International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain-based system for Secure Document Verification using QR codes

Chaitanya Raghuvanshi
Department of Information Technology
Pune Institute of Computer Technology
Pune, India
chaitanyaraghuvanshi88@gmail.com

Sai Shelar
Department of Information Technology
Pune Institute of Computer Technology
Pune, India
saisanjayshelar@gmail.com

Tanmay Sonanis
Department of Information Technology
Pune Institute of Computer Technology
Pune, India
tanmaysonanis186@gmail.com

Yash Rathod
Department of Information Technology
Pune Institute of Computer Technology
Pune, India
yashrathod@gmail.com

Mrs. Rashmi Chhattani
Department of Information Technology
Pune Institute of Computer Technology
Pune, India
rschhattani@pict.edu

***Abstract*—Employers now face significant difficulties in confirming educational credentials in today's competitive labor market, especially when hiring a large number of recent graduates. Businesses are frequently burdened with expensive and time-consuming procedures to verify the legitimacy of credentials like degrees and transcripts. A more effective, secure, and trustworthy method of confirming academic credentials is becoming more and more necessary as fake certificates become more common. In order to counter the spread of phony credentials, this paper promotes the creation of a blockchain-enabled digital certificate verification system. Digital certificates will be created by the system and stored in a blockchain-based setting, offering a decentralized, transparent, and impenetrable verification process.Employers, educational institutions, and other stakeholders will be able to verify each certificate in real time thanks to its secure blockchain storage and dynamic QR code identification. The suggested remedy entails building a unique blockchain on an open-source platform with a customized mining approach to improve security and performance. Controlled updates will be made possible by smart contracts, enabling authorized parties to make required modifications while maintaining the integrity of the blockchain. This dynamic approach guarantees that educational records can be updated without jeopardizing the security or legitimacy of certificates that have already been issued. This system will drastically cut down on the time, effort, and expenses associated with conventional verification techniques by utilizing blockchain's immutability and decentralization.It also provides businesses and educational institutions with a scalable solution that expedites the verification process and increases confidence in the legitimacy of educational records.**

***Index Terms*—Blockchain, Smart Contracts, Dynamic QR Code, E-Certificate, Immutability.**

I. Problem Statement

Fake educational certificates are a major problem in the current system, especially in India where it is relatively simple to obtain fraudulent certificates. Businesses that hire a lot of recent graduates frequently invest a lot of money in confirming the legitimacy of their transcripts and certificates of education. We suggest utilizing blockchain technology to implement a Digital Certificate System in order to address this issue. This solution can effectively address the problem of phony credentials by offering a safe and trustworthy way to validate educational credentials.

II. Introduction

Verifying the legitimacy of candidates' educational credentials is becoming more and more difficult for businesses in today's fast-paced, international labor market, especially when hiring a large number of recent graduates. Because it is now easier to create and more difficult to identify fraudulent academic documents, the issue of fake certificates has gotten worse.

Traditional certificate verification techniques are ineffective because they depend on manual inspections or outside verification organizations, both of which can be expensive, time-consuming, and prone to human error. For companies, the inability to quickly and accurately confirm educational credentials jeopardizes the hiring process and raises concerns about the integrity and performance of employees. To expedite the process of verifying academic documents while maintaining their authenticity, a safe, scalable, and automated solution is therefore desperately needed.

By offering a decentralized, transparent, and indestructible platform for the storage and validation of digital certificates, blockchain technology presents a promising solution for this problem. Businesses and educational institutions can create a Digital Certificate Verification System that eliminates the risk of fraud and drastically cuts down on the time and expense involved with conventional verification methods by utilizing blockchain's immutability. Dynamic QR-coded digital certificates will be issued by this system and stored on a specially created blockchain, guaranteeing that authorized parties can safely access and validate the certificates in real

time. A custom blockchain with a special mining approach designed to maximize security and performance in the context of educational certificate verification is proposed in this paper, which investigates the design and implementation of such a system on an open-source platform.

The primary objectives of this project are:

- To design and develop a dynamic and secure e-certificate generation system using smart contracts within a blockchain environment.
- To create a custom blockchain on an open-source platform, incorporating a tailored mining strategy and smart contract functionality.
- To evaluate and analyze system performance through the use of a consensus algorithm for proof of validation.

