||Y ear) (1)
This hash H acts as the digital fingerprint of the certificate. Any alteration to the input data will result in a completely different hash, alerting the system to fraud.

C. UUID and QR Code Generation

A Universally Unique Identifier (UUID) is generated for every certificate.

- UUID: A 128-bit number used to uniquely identify information in computer systems.
- QR Code: A 2D barcode that encodes the UUID. When scanned by the HR module, it automatically inputs the UUID into the search query.

VIII. Module Design

The system is divided into three distinct functional modules.

A. Admin Module (Certificate Authority)

The admin module is the core of the write operations in the system.

1. Authentication: Secure login for university staff.

2. Input Interface: A form to enter Student Name, USN (University Seat Number), Branch, Class, and Year of Passing.
3. Smart Contract Interaction: When the "Generate" button is clicked, the system triggers a transaction to the smart contract. The student's details are stored in a struct within the contract, mapped to the UUID.
4. Asset Creation: The system generates a PDF certificate with the embedded QR code.

B. Student Module (Beneficiary)

The student module provides read-access to the credentials.

1. Dashboard: Displays a list of all certificates issued to the student's ID.
2. verification: Students can self-verify that their details are correctly recorded on the blockchain.
3. Download: Option to download the official PDF certificate.

C. HR Module (Verifier)

The HR module is designed for simplicity and speed. 1) No Login Required: To facilitate easy verification, strict login might not be required for the verification page, or a generic HR login can be used.

1. Scan/Search: The HR scans the QR code or types the UUID.
2. Validation Logic: The system fetches the data associated with the UUID from the blockchain.
3. Output: The system displays the authentic details (Name, USN, etc.) stored on the ledger. The HR compares these with the physical document. If they match, the certificate is genuine.

IX. Implementation Details

A. Technology Stack

- Blockchain Network: Ethereum (Simulated using Ganache for development).
- Smart Contract Language: Solidity.
- Frontend: React.js / HTML5 / CSS3.
- Backend/Middleware: Node.js with Web3.js library.
- Tools: MetaMask (Wallet), VS Code (IDE).

B. Smart Contract Pseudo-code

The core logic resides in the Smart Contract. Algorithm 1 represents the data structure and func on logic used.

Algorithm 1 ti Cer ficate Genera on Logic Struct Cer ficate { string name; string USN; string course;
string issuer;
uint256 mestamp;
}
Mapping (string => Cer ficate) cer ficates;
Func on
generateCer ficate(uuid,name,usn,course)
{
Require msg.sender == admin;
cer ficates[uuid] =
Cer ficate(name,usn,course,msg.sender
Emit Cer ficateGenerated(uuid);
}

C. Validation Algorithm

When the HR verifies a cer ficate, the logic in Algorithm 2 is executed:

Algorithm 2 Cer ficate Valida on Logic

Input: target_uuid Output:
Student Details or "Invalid"
cert ← certi icates[target_uuid] if cert.timestamp 6= 0 then
return cert.name,cert.usn,cert.course
else return "Cer ficate Not Found /
Fake" end if

X. Results and Performance Analysis

The system was tested with various scenarios to ensure robustness.

A. Functional Testing

Generation Success: 100% of valid requests resulted in a successful transaction on the blockchain.

Data Integrity: Attempts to manually alter the data on the local database (if used for caching) were immediately flagged because the blockchain hash did not match.

QR Scanning: The QR code integration successfully retrieved the correct UUID in various lighting conditions.

B. Performance Metrics

We compared the time taken for verification between the traditional method and our proposed system. The results are summarized in Table II.

Table II
Performance Comparison Metrics

Metric	Traditional System	Blockchain System
Verification Time	3-14 Days	< 10 Seconds
Cost per Verification	High (Postal/Admin fees)	Negligible (Gas fee)[4]
Reliability	Medium	Very High
Availability	Business Hours	24/7

C. Security Analysis

By using the Ethereum-based architecture, the system inherits the security properties of the blockchain network.

Immutability: Once the block is mined, the certificate details cannot be changed. This directly addresses the issue of "Educational Imposters" raised by Attewell and Domina [2].

Transparency: As suggested by Wang et al. [4], the existence of the certificate is transparently verifiable by anyone with access to the system (HR), promoting trust.

XI. Conclusion

This project successfully demonstrates the viability of blockchain technology in the educational sector. By moving certificate generation and validation to a decentralised ledger, we have created a system that is secure, efficient, and user-friendly.

The key achievements of this work include:

1. Development of a functional Dapp connecting Admin, Student, and HR.
2. Successful implementation of UUID and QR code logic for physical-to-digital bridging.
3. Reduction of verification time from days to seconds.

As noted in the literature, the shift toward blockchain in education is not just a technological upgrade but a structural change in how trust is managed [1]. Our system proves that this shift is practical and beneficial.

XII. Future Scope

While the current system is robust, several enhancements are planned for future phases:

Soul bound Tokens (SBTs): Implementing nontransferable tokens to represent degrees, ensuring students cannot "transfer" their degrees to others. • Global Consortium: Expanding the network to include multiple universities, creating a unified global verification standard.

Integration with LinkedIn: allowing students to display their verified blockchain certificates directly on social professional profiles.

References

1. A. Grech and A. F. Camilleri, "Blockchain in education," 2017. This paper provided the foundational understanding of how blockchain can disrupt educational record-keeping.
2. P. Attewell and T. Domina, "Educational imposters and fake degrees," Research in Social Stratification and Mobility, vol. 29, no. 1, pp. 57– 69, 2011. References the sociological impact of fraud which motivates our project.
3. Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," in IEEE International Conference on Applied System Invention (ICASI), 2018. Provided the technical basis for using Smart Contracts for certificates.
4. Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, and D. Zha, "Blockchain-Based Certificate Transparency and Revocation Transparency," in Financial Cryptography and Data Security, vol. 10958, Springer, Berlin, Heidelberg, 2019. Guided our design regarding transparency and future revocation features.
5. R. S. A. Omoka, "Application of permissioned blockchain technology on population data consolidation and sharing," Doctoral dissertation, Strathmore University, 2020. Influenced our choice of a permissioned architecture for the Admin module.
6. Ø. Sæbø, "From promise to practice: humanitarian digital identities in the forced migration..." [Online]. Available: Research Gate. Provided insights into digital identity management.