Blockchain-Based Certificate Verification System

A PROJECT REPORT
(19CSE312 DISTRIBUTED SYSTEMS)

Submitted by

BL.EN.U4CSE22018	E. Manikanta
BL.EN.U4CSE22050	R. Henry Koushal
BL.EN.U4CSE22068	Y. Veera Manikanta

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

AMRITA SCHOOL OF COMPUTING, BENGALURU
AMRITA VISHWA VIDYAPEETHAM
BENGALURU - 560 035

May 2025

AMRITA VISHWA VIDYAPEETHAM

AMRITA SCHOOL OF COMPUTING

BENGALURU, 560035

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **"Blockchain-Based Certificate Verification System"** submitted by

BL.EN.U4CSE22018 E. Manikanta

BL.EN.U4CSE22050 R. Henry Koushal

BL.EN.U4CSE22068 Y. Veera Manikanta

in partial fulfillment of the requirements as part of my Bachelor of Technology in **"COMPUTER SCIENCE AND ENGINEERING"** is a bonafide record of the work carried out under my guidance and supervision at Amrita School of Computing, Bengaluru.

Dr. Supriya M.
Associate Professor
Dept. of CSE
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India

This project report was evaluated on **12/05/25**.

Dr. Supriya M.

ACKNOWLEDGEMENTS

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who made it possible, and whose constant encouragement and guidance have been a source of inspiration throughout the course of this project work.

We offer our sincere pranams at the lotus feet of **"AMMA," MATA AMRITANANDAMAYI DEVI**, who showered her blessings upon us throughout the course of this project work.

We owe our gratitude to **Prof. Manoj P.**, Director, Amrita Vishwa Vidyapeetham, Bengaluru Campus. We thank **Prof. Sriram Devanathan**, Principal, Amrita School of Engineering, Bengaluru for his support and inspiration.

We would like to place our heartfelt gratitude to **Dr. Gopalakrishnan E. A.**, Chairperson & Principal, Amrita School of Computing and Amrita School of AI, Bengaluru for his valuable support and inspiration.

It is a great pleasure to express our gratitude and indebtedness to our project guide, **Supriya M, Associate Professor**, Department of Computer Science and Engineering, Amrita School of Computing, Bengaluru, for their valuable guidance, encouragement, moral support, and affection throughout the project work.

We would like to express our gratitude to the project panel members for their suggestions, encouragement, and moral support during the project work, and to all faculty members for their academic support. Finally, we are forever grateful to our parents, who have loved, supported, and encouraged us in all our endeavors.

ABSTRACT

The Blockchain-Based Certificate Verification System is a web-based application designed to securely issue and verify digital certificates securely through blockchain technology.It has the ability to allow users to register, login, and issue certificates that comprise a registration number, recipient in formation, and a QR code for verification. The system permits certificate validation via either a hash value or QR code, making the process of verification easy. Through the utilization of blockchain's decentralized and unchangeable features, the application guarantees tamper-proof storage and reinforces trust in the authenticity of certificates. This solution greatly enhances certificate management's reliability, transparency, and efficiency both in academia and the workplace.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1

In the current digital era, the issuance and authentication of certificates have gained importance for academic and professional qualifications. Paper-based certificate issuance through traditional means is vulnerable to forgery and difficult to authenticate. Digital certificates provide an answer by introducing a secure, tamper-resistant way of credentialing. This project solves this problem through creating a web application that makes use of the blockchain technology for issuing and verification of digital certificates. The web application is expected to be convenient and efficient and in such a way that will simplify the certificate issuance and verification process while still ensuring security.

1.2

The project applies up-to-date web development techniques to build a scalable and stable solution. By incorporating blockchain technology, the application makes sure that every certificate is traceable, being unique in nature, thus making the system more secure and reliable. The application of a QR code for every certificate provides an added level of convenience and security, where users can easily and quickly verify. The application is designed to be intuitive, making it accessible to users with varying levels of technical expertise.

1.3

The evolution of the project entailed several significant steps such as web application design and implementation, integration of blockchain technology, and strict testing to guarantee functionality and security. The application was developed with user authentication, issuance of certificates, and verification capabilities. Blockchain technology being applied guarantees that every certificate is stored in tamper-proof form, offering a high degree of security and integrity.

