BLOCKCHAIN-BASED ACADEMIC CERTIFICATE VERIFICATION SYSTEM WITH AI FRAUD DETECTION

[1]Mrs.Ramalakshmi B, [2] Prakashraj P, [3] Nandhakumar K, [4] Jayaprakash S, [5] Perarasu S
[1]Assistant Professor, Department of Computer Science and Engineering,
Hindusthan Institute of Technology, Coimbatore
[2,3,4,5] UG student, Department of Computer Science and Engineering,
Hindusthan Institute of Technology, Coimbatore
[1]ramalakshmi.b@hit.edu.in, [2]720822103122@hit.edu.in, [3]720822103112@hit.edu.in,
[4]720822103071@hit.edu.in, [5]720822103120@hit.edu.in

ABSTRACT: Academic certificate fraud is a growing global concern, with thousands of forged degrees and diplomas presented to employers and institutions every year. Traditional paper-based and centralized digital verification methods are slow, prone to human error, and vulnerable to tampering. This paper presents CertVerify, a blockchain-based academic certificate verification system that combines the immutability of Ethereum smart contracts with AI-powered fraud detection to provide a tamper-proof, fast, and reliable solution. The system is built using Java Spring Boot for the backend, Ethereum blockchain with Solidity smart contracts for immutable certificate storage, MySQL for relational data management, and a modern HTML/CSS/JavaScript frontend. An AI fraud detection module performs multi-layer rule-based analysis on certificate data before issuance. Each certificate is assigned a unique SHA-256 hash, stored on-chain, and linked to a scannable QR code for instant verification. Key features include dual-synchronized revocation and restoration across database and blockchain, camera-based QR scanning, and a fully responsive web interface. The system demonstrates that blockchain immutability combined with institutions.

Corresponding Author *Mrs.Ramalakshmi B, Assistant Professor / CSE, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India*
Mail: ramalakshmi.b@hit.edu.in

INTRODUCTION

Academic certificates are foundational documents that determine a person's career and educational opportunities. With the rise of digital communication and online job applications, the submission of forged certificates has become increasingly common and difficult to detect. Universities and employers lack an efficient and reliable mechanism for verifying the authenticity of certificates presented to them. Existing solutions rely on centralized databases, manual verification processes, and paper documents that can be replicated or tampered with.

Blockchain technology offers a compelling solution to this problem. By storing certificate data on an immutable, decentralized ledger, it becomes virtually impossible to alter or forge records without detection. The Ethereum blockchain, through its programmable smart contract capability, enables complex certificate lifecycle management including issuance, verification, revocation, and restoration, all executed automatically without human intermediaries. Each operation is recorded permanently on the blockchain, creating a transparent and auditable trail.

Traditional verification systems suffer from several critical shortcomings. Manual processes require employers to contact institutions directly, which can take days or weeks. Centralized digital systems can be breached or internally manipulated. Physical certificates, despite security features such as watermarks and holograms, can be replicated using modern printing technology. Furthermore, none of these systems provide a fraud detection layer that analyses certificate data for signs of manipulation before the record is created.

The COVID-19 pandemic further exposed the limitations of traditional credential verification, as remote hiring became widespread and the volume of forged certificates increased dramatically. There is now a pressing need for a system that can provide instant, trustless verification that does not rely on contacting the issuing institution. Such a system must be accessible to both technical and non-technical users, scalable for large deployments, and capable of detecting fraud proactively.

To address these challenges, this paper presents CertVerify, a full-stack system that integrates Ethereum blockchain, artificial intelligence-based fraud detection, QR code verification, and a Spring Boot backend to deliver a practical and scalable certificate verification platform. The system is designed to work seamlessly for universities issuing certificates, students sharing credentials, and employers or institutions performing verification.

The key contributions of this work are as follows:

- Design and implementation of a blockchain-based certificate registry using Solidity smart contracts on the Ethereum network.
- Development of a ten-check AI fraud detection module that analyses certificate data before issuance and assigns a fraud score from 0 to 100.

