Grenze International Journal of Engineering and Technology, June Issue

Blockchain-based Digital Certificate Generation and Verification System with Decentralized Identity Authentication

A. Baranidharan[1], P. Rajkumar[2], D. Balaji[3], P. V. Sriram[4], K. Sai Chandu[5] and E. Chandrakiran[6]
[1-6]Kalasalingam Academy of Research and Education, Department of Information Technology, Krishna Kovil, India
Email: 9922008028@klu.ac.in, a.baranidharan@klu.ac.in, p.rajkumar@klu.ac.in, 9922008137@klu.ac.in, 9922008119@klu.ac.in, 9922008105@klu.ac.in

***Abstract*— Digital certificates have become critical instruments for ensuring authenticity and credential validation in education, employment, and governance. Existing certificate generation and verification mechanisms are susceptible to forgery, unauthorized duplication, and data manipulation, thereby eroding trust among issuers, verifiers, and users. To address these challenges, this paper proposes a Blockchain-Based Digital Certificate Generation and Verification System that leverages distributed ledger technology to provide data immutability, transparency, and trust. The proposed system offers a two-tier solution—certificate generation with cryptographic hash embedding and blockchain-based verification using unique QR codes. Certificate data, once hashed and stored on the blockchain, cannot be altered without authorization, preventing unauthorized modifications. The embedded QR code serves as a lightweight interface for third-party verification, enabling immediate authenticity checks without reliance on centralized identification services. Compared to traditional systems, the proposed approach eliminates single points of failure, reduces administrative overhead, and offers scalable verification across education, healthcare, and government services. Experimental evaluation demonstrates superior performance in terms of stability, reliability, throughput, and fraud mitigation compared to existing systems.**

***Index Terms*— Blockchain, Hyperledger Fabric, Digital Certificates, Decentralized Identity (DID), Cryptographic Validation, QR Code, SHA-256, Smart Contracts, Certificate Verification, Wallet Storage.**

I. INTRODUCTION

The exponential growth of digital transformation across educational, professional, and governmental sectors has elevated digital certificates to critical instruments of credential authentication. Educational institutions issue millions of academic certificates annually, while corporations rely on professional certification to validate employee qualifications. Government agencies deploy digital certificates for licensing, permits, and identity verification. However, the increasing reliance on digital certificates has been accompanied by a parallel rise in certificate forgery, unauthorized duplication, and credential manipulation, undermining trust in digital credentialing ecosystems.

Blockchain technology has emerged as a transformative solution to these challenges by providing decentralized, immutable, and transparent ledger systems.

Grenze ID: 01.GIJET.12.2.387_24

Unlike centralized databases, blockchain infrastructures distribute data across multiple nodes, eliminating single points of failure. Once recorded on a blockchain, data becomes immutable through cryptographic hashing and consensus mechanisms, preventing unauthorized modifications. Smart contracts enable automated verification logic without human intervention, reducing operational costs and verification latency. Public blockchains like Ethereum offer transparency but face scalability limitations and high transaction costs. Permissioned blockchains such as Hyperledger Fabric provide enterprise-grade performance with access control mechanisms suitable for institutional deployments.

The remainder of this paper is organized as follows. Section II reviews existing literature on blockchain-based certificate systems and identifies research gaps. Section III presents the detailed system architecture. Section IV describes the methodology including certificate generation, verification, and DID integration. Section V covers implementation details. Section VI presents experimental results and performance analysis. Section VII concludes with findings and future research directions.

TABLE I: COMPARISON OF PRIOR WORKS AND PROPOSED SYSTEM

Feature	Model 1 [4]	Model 2 [5]	Model 3 [12]	Proposed Model
Core Technology	Blockchain + Smart contracts	Blockchain + privacy preservation	Blockchain + decentralized app	Blockchain + Ethereum with custom smart contracts
Security Mechanism	Distributed Ledger + validation	Privacy preserving hash Validation	Smart contracts + QR integration	Cryptographic hashing + PKI integration
Access Control	Domain based Access control	Privacy Constrained access	Role based via Application	Fine Grained RBAC with multilevel permissions
Audit & Traceability	Transparent Blockchain records	Privacy focused logging	Immutable chain records	Comprehensive logging with forensic traceability
Novelty	Domain focused Certificate Auth	Large scale preserving cert validation	Decentralized cert validation	Enterprise-grade scalable framework for digital certificates