1.4

In summary, this project illustrates the value of blockchain technology in the security and efficiency of digital certificate management. Through a safe and easy-to-use environment for issuing and authenticating certificates, the application reduces the issues related to physical paper certificates. Future research could focus on increasing the application's capabilities, such as automated renewal of certificates and compatibility with other systems for wider use. Generally, this project presents a strong solution to digital certificate management, adding strength and trustworthiness to credentials issued.

Chapter 2

LITERATURE REVIEW

2.1

Academic certificate forgery has become a serious issue due to advances in technology that support the easy copying of documents. Traditional verification procedures are costly and time-consuming and require high levels of manual intervention and third-party intermediaries. Blockchain technology, with its decentralized and tamper-evident nature, offers an answer by supporting the secure and efficient means of verifying academic credentials. The proposed model leverages blockchain's inherent properties, such as hash functions and digital signatures, to allow for a system where certificates can be verified quickly and reliably. The process not only enhances security but also lightens the issuer's and employer's load [1].

2.2

Blockchain technology has drawn general interest due to its potential for disrupting academic certificate authentication through secure, transparent, and tamper-resistant solutions.Systematic literature review in the paper examines 34 studies published from 2018 to 2022 and summarizes key themes and challenges for blockchain-based systems for this application. It requires stringent security protocols, efficient management of data, and pragmatic models for facilitating blockchain's adoption in the higher education sector. Review also demands adherence to legal and regulatory requirements to enable the universal deployment of such systems. Emerging avenues for further studies include an exploration of the scalability, interoperability, and field deployment of blockchain technology for learning environments [2].

2.3

Blockchain technology is studied as a way to safely store academic certificates, addressing the problem of digital cer tificate forgery. The system proposed takes advantage of blockchain's decentralization and transparency to provide a se cure, tamper-evident means of certificate

verification. It is built on top of fundamental concepts like hash functions, public private key cryptography, and smart contracts that provide the foundation for blockchain functionality. The paper mentions Ethereum and Hyperledger as instances of their contribution towards the development of secure, decentralized applications. It also discusses issues of scalability and privacy of blockchain implementations and suggests potential solutions to these issues in the context of educational certificate management [3].

2.4

Blockchain has increasingly been used to secure academic credentials, with institutions such as the University of Nicosia and Sony Global Education pioneering its use towards veri f iable certificate issuance. Products such as CredenceLedger, IU-SmartCert, and OpenCerts seek to improve data authen ticity, but most of them do not incorporate legacy databases or have affordable deployment. Contemporary models tend to store just hashes or use completely blockchain-based infras tructure, constraining their flexibility and tampering detection to a finite number. A number of studies point towards the ability of smart contracts and hybrid solutions to overcome these limitations. Even with innovation, most solutions fail to align off-chain and on-chain data in an efficient manner. This shortcoming presents the demand for an affordable, scalable system that achieves decentralization and compatibility [4].

2.5

Blockchain has drawn serious attention in supply chain management as it can verify product authenticity with decen tralization and immutability. Previous systems attempted IoT integration, secure mobile applications, and machine learning to identify counterfeits, especially in the pharmaceutical and food supply chains. Initiatives such as IBM's Trust Chain and VeChain proved the practical application of blockchain in tracking raw materials and vaccine history. Legacy methods lacked end-to-end verification and contained weaknesses in data tampering at certain checkpoints. The three-entity model adds security by engaging manufacturers, sellers, and con sumers in a unified verification process. The three-way sys tem improves end-to-end traceability and constructs consumer confidence [5].

2.6

Global efforts to digitize and secure academic credentials have been prompted by blockchain's decentralized and impen etrable nature. Although they set the foundation, initiatives like Blockcerts and EduCTX frequently lacked government over sight, revocation procedures, and nationwide scalability. New developments combine role-based access to safely manage issuers and verifiers, smart contracts for automation, and IPFS for off-chain storage. While some

frameworks concentrate on metadata hashing to reduce on-chain expenses, others expand verification to include foreign qualifications. All educational levels are brought together under a single, verifiable, and legally compliant framework by more recent systems such as ElimuChain, which exhibit comprehensive architectures [6].

2.7

Blockchain technology has been explored as a means to increase transparency and traceability in agriculture, appli cations ranging from food safety to carbon offset tracking. Earlier studies highlight the application of mobile platforms and IoT to connect farmers with consumers and reduce mid dlemen intervention. Other studies highlight the application of augmented reality (AR) to enhance consumer knowledge of product origin and sustainability efforts. Blockchain has also been proposed to securely trade carbon credits, ensur ing authenticity and traceability across supply chains. While promising prototypes and pilot implementations, scalability, interoperability, and field deployment challenges persist. How ever, these advances underscore the growing potential of blockchain-AR synergy for sustainable agriculture [7].