III. Literature Survey

A. Blockchain and Smart Contract for Digital Certificate

A blockchain-based digital certificate system is suggested as a solution to the problem of certificate duplicates. This system makes use of the immutability of blockchain technology to guarantee that digital certificates are verifiable and anti-counterfeit. This system's digital certificate issuance procedure is as follows: First, a paper certificate's electronic version is created and saved in a database along with other pertinent information. The electronic file is then saved in a block on the blockchain after the system computes a hash value for it. In order to facilitate verification through mobile scanning or online inquiries, a matching QR code and inquiry string code are made and attached to the physical certificate.This system uses the immutable characteristics of blockchain technology to increase the legitimacy of paper-based certificates while also reduces the risk of certificate loss by providing secure electronic versions.

B. Security Applications and Challenges in Blockchain

Despite being widely known, blockchain technology is frequently misinterpreted, particularly with regard to its present and potential uses. Blockchain technology is used in many systems to improve security and privacy, but it has built-in drawbacks and new problems. This study looks at popular blockchain security applications, identifies the main problems they encounter, and talks about more general issues that could better direct future research.

C. Validation through Public Ledgers and Blockchains

Public key infrastructures (PKIs) are essential for enabling online services like cloud services, email, social networking, online banking, e-government, e-commerce, and more that rely on certificate-based authentication. Certificate revocation lists (CRLs), which must always be available and reliable whenever a certificate is used, are a significant weakness in contemporary PKIs. Typically, the certification authority (CA) is the only entity responsible for managing the CRL for a collection of certificates, which results in a single point of failure in the system. By keeping CRLs on a public, decentralized, and secure ledger, we offer a solution to this problem in which several CAs work together. We employ a public ledger model based on blockchain technology, which was initially created for cryptocurrencies and is currently being used more and more for online applications that demand high levels of security and reliability.

D. BlockSIM: A practical simulation tool for optimal network design, stability and planning

In this work, we introduce BlockSIM, a feature-rich open-source blockchain simulation tool that aids blockchain architects in assessing the functionality of suggested private blockchain networks. By running multiple scenarios, BlockSIM enables users to identify the best system parameters for their particular requirements. By contrasting the outcomes of the simulation with real blockchain networks, we demonstrate that BlockSIM is a useful tool for architects to design and build scalable, reliable, and resilient blockchain systems. We also present a real-world example showing how BlockSIM can be used for designing and planning useful blockchain networks.

E. Proof-of-Property- A Lightweight and Scalable Blockchain Protocol

The methodology put forward in this paper expands upon Ethereum's idea of explicitly preserving the state of the system in every block. By adding the pertinent part of the system state to new transactions, it expands on this concept. As a result, users can verify transactions without having to download the complete blockchain beforehand. Use cases that don't require an infinite and comprehensive transaction history but still call for scalable blockchain technology are supported by this method. Participants' storage and processing needs are thus greatly decreased. Additionally, by reducing data synchronization procedures, the system becomes more efficient and provides a more flexible and lightweight solution for blockchain applications that value scalability.

F. Blockchain and Smart Contract for Digital Document Verification

The proposed system would upload the person's complete behavioral and personality records, connected to their unique ID, to the blockchain in addition to their degree certificate. This data will be safely stored because blockchain technology is immutable. The student first submits their certificate or identification to the electronic certificate system in order to request an e-certificate. After the request is received, the system confirms the authenticity of the certificate with the relevant university, school, or organization and saves the serial number and e-certificate on the blockchain. After that, a QR code is created and sent to the user. The user only needs to submit the certificate's serial number and the QR code generated by the e-certificate system when applying to a company.

G. Using blockchain and smart contracts for secure data provenance management

In this study, we employ blockchain technology to facilitate safe and trustworthy source data management, verification, and collection. The Open Provenance Model (OPM) and smart contracts are used by the system to create unchangeable data trails. Assuming that most participants behave honorably, our suggested framework effectively collects and verifies provenance data, guaranteeing security and preventing malicious modifications.

H. Intelligent Data Storage in Electronic Voting Machine using Blockchain System

For use in city or national elections, we present in this paper an alternative electronic voting system that makes use of open-source blockchain technology. The blockchain-based system will be anonymous, dependable, and safe, with the goal of boosting public confidence in government and voter turnout. The system guarantees the integrity of votes cast by leveraging the immutability and transparency of blockchain technology. Additionally, it provides real-time auditing and monitoring capabilities, enabling stakeholders to confirm the election process at any point.