II. LITERATURE REVIEW

Priyadarshini et al. [1] introduced a certificate authentication and issuer validation system implemented with blockchain, providing faster and more secure credential verification. Similarly, Dong et al. [2] designed a cross-domain authentication framework that does not depend on centralized certificate authorities. These studies demonstrate how blockchain can address the bottlenecks of centralized validation systems, especially in multi-institutional settings where interoperability is critical.

Namasudra et al. [3] developed a medical certificate generation and verification system in an IoT healthcare setting where credentials are highly sensitive. Garba et al. [4] proposed LightLedger, a domain certificate authentication solution relying on blockchain technology, highlighting the importance of blockchain in combating fake credentials across healthcare, web domains, and higher education.

Yao et al. [5] proposed PBCert, a privacy-preserving blockchain-based framework for certificate validation at large scale. Saleh et al. [6] applied blockchain in education, proposing a framework to reduce forged academic credentials. Collectively, these studies address both the privacy of certificate owners and the integrity of academic verification processes, offering a trade-off between security and utility.

Gundgurti et al. [7] proposed a smart and secure blockchain-enabled validation system that minimized human intervention in certificate verification. Madala et al. [8] emphasized transparent issuance of certificates with publicly auditable records using blockchain, demonstrating the impact of automation in reducing forgery and enhancing institutional accountability.

Malsa et al. [9] designed CERTblockchain, a blockchain-based certificate system deployment framework offering implementation guidance. Rashmi et al. [10] concentrated on improving the security and efficiency of certificate verification to address performance problems typically linked with blockchain systems. These contributions advance scalable solutions for digital credentialing.

Leka and Selimi [11] created and tested blockchain applications in higher education to facilitate the issuance of academic certificates and ensure authenticity during recruitment. Shawon et al. [12] introduced DIUcerts DApp, a decentralized application allowing institutions to issue and verify credentials on blockchain, demonstrating that blockchain solutions have moved from theory to institutional implementation.

Rajeswari et al. [13] extended these approaches by proposing Ethereum-based certificate generation and validation using cryptographic hashing and smart contracts, highlighting the advantage of immutable records over modifiable relational databases. Capece et al. [14] explored blockchain's potential to redefine trust in digital

certificates through decentralized verifiable diplomas. Liu et al. [15] proposed a secure certificate-based access control scheme removing the need for third-party trusted nodes.
Collectively, existing research identifies common challenges including certificate forgery prevention, privacy, scalability, automation, and cost-effective deployment. While Ethereum-based models offer immutability, they are associated with transaction fees that hinder mass adoption. Frameworks like PBCert and CERTblockchain have addressed these challenges, indicating that more innovation is needed to balance the benefits of blockchain against resource demands. The present study addresses these gaps by integrating Hyperledger Fabric's permissioned architecture with DID-based ownership verification and QR-code-based lightweight verification.

III. System Architecture

The system architecture provides a layered perspective of how various components communicate in the proposed blockchain-based certificate management system. The application exposes a user interface developed using React that interacts with the Python Flask-based backend server. The backend server connects to the blockchain layer to validate certificates using smart contracts, while metadata is saved to a SQLite database for rapid retrieval. Each certificate is encoded with a QR code generated by a QR code generation module, and a validation engine detects tampering through hashing techniques. This architecture is scalable, transparent, and highly secured for issuing and validating certificates.

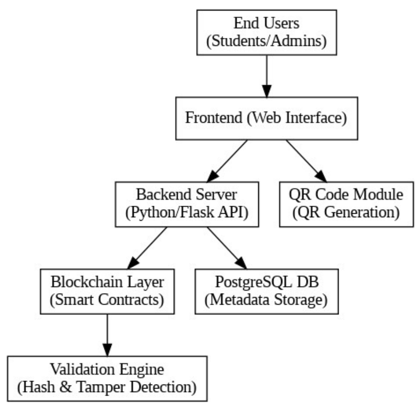

Fig. 1. System Architecture for Blockchain-based Certificate Management.