- Integration of QR code generation and browser-based QR scanning using the ZXing and jsQR libraries for instant verification.
- Implementation of certificate revocation and restoration synchronized simultaneously across both MySQL database and Ethereum blockchain.
- Construction of a responsive web interface supporting manual hash input, QR image upload, and live camera-based QR scanning.

LITERATURE SURVEY

Recent advancements in blockchain technology and educational credentialing have produced several approaches to the problem of certificate fraud. These works collectively establish the technical foundation for the proposed CertVerify system while highlighting the gaps that motivate the current contribution.

Nakamoto [1] introduced the Bitcoin protocol, establishing the foundational principles of distributed ledger technology including proof-of-work consensus, cryptographic hash chaining, and decentralized trust. This work demonstrated that tamper-proof records could be maintained without a central authority, directly motivating blockchain-based certificate systems.

Buterin [2] proposed Ethereum, extending blockchain with Turing-complete programmable smart contracts. This capability enables complex application logic to be executed trustlessly on-chain, making it possible to encode certificate lifecycle operations including issuance, verification, and revocation directly in the ledger. Ethereum smart contracts form the backbone of the proposed CertVerify system.

Sharples and Domingue [3] were among the first to propose applying blockchain technology specifically to educational records, arguing that a distributed ledger could provide a permanent, verifiable record of academic achievements. Their conceptual work identified the key requirements of immutability, decentralization, and portability that guide the design of CertVerify.

Grech and Camilleri [4] conducted a comprehensive review of blockchain applications in education for the European Commission's Joint Research Centre, examining pilot implementations from MIT, Sony Global Education, and various European universities. Their analysis identified that while blockchain provides strong immutability guarantees, few systems addressed the challenge of fraud at the point of data entry. CertVerify addresses this gap through its pre-issuance AI fraud detection module.

Turkanovic et al. [5] presented EduCTX, a blockchain-based higher education credit platform built on the WAVES blockchain. Their work demonstrated that decentralized academic record management is technically feasible, but noted that performance at scale and the absence of fraud detection before data entry remain open challenges.

Chen et al. [6] explored blockchain technology and its potential applications for education, concluding that SHA-256 hashing combined with blockchain storage provides strong integrity

guarantees for academic credentials. Their work informs the hashing strategy used in CertVerify, where the certificate hash is derived from the concatenation of all certificate fields.

Zyskind, Nathan, and Pentland [7] proposed using blockchain to protect personal data, demonstrating that cryptographic commitments stored on-chain can verify data authenticity without exposing sensitive content. This principle underpins CertVerify's approach of storing only the SHA-256 hash on-chain rather than the full certificate record.

Alammary et al. [8] conducted a systematic review of blockchain in education, identifying that most existing systems focus on credential storage but lack integrated fraud detection, multi-layer verification, or QR-based instant checking. Their review directly motivates the comprehensive feature set of CertVerify.