I. An Empirical Study of Blockchain-based Decentralized Applications

The paper offers a thorough empirical investigation of a dataset including 734 decentralized applications (dapps) gathered from three main open dapp markets: Ethereum, State of the Dapps, and DAppRadar. We have looked at dapp popularity and found trends in how smart contracts are set up inside dapps. Drawing from these revelations, we offer suggestions to enable users and developers to properly grasp and use dapps. We also look at elements affecting dapp market success or failure. Our research also draws attention to issues with scaling and maintaining dapps over time and offers optimization techniques to increase performance and user involvement.

J. sCompile: Critical Path Identification and Analysis for Smart Contracts

This paper offers a different approach to automatically find important program paths in smart contracts, including those with several function calls and inter-contract calls. Ranked by their criticality, the paths are presented to users with obvious alerts for examination; infeasible paths are thrown away. We consider paths including financial transactions to be critical and give priority to those that might violate important qualities. Symbolic execution is used just on the top-ranked critical paths to guarantee scalability. A tool called sCompile has put this method into practice; it has been tried on 36,099 smart contracts.

IV. Proposed Methodologies

A. Introduction to Methodology

In this section, we describe the approaches used to plan, create, and deploy a safe and effective blockchain and QR code-based digital document verification system. The procedures followed guarantee a methodical approach to achieving the goals of improved security, tamper-proof validation, and dynamic certificate generation.

B. Development Approach : WaterFall Model

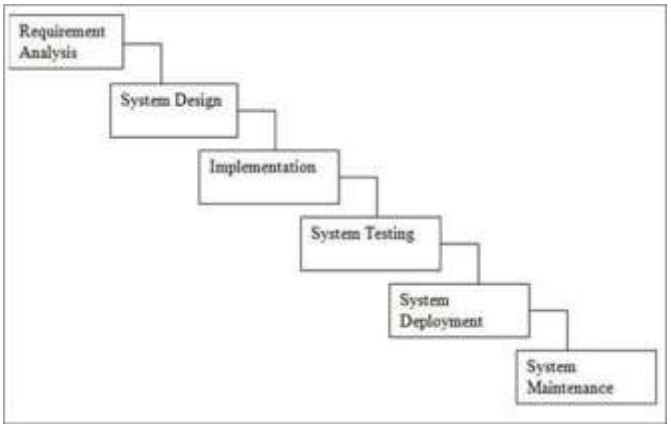


Fig. 1: WaterFall Model

1) ***Requirements Analysis****:* At this stage, use case definitions, business requirements, and related documentation are examined and produced.Finding the root cause of certificate fraud in educational institutions was part of the requirements analysis. This stage outlined the system's requirement to use blockchain technology to develop an unchangeable, impenetrable certificate verification procedure.

2) ***Design****:* The designs of the data models will be established at this stage, along with various data preparation and analysis tasks.

To show how users, the certificate generation system, and the blockchain interact, detailed architecture and data flow diagrams were created during the design phase. Employers, universities, and students' interactions with the system are depicted in the use case diagram below.

- **System Architecture:**

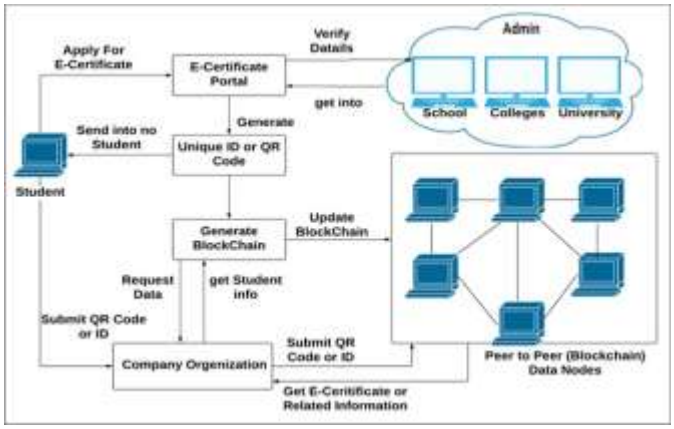


Fig. 2: System Architecture

Show the overall structure, components like blockchain nodes, certificate generation modules, and user interaction interfaces.