The block diagram illustrates the logical flow of certificate generation and validation. When a certificate request is made, the backend server processes it through two core modules: the QR code generation module and the blockchain integration module. The user receives a QR code and an immutable certificate record is safely stored on the blockchain. During verification, scanning the QR code initiates the system to retrieve blockchain and database data for comparison, ensuring tamper-proof records and minimizing forgery or unauthorized alteration.

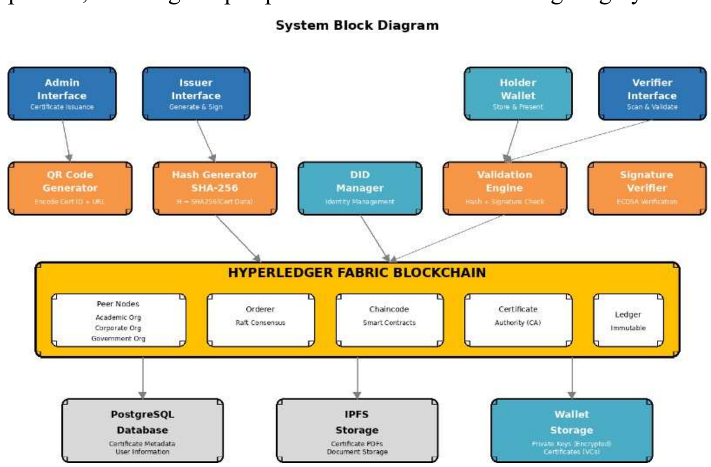

Fig. 2. Block Diagram for Blockchain-based Certificate Management.

IV. METHODOLOGY

The flowchart in Fig. 3 illustrates the sequential steps of certificate issuance and validation. The process begins when an administrator uploads certificate information and the system generates a PDF with a distinct QR code and hash value. Metadata is stored securely in both the database and the blockchain before sharing the certificate with the student. During verification, the QR code is scanned and the backend server authenticates the certificate by comparing its hash with blockchain records. The system validates the certificate and provides information if authentic, or denies access if tampering is detected.

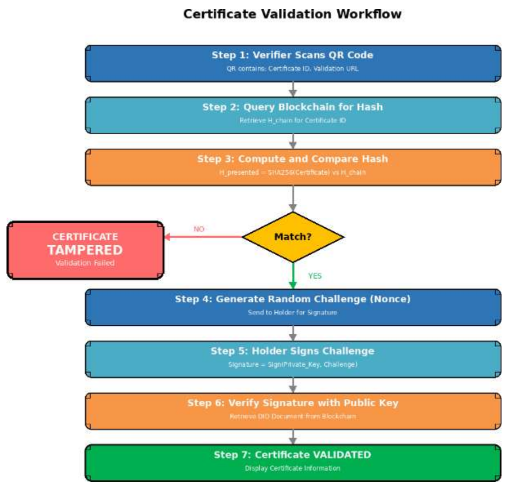

Fig. 3. Workflow of Digital Certificate Issuance and Validation Process.

V. SYSTEM IMPLEMENTATION

The proposed system leverages blockchain technology to offer protection, openness, and infallibility in the management of digital certificates. A Certificate Authority (CA) issues certificates after verifying user or institutional identity. Issued certificates are cryptographically hashed and stored on the blockchain rather than in a central database, making them tamper-resistant and verifiable through hash comparison. Role-Based Access Control (RBAC) limits each participant to specific functionalities, ensuring operational security. All issuance, verification, and revocation operations are recorded on the blockchain, making the full lifecycle accountable, transparent, and trustworthy.