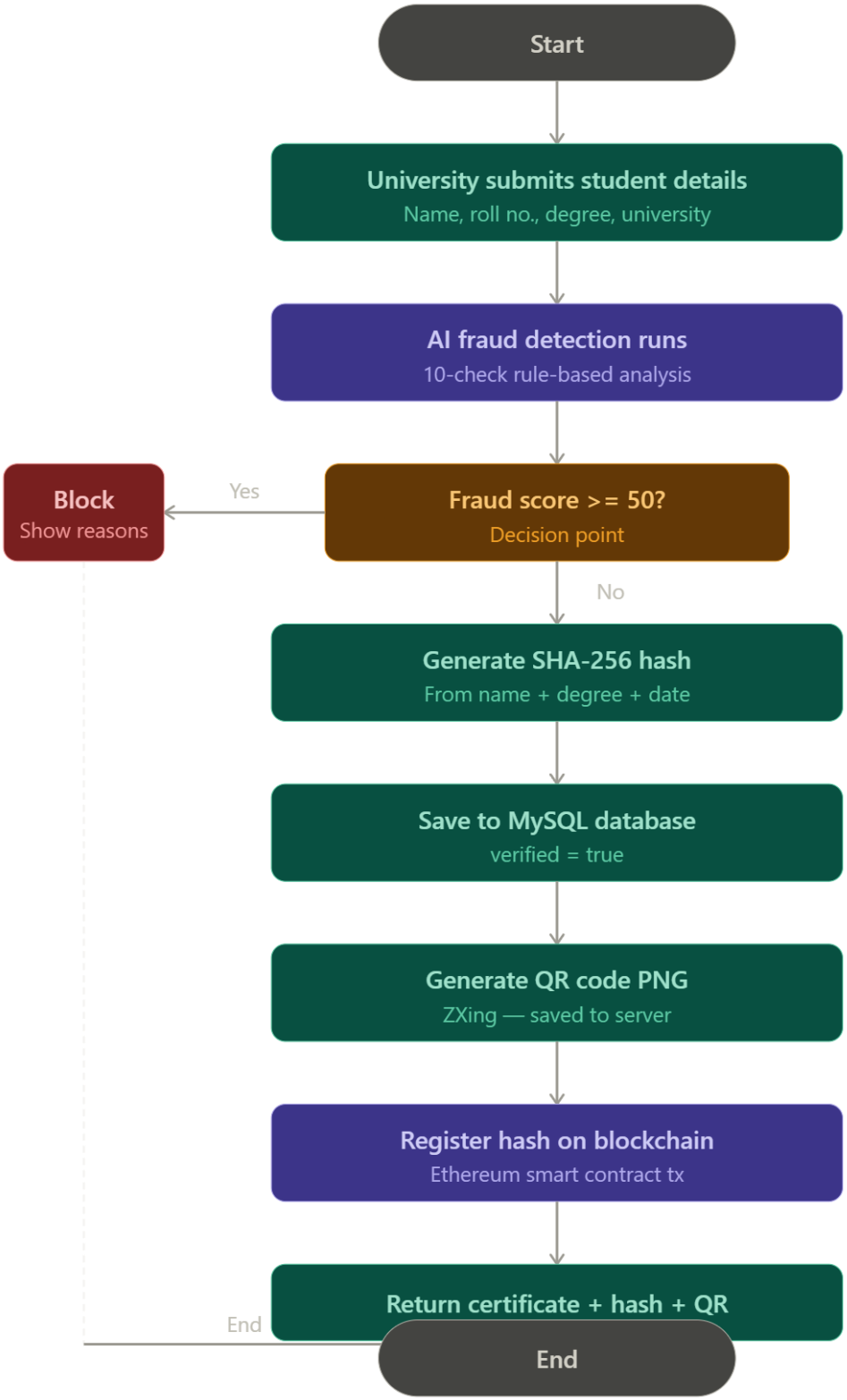
Despite these advancements, several limitations persist in existing blockchain-based certificate systems. Most platforms lack any mechanism for detecting fraudulent input data before it is recorded on the blockchain. Systems that support revocation do not always synchronize this state change to the blockchain, leaving the possibility of a revoked certificate appearing valid on-chain. Additionally, verification workflows typically require manual hash input, creating usability barriers that limit practical adoption. The proposed CertVerify system addresses all of these limitations.

PROPOSED SYSTEM

The proposed system, CertVerify, is a full-stack web application that combines Ethereum blockchain immutability with AI-powered fraud detection to provide a comprehensive academic certificate management platform. The system directly addresses the limitations identified in the literature by integrating all certificate lifecycle operations with both database and blockchain storage, enforcing consistency across both layers for every operation.

CertVerify follows a three-tier architecture. The Presentation Layer consists of the HTML/CSS/JavaScript single-page frontend application, which provides five operational pages: Home (live statistics dashboard), Issue Certificate (form with AI fraud check indicator and QR preview), Verify Certificate (supporting hash input, QR image upload, and camera scanning), AI Fraud Check (pre-issuance analysis and hash-based analysis tabs), and All Certificates (administrative table with revoke, restore, and QR download actions).