- **Class Diagram:**

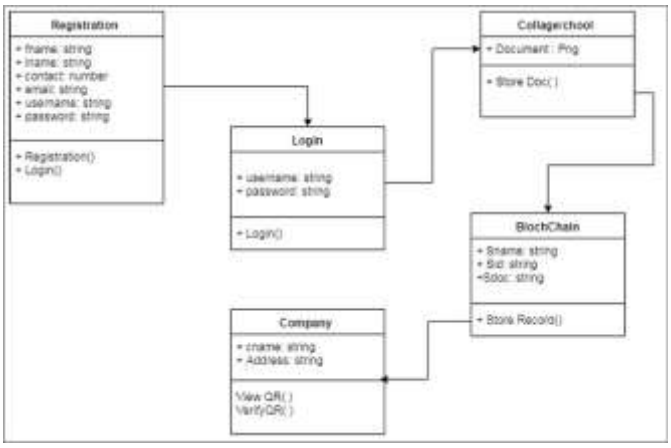
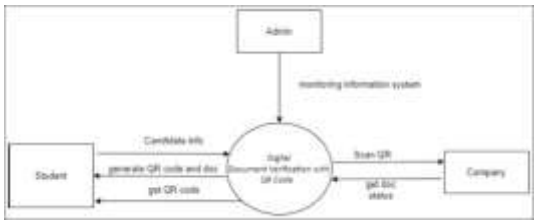


Fig. 3: Class Diagram

Represent the object-oriented structure (e.g., classes for User, Certificate, Blockchain, Smart Contract).

- **Data Flow Diagrams (DFD):**

(a) DFD Level-0



(b) DFD Level-1

DFD Level-2

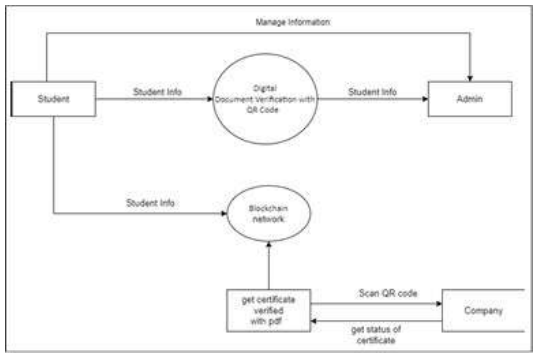


Fig. 4: Data Flow Diagrams for the System

Show how data flows from the user (e.g., certificate request) through the system (e.g., stored in blockchain, QR code generation).Demonstrating the flow of data from a student's certificate application to the creation of a QR code stored on a blockchain.

3) ***Implementation****:* In this phase, the model's actual devel- opment will take place. The back-end and front-end compo- nents of the agent will be developed using suitable algorithms, mathematical models, and design patterns based on the data model designs and requirements from earlier stages.

4) ***Testing****:* In this step, the model that was created using the earlier phases will be put to the test. The trained model will be subjected to a number of validation tests.

5) ***Deployment****:* This stage will test the model that was developed based on the earlier phases. The trained model will be put through a number of validation tests.

6) ***Maintenance****:* As the developed solution is used, the model will be subjected to a variety of inputs and scenarios, which could potentially impact the model's overall accuracy. Alternatively, as time goes on, the model may no longer meet the evolving business needs. As a result, frequent maintenance is required to keep the model operating in the intended state.

C. Blockchain and Smart Contracts Methodology

Our certificate verification system is based on blockchain technology, which guarantees that the stored certificates are verifiable and unchangeable. Trustworthiness is increased by using smart contracts, which automate the certificate gen- eration and validation procedures without requiring human intervention.

1) ***Blockchain Architecture****:* The utilized blockchain is a private, customized blockchain with nodes run by reliable aca- demic institutions. No certificates can be altered or tampered with after they are issued thanks to the consensus process.

2) ***Smart Contract Mechanism****:* When the institution ver- ifies, a smart contract is set up to automatically issue a digital certificate. After that, it creates a special hash for the certificate, which is linked by a QR code and saved on the blockchain.

D. QR Code Technology

A convenient way to retrieve and validate certificates is through QR codes. Every certificate that the blockchain issues is linked to a distinct QR code that includes the URL to the blockchain's verification page.

1) ***QR Code Generation****:* A dynamic QR code with a URL pointing to the certificate's distinct hash in the blockchain is created upon certificate issuance. Employers or educational institutions can instantly verify this.