2.8

Increasing traffic congestion and accidents have necessitated the incorporation of new technology into transport infrastruc tures. Various vehicle-to-vehicle and vehicle-to-infrastructure authentication schemes have been proposed previously. Most of the proposed schemes were either susceptible to insider attacks or had high computational overheads. Edge computing and federated learning have been suggested for real-time pro cessing and privacy, but are not tamper-resistant themselves. Blockchain has already been shown to be an effective tool for enabling trust and immutability in accident detection systems. Previous research based on certificate-based or certificateless authentication was plagued by dynamic node addition and key management problems. The system proposed here advances the previous results by employing blockchain to securely, scalably, and tamper-resistantly share accident data in ITS networks [8].

2.9

Academic credential verification has increasingly shifted to ward blockchain platforms for increased transparency, privacy, and automation. MIT's Blockcerts led the way but was held back by factors like student engagement dependency and in compatibility with legacy document processes. Other projects employed platforms like Bitcoin, Ethereum, and Hyperledger to verify degrees but mostly dealt with digital documents only or necessitated redesigning certificates. Others employed barcode or QR-code approaches, which still meant altering physical

documents. Docschain overcomes these shortfalls by combining OCR with blockchain, facilitating hardcopy degree verification without adjustment. Its semiprivate structure also supports institutional control alongside decentralized valida tion [9].

2.10

Blockchain has emerged as an education disruptor, pro viding tamper-proof storage and authentication of academic credentials. MIT's Blockcerts pioneered the process by pub lishing hashes of certificates on the blockchain, providing integrity and authenticity. Alternatives such as X.509-based systems and Ethereum smart contracts push decentralization and automation of certificate issuance even further. Some frameworks integrate Merkle trees and IPFS for efficient data management, providing transparency without sacrificing privacy. Smart contracts and platforms such as Disciplina promise scalable, domain-independent solutions. Progress has been made, but trust, interoperability, and mass adoption are still challenges in educational blockchain applications [10].

2.11

Smart grids are designed to increase energy efficiency and reliability but face severe cybersecurity challenges due to their bidirectional communication networks. Past work has used cryptographic protocols such as ECC and AES to improve confidentiality and integrity of data, particularly for resource-constrained devices. Blockchain has been used to distribute trust and automate energy trade, but solutions were faced with scalability, energy usage, and privacy compromises. Existing models focus on the integration of smart contracts and lightweight authentication to protect P2P communication among smart meters, aggregators, and virtual power plants. Some also use biometric-based key generation using fuzzy extractors to enhance user authentication. Yet, one solution that integrates strong encryption, block transparency, and scalability was underdeveloped [11].

2.12

Academic credential forgery is a global issue, and orga nizations want secure and transparent verification systems. Traditional centralised methods are resource-intensive, tamper prone, and time-consuming. Various blockchain-based solu tions have been suggested, with platforms like Ethereum and Hyperledger used to store certificates, run smart contracts, and offer immutability. Techniques such as IPFS storage, QR code embedding, and cryptographic hashing offer enhanced security and availability of data. Some studies propose the use of decentralized apps (DApps) for real-time verification with no manual intervention. Few of these offer compatibility with standard certificate formats and on-chain revocation with minimal user-side cryptographic management [12].

2.13

Academic credential validation has been plagued by forgery, inefficiency, and privacy infringement for a long time. Some initiatives like Blockcerts by MIT, SmartCert, and RecordsKeeper introduced blockchain-based solutions to avoid certificate forgery with cryptographic signing and decen tralized storage. However, there are gaps in achieving ba sic security themes of authentication, authorization, privacy, confidentiality, and ownership. Models from platforms like Hyperledger and Ethereum lack in current models, with most overlooking user control or publishing data into public ledgers. Current work prioritizes role-based access, private channels, and unique hash-based verification to enhance trust and data protection. These developments guide endeavors towards a secure, open, and privacy-aware credentialing system [13].

2.14

Digitization amplified the risk of forgery, and the adoption of blockchain technology has been spurred to provide verifica tion and proof of ownership. Traditional means like stamps and barcodes were not sufficient, and