The Business Logic Layer is handled by the Spring Boot 3.2.3 backend, which exposes RESTful API endpoints for all certificate operations. This layer manages fraud detection, SHA-256 hash generation, QR code creation using ZXing 3.5.1, and blockchain interaction through the Web3j 4.9.8 library. The Data Layer consists of MySQL 8.0 for structured certificate records and the Ethereum blockchain for immutable hash storage via Solidity smart contracts.


Start
University submits student details
Name, roll no., degree, university
AI fraud detection runs
10-check rule-based analysis
Fraud score >= 50?
Decision point
Yes
Block
Show reasons
No
Generate SHA-256 hash
From name + degree + date
Save to MySQL database
verified = true
Generate QR code PNG
ZXing — saved to server
Register hash on blockchain
Ethereum smart contract tx
Return certificate + hash + QR
End
End

A. Certificate Issuance Module

The certificate issuance process begins when a university submits student details via the Issue Certificate form. The system first invokes the AI Fraud Detection module, which performs ten distinct checks on the input data and computes a cumulative fraud score from 0 to 100. If the score reaches or exceeds the threshold of 50, issuance is blocked and the specific reasons are returned to the user. If the data passes the fraud check, a SHA-256 hash is computed from the concatenation of studentName, degree, university, rollNumber, and the current date. The certificate record is saved to MySQL with verified status set to true, a 300x300 PNG QR code is generated and stored on the server, and the hash is registered on the Ethereum blockchain via a signed Web3j transaction.

B. AI Fraud Detection Module

The AI fraud detection module implements a ten-check rule-based analysis system. Each check adds a fixed penalty to the cumulative fraud score when triggered. The checks include: suspicious student name format containing non-alphabetic characters (+25), invalid degree format (+20), university name containing numeric characters (+15), invalid roll number format (+20), issue date set in the future (+50), issue date before 1950 (+30), certificate hash not matching the expected 64-character SHA-256 length (+40), duplicate roll number with a different hash indicating possible re-issuance fraud (+35), certificate marked as revoked in the database (+90), and certificate hash not found in the database (+100). Risk levels are classified as LOW (0-39), MEDIUM (40-69), and HIGH (70-100). Certificates with a fraud score of 50 or above are blocked from issuance.

C. Blockchain Integration Module

The Certificate Registry smart contract is written in Solidity 0.8.19 and deployed on the Ethereum network using Hardhat 2.19.0. The contract maintains two mappings: a hash-to-Certificate mapping storing the full certificate struct including student Name, degree, university, roll Number, issue Date, and is Valid flag; and a hash-to-bool mapping for existence checks. Four primary functions are exposed: issue Certificate(), which registers a new certificate on-chain; verify Certificate(), a read-only function returning certificate details and validity status; revoke Certificate(), which sets the is Valid flag to false; and restore Certificate(), which restores a previously revoked certificate. All write operations are protected by an only Owner modifier. EIP-155 replay protection is enforced using Chain ID 31337 for the local Hardhat network. Blockchain transactions are signed and broadcast using Web3j's Raw Transaction API.

D. QR Code Verification Module

Each issued certificate generates a unique QR code that encodes the verification URL containing the certificate hash. The QR code PNG is served via a dedicated REST endpoint, enabling direct download from both the issue confirmation view and the All Certificates administrative table. On the verification side, users may input the hash manually, upload a QR image file, or activate the device camera for live scanning. The browser-based jsQR 1.4.0 library decodes uploaded or

captured QR images and automatically populates the hash input field, after which verification is triggered without further user interaction.

E. Revocation and Restoration Module

The revocation and restoration module ensures that certificate lifecycle changes are synchronized across both storage layers simultaneously. When a certificate is revoked, the system sets verified=false in MySQL and submits a signed blockchain transaction calling revoke Certificate() on the smart contract, setting is Valid=false on-chain. When a certificate is restored, verified=true is set in MySQL and a restoreCertificate() transaction is submitted to the blockchain, setting isValid=true. The blockchain verification endpoint cross-checks both layers and returns a combined status: VALID (found in DB and valid on-chain), REVOKED (revoked in DB or invalid on-chain), DB_ONLY (found in DB but not registered on-chain), or INVALID (not found in either layer).