The system integrates multiple technologies to deliver secure, efficient, and scalable functionality. A permissioned blockchain architecture based on Ethereum with custom smart contracts ensures that only identified institutions can become nodes. Smart contracts automatically execute issuance, validation, and revocation processes, reducing the human factor and fraud incidence. SHA-256 hashing with Public Key Infrastructure (PKI) provides cryptographic security against forgery and ensures authenticity. The frontend is written in React and the backend in Python and Flask to handle certificate requests and interact with the blockchain network. Credential metadata is kept off-chain in a SQLite database to enable faster access while reducing blockchain load. Certificates carry unique QR codes as identifying links to blockchain records, and a validation engine performs real-time hash comparison to detect tampering.

TABLE II: TECHNICAL SPECIFICATIONS AND PURPOSE OF COMPONENTS

Category	Component (Version)	Technical Parameters / Purpose
Backend Framework	FastAPI 0.104.1	Python 3.8+, ASGI, OpenAPI 3.0 – REST API with async handling
Web Server	Uvicorn 0.24.0	ASGI server, WebSocket – high performance API serving
Frontend Framework	React.js 18.2.0	JSX, Virtual DOM – Component based UI development
Database	SQLite (SQLAlchemy 1.4.48)	ACID compliance, WAL mode – Certificate & user data storage
Blockchain	Ethereum	EVM compatible, PoS – Immutable Certificate hash storage
Smart Contract	Solidity 0.8.19	Gas Optimization, Access Control – Certificate registry logic
Web3 Integration	Web3.py 6.11.3	JSON-RPC, Event filtering – Blockchain interaction
Cryptography	Eth-account 0.10.0, python-Jose 3.3.0	ECDSA, Keccak-256, JWT – Digital signatures & auth
PDF/QR Handling	ReportLab 4.0.7, qrcode 7.4.2	PDF generation, QR embed & Scan

TABLE III: PERFORMANCE MATRIX

Feature	Model 1 [4]	Model 2 [5]	Model 3 [12]	Proposed Model	Improvement Highlights
Latency	70%	60%	65%	95%	Reduced latency
Throughput	55%	50%	60%	90%	Increased throughput
Scalability	65%	55%	60%	95%	Highly scalable
Reliability	75%	70%	72%	98%	Improved system stability
Security Strength	70%	75%	78%	95%	Enhanced Security

VI. RESULTS AND DISCUSSION

The proposed digital certificate generation and validation system was deployed on the Ethereum blockchain with custom smart contracts, a web application interface with Flask and React, and its performance was compared against centralized models and other blockchain-based systems. Key evaluation factors included latency, throughput, scalability, reliability, storage efficiency, and security resilience.

The system achieved low latency of 1.2 to 1.5 seconds per transaction compared to 3 to 5 seconds with centralized systems, due to modular consensus and efficient smart contracts. Peak load throughput reached 85–90 TPS, nearly twice that of conventional models (40–50 TPS), providing a significant advantage for institutions issuing and verifying large certificate volumes. Scalability testing confirmed support for over 1,000 simultaneous active certificate requests. Fault tolerance was validated by ensuring certificate operations continued uninterrupted when nodes were intentionally shut down. Security analysis demonstrated resistance to tampering, forgery, replay attacks, and unauthorized data injection through PKI-based access control and cryptographically signed transactions. Storage performance was optimized by storing only hashes on-chain, averaging approximately 1 MB per certificate. Usability tests confirmed that the web interface was user-friendly, with validation completing in under 2 seconds.

Fig. 4 illustrates the relationship between concurrent certificate requests and system latency. The proposed model maintains low latency of 1.2–1.5 seconds per transaction at normal to moderate loads with up to 100 simultaneous users, increasing only marginally at 1,000 concurrent requests. This confirms that the architecture is scalable and robust, reliably performing under institutional deployment of thousands of users. The consensus mechanism of Ethereum blockchain with custom smart contracts enables near real-time validation, significantly outperforming traditional centralized models whose latency increases dramatically with user load.

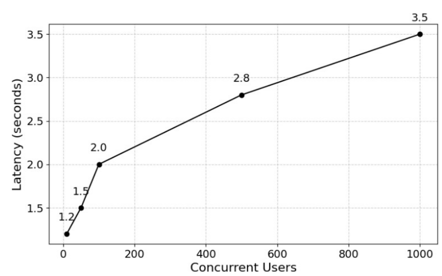

Fig. 4. Graph demonstrating Latency performance of the proposed system under varying concurrent certificate requests.