*2) **QR Code Scanning and Verification**:* When a QR code is scanned, the system retrieves the stored hash from the blockchain and compares it with the provided certificate, confirming its validity and originality.

E. Testing and Validation

To verify system performance, security, and certificate generation accuracy, extensive testing was carried out. To make sure the smart contracts worked as intended and that the blockchain could not be altered, a number of test cases were created.

*1) **System Testing**:* System testing included security testing to make sure that tampering or unwanted access was impossible, as well as functional testing to verify certificate generation processes.

V. CONCLUSION

To prevent certificate fraud and guarantee the safety, authenticity, and privacy of graduation certificates, a number of technologies have been investigated. But there are still issues with data security and privacy with a lot of these solutions. By providing an open and transparent procedure for automated certificate issuance, a new blockchain-based system successfully lowers certificate forgeries. This makes it simple for businesses or groups to confirm any certificate in the system.

The proposed solution guarantees accurate, trustworthy information on digital certificates, lowers management expenses, and stops document forgery. Our system offers a safe, scalable, and impenetrable method of digital document verification by combining smart contracts, blockchain technology, and the Waterfall model. Because QR codes are integrated, accessibility is further improved, making this a complete and efficient solution for both employers and educational institutions.

REFERENCES

[1] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051.

[2] A. Draper, A. Familrouhani, D. Cao, T. Heng and W. Han, "Security Applications and Challenges in Blockchain," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-4.

[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Got tardi, Daniele Sciarroni and Luca Spalazzi Certificate, "Validation through Public Ledgers and Blockchains" In Proceedings of the First Italian Con ference on Cybersecurity (ITASEC17) 2017.

[4] Neethu Gopal, Vani V Prakash, "Survey on Blockchain Based Digital Certificate System" International Research Journal of Engineering and Technology (IRJET) Nov 2018.

[5] S. Pandey, G. Ojha, B. Shrestha and R. Kumar, "BlockSIM: A practical simulation tool for optimal network design, stability and planning," 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 133-137.

[6] C. Ehmke, F. Wessling and C. M. Friedrich, "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol," 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Gothenburg, Sweden, 2018, pp. 48-51.

[7] S. Saha, H. Gupta, N. R. Teja, S. Kothari and D. V. N. S. Kumar, "An Efficient Blockchain and Smart Contracts Based Approach for Document Verification," 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 2023, pp. 1-8.

[8] kumari, S.Sunitha and D.Saveetha. "Blockchain and Smart Contract for Digital Document Verification." International Journal of Engineering & Technology (2018): n. pag.

[9] Ramachandran, Aravind, and Dr Murat Kantarcioglu. "Using blockchain and smart contracts for secure data provenance management." arXiv preprint arXiv:1709.10000 (2017).

[10] S. S. Jacob, L. J. Varghese, S. Jaisiva, S. D. Kumar, R. Lakshana and R. Keerthana, "Intelligent Data Storage in Electronic Voting Machine using Blockchain System," 2024 Third International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), Villupuram, India, 2024, pp. 1-5.

[11] Wu, Kaidong. "An empirical study of blockchain-based decentralized applications." arXiv preprint arXiv:1902.04969 (2019).

[12] Chang, J., Gao, B., Xiao, H., Sun, J., Cai, Y., Yang, Z. (2019). "sCompile: Critical Path Identification and Analysis for Smart Contracts". In: Ait-Ameur, Y., Qin, S. (eds) Formal Methods and Software Engineering. ICFEM 2019. Lecture Notes in Computer Science(), vol 11852. Springer, Cham.

[13] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021.

[14] O. Ali, A. Jaradat, A. Kulakli and A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," in IEEE Access, vol. 9, pp. 12730-12749, 2021.

[15] M. Kaur, M. Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty and S. K. Pani, "MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols," in IEEE Access, vol. 9, pp. 80931-80944, 2021.

[16] M. A. Ferrag and L. Shu, "The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial," in IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17236-17260, 15 Dec.15, 2021.

[17] S. Mthethwa, N. Dlamini and G. Barbour, "Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-5.

[18] G. V. Lakshmi, S. Gogulamudi, B. Nagaeswari and S. Reehana, "BlockChain Based Inventory Management by QR Code Using Open CV," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-6.