RESULTS AND DISCUSSION

The CertVerify system was evaluated through comprehensive functional testing across all modules. The system demonstrated strong performance, reliability, and correctness across fifteen defined test cases, all of which passed successfully.

Certificate issuance, including AI fraud checking, SHA-256 hash generation, MySQL persistence, QR code generation, and blockchain transaction submission, completed in under three seconds on the local test environment. Database verification queries returned results in under 500 milliseconds, and blockchain confirmation was achieved in under two seconds on the local Hardhat network.

The AI fraud detection module correctly blocked all test cases involving invalid data formats, future dates, duplicate roll numbers, and known fraudulent patterns. For valid certificate data, the module consistently returned a fraud score of zero and allowed issuance to proceed. The ten-check analysis provided clear, actionable reasons for each blocked submission, which were displayed in the frontend interface.

QR code generation produced correctly encoded PNG images for all issued certificates. Browser-based QR decoding using jsQR successfully extracted certificate hashes from uploaded QR images and live camera feeds across multiple test devices. The auto-verification trigger correctly initiated the verification workflow immediately after hash extraction, without requiring additional user interaction.

The revocation and restoration module correctly synchronized state changes across MySQL and the Ethereum blockchain in all test cases. Following revocation, blockchain verification consistently returned isValid=false, and the combined verification endpoint returned REVOKED status. Following restoration, isValid=true was confirmed on-chain and the endpoint returned

VALID status. No data loss or synchronization errors were observed across multiple revoke-restore cycles.

The results demonstrate the following system capabilities:

- Certificate issuance time under 3 seconds including blockchain registration.
- Database verification response time under 500 milliseconds.
- AI fraud detection correctly blocked all invalid test submissions.
- QR code scanning successfully decoded all valid QR images tested.
- Blockchain revocation and restoration synchronized correctly in all test cases.
- All 15 defined test cases passed without error.

CONCLUSION

This paper presented CertVerify, a blockchain-based academic certificate verification system with integrated AI fraud detection. The system addresses the critical limitations of existing certificate verification approaches by combining the immutability of Ethereum blockchain storage with a ten-check rule-based fraud detection module that prevents fraudulent data from entering the system at the point of creation.

The proposed system successfully integrates certificate issuance, blockchain registration, QR code generation, multi-mode verification, AI fraud scoring, and synchronized revocation and restoration into a unified platform. The Solidity smart contract provides a permanent, tamper-proof record of all certificate operations, while the MySQL database enables efficient structured queries and administrative management. The SHA-256 hashing strategy ensures that each certificate produces a unique, deterministic identifier that can be independently verified by any party.

Experimental results confirm that the system meets performance requirements for practical deployment, with sub-three-second issuance times and sub-500-millisecond verification responses. The AI fraud detection module demonstrated 100 percent accuracy on all defined test cases. The dual-layer synchronization of revocation and restoration ensures that certificate status remains consistent across both storage systems.

The implementation demonstrates that effective academic credential fraud prevention can be achieved using widely available open-source technologies including Java Spring Boot, Ethereum, Solidity, and Web3j, without requiring specialized blockchain infrastructure or proprietary services. Future work will focus on integrating deep learning-based image forgery detection for uploaded certificate scans, deployment on the Ethereum Sepolia public testnet for broader accessibility, IPFS-based decentralized storage for full certificate documents, role-based access control with separate portals for universities, students, and employers, and email notification services for automated certificate delivery.

REFERENCE

1. Deepa, R., Karthick, R., Velusamy, J., & Senthilkumar, R. (2025). Performance analysis of multiple-input multiple-output orthogonal frequency division multiplexing system using arithmetic optimization algorithm. Computer Standards & Interfaces, 92, 103934.