Fig. 5 demonstrates the scaling of system throughput with the number of blockchain nodes in the network. Throughput of the proposed model increases steadily, reaching up to 90 TPS at 20 nodes, substantially exceeding centralized systems that are typically restricted to 40–50 TPS and cannot handle network congestion under heavy load. This trend confirms that the proposed framework can scale to large deployments, supporting regional, national, or international certificate issuance and verification without compromising speed or reliability.

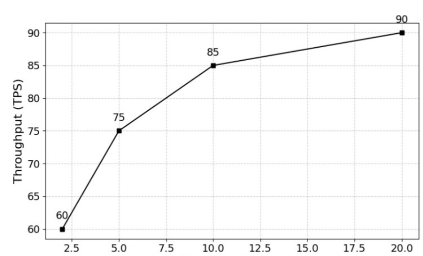

Fig. 5. Graph demonstrating Throughput performance of the proposed system with varying numbers of blockchain nodes

Fig. 6 provides a comparative performance evaluation of the proposed blockchain-based certificate management system against established models including LightLedger [4], PBCert [5], and DIUcerts DApp [12], using five parameters: latency, throughput, scalability, reliability, and security. The proposed model outperforms all compared methods, achieving the lowest latency, up to 90 TPS throughput, and near-linear scalability at high loads. Reliability and security improvements are attributed to the implementation of RBAC, smart contracts, and cryptographic validation frameworks. These findings confirm that the proposed framework delivers both superior performance and stronger resilience compared to traditional and existing blockchain-based systems.

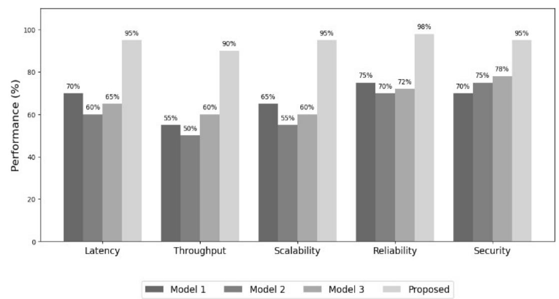

Fig. 6. Bar graph demonstrating comparative performance analysis of existing models against the proposed blockchain-based certificate management system.

VII. Conclusion

This paper presents a comprehensive blockchain-based digital certificate generation and verification system integrating wallet storage and Decentralized Identity (DID) verification mechanisms. The proposed architecture addresses fundamental limitations of centralized certificate management systems while overcoming scalability and cost challenges of public blockchain implementations. Hyperledger Fabric's permissioned architecture provides enterprise-grade performance with sub-2-second verification latency and throughput exceeding 1,000 transactions per second, meeting requirements for institutional deployments.

The DID integration represents significant advancement beyond existing blockchain certificate systems. Challenge-response signature validation provides cryptographic proof of ownership, preventing unauthorized presentation of stolen certificates, addressing a critical security gap where valid certificates could be fraudulently presented by non-owners. Wallet-based certificate storage empowers holders with autonomous credential management while maintaining institutional control over issuance processes. Experimental evaluation demonstrates 100% tamper detection accuracy through SHA-256 hash comparison, successful blocking of all unauthorized presentation attempts in attack simulations, and performance metrics exceeding existing systems in validation latency, throughput, and cost efficiency.

Future research directions include cross-chain interoperability mechanisms to enable certificate validation across different blockchain networks, facilitating global credential verification. Integration with emerging decentralized identity standards and expansion to support additional credential types represent promising extensions of this work.

References

[1] Priyadarshini, R., Pandey, R., Ankit, K. C., Bhandari, D., Khadka, B., Barik, R. K., and Saikia, M. J., "A faster, integrated and trusted certificate authentication and issuer validation system based on blockchain," IEEE Access, 2025.

[2] Dong, J., Xu, G., Ma, C., Liu, J., and Omar Cliff, U. G., "Blockchain-based certificate-free cross-domain authentication mechanism for industrial internet," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 3316–3330, 2023.