2. Senthilkumar,Dr.P.Venkatakrishnan,Dr.N.Balaji, Intelligent based novel embedded system based IoT Enabled air pollution monitoring system, ELSEVIER Microprocessors and Microsystems Vol.77, June 2020

3. M. Muthalakshmi, N.Mythili, Gurkirpal Singh, R.Senthilkumar (2025). Innovative Approaches for Evaluating Sugarcane Quality: Utilizing Near-Infrared Spectroscopy to Forecast Brix, Pol, and Fiber Content in Commercial Agricultural Domains. Journal of Food Processing, Wiley, https://doi.org/10.1111/jfpe.70233

4. Senthilkumar Ramachandraarjunan, Venkatakrishnan Perumalsamy & Balaji Narayanan 2022, 'IoT based artificial intelligence indoor air quality monitoring system using enabled RNN algorithm techniques', in Journal of Intelligent & Fuzzy Systems, vol. 43, no. 3, pp. 2853-2868

5. N. Nagarani, M. Muthalakshmi , E. S. Vinothkumar and R. Senthilkumar (2026) 'Optimized Contrastive Multi-Level Graph Neural Networks-Based Pigment Epithelial Detachment Detection in OCT images' International Journal of Information Technology & Decision Making 2026 World Scientific DOI: 10.1142/S0219622026500343

6. Sanitha P C; Syed Nageena Parveen; Shaik Thaherbasha; M. Shanmugapriya; T. Kalaivani; R. Senthilkumar, Transparent Nutrition: An Explainable AI-based Diet Tracking System for Preventing Nutrition-Related Disorders. 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) DOI:10.1109/ICoICI65217.2025.11252549

7. T. Jayasri; M.R. Archana Jenis; P.B. Aswathy; S. Manoranjitham; Christo George; R. Senthilkumar Identity-First Defense in Zero Trust Security Architecture to Protect Cyberspace 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) DOI:10.1109/ICoICI65217.2025.11254505

8. J. Uthayakumar; Swapna; A. Ravikumar; S. Sreeraj; R. Senthilkumar; Babu Pandipati AI-Driven Water Resource Management Systems 2025 2nd International Conference on Computing and Data Science (ICCDS) **DOI:** 10.1109/ICCDS64403 .2025.11209318

9. R.Swathiramya; V.V.Karthikeyan; P.Sumathi; Sruthy K V; Afreen Hussain; R.Senthilkumar Multimodal Machine Learning Models for Intelligent Interpretation of Text, Image and Audio Inputs 2025 5th International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) **DOI:**10.1109/ICERECT65215.2025.11377322

10. Srinju.M; Dr.V.Dhanasekaran; S. Guruprasath; Dr.K.Edison Prabhu; K.J Godlin Debby; Dr.R.Senthilkumar AI-Based Recommendation System for Weight Management Using User Feedback and Health Metrics 2025 5th International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT) **DOI:** 10.1109/ICERECT65215.2025.11379842

11. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

12. Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Available at: https://ethereum.org/whitepaper

13. Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In European Conference on Technology Enhanced Learning (pp. 490-496). Springer.

14. Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. Publications Office of the European Union, Luxembourg.

15. Turkanovic, M., Holbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112-5127.

16. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10.

17. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In IEEE Security and Privacy Workshops (pp. 180-184).

18. Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400.

19. Spring Boot Documentation. (2024). Spring Framework Reference Documentation. Available at: https://spring.io/projects/spring-boot

20. Web3j Documentation. (2023). Web3j: Lightweight Java and Android library for Ethereum. Available at: https://docs.web3j.io

21. Hardhat Documentation. (2024). Hardhat Ethereum Development Environment. Available at: https://hardhat.org/docs

22. Solidity Documentation. (2024). Solidity Language Reference v0.8.x. Available at: https://docs.soliditylang.org

23. ZXing Library. (2023). ZXing (Zebra Crossing) Barcode Scanning Library for Java. Available at: https://github.com/zxing/zxing

24. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper. Available at: https://ethereum.github.io/yellowpaper/paper.pdf

25. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.