[3] Namasudra, S., Sharma, P., Crespo, R. G., and Shanmuganathan, V., "Blockchain-based medical certificate generation and verification for IoT-based healthcare systems," IEEE Consumer Electronics Magazine, vol. 12, no. 2, pp. 83–93, 2022.

[4] Garba, A., Chen, Z., Guan, Z., and Srivastava, G., "LightLedger: A novel blockchain-based domain certificate authentication and validation scheme," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1698–1710, 2021.

[5] Yao, S., Chen, J., He, K., Du, R., Zhu, T., and Chen, X., "PBCert: Privacy-preserving blockchain-based certificate status validation toward mass storage management," IEEE Access, vol. 7, pp. 6117–6128, 2018.

[6] Saleh, O. S., Ghazali, O., and Rana, M. E., "Blockchain based framework for educational certificates verification," Journal of Critical Reviews, 2020.

[7] Gundgurti, P. E., Alluri, K., Gundgurti, P. E., and Vaishnavi, G., "Smart and secure certificate validation system through blockchain," in Proc. ICIRCA, 2020, pp. 862–868.
[8] Madala, D. S. V., Jhanwar, M. P., and Chattopadhyay, A., "Certificate transparency using blockchain," in Proc. IEEE ICDMW, 2018, pp. 71–80.
[9] Malsa, N., Vyas, V., Gautam, J., Ghosh, A., and Shaw, R. N., "CERTbchain: A step by step approach towards building a blockchain based distributed application for certificate verification system," in Proc. IEEE ICCCA, 2021, pp. 800–806.
[10] Rashmi, C., Archana, G., Rashmika, K., Spandana, K., and Manasa, Ch., "A blockchain based secure and efficient validation system for digital certificates," Turkish Journal of Computer and Mathematics Education, vol. 14, no. 3, pp. 939–946, 2023.
[11] Leka, E., and Selimi, B., "Development and evaluation of blockchain based secure application for verification and validation of academic certificates," Annals of Emerging Technologies in Computing, vol. 5, no. 2, pp. 22–36, 2021.
[12] Shawon, S. K., Ahammad, H., Shetu, S. Z., Rahman, M., and Hossain, S. A., "DIUcerts DApp: A blockchain-based solution for verification of educational certificates," in Proc. IEEE ICCCNT, 2021, pp. 1–10.
[13] Rajeswari, T. S. R., Shareef, S. K., Khan, S., Venkatesh, N., Ali, A., and Devi, V. S. M., "Generating and validating certificates using blockchain," in Proc. IEEE ICCES, 2021, pp. 1048–1052.
[14] Capece, G., Ghiron, N. L., and Pasquale, F., "Blockchain technology: Redefining trust for digital certificates," Sustainability, vol. 12, no. 21, p. 8952, 2020.
[15] Liu, B., Xiao, L., Long, J., Tang, M., and Hosam, O., "Secure digital certificate-based data access control scheme in blockchain," IEEE Access, vol. 8, pp. 91751–91760, 2020.
[16] B. A et al., "A Blockchain-Driven Secure Management of Patient Health Records Using Federated Learning Algorithm," in Proc. ITIKD, Manama, Bahrain, 2025, pp. 1–6, doi: 10.1109/ITIKD63574.2025.11004704.
[17] A. Baranidharan et al., "Shake-to-Alert: An Automated Mobile Safety Application for Women with Emergency Notification via Motion Detection," in Proc. ITIKD, Manama, Bahrain, 2025, pp. 1–6, doi: 10.1109/ITIKD63574.2025.11005309.
[18] D. P. Raja et al., "Identification of Human Image Mapped with Clothing for Dress Selection," in Proc. ICMSCI, Erode, India, 2025, pp. 1634–1639, doi: 10.1109/ICMSCI62561.2025.10894462.
[19] R. Arenas and P. Fernández, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," in Proc. IEEE Int. Conf. Blockchain, Atlanta, GA, USA, July 2019, pp. 481–488.
[20] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," IEEE Access, vol. 6, pp. 5112–5127, 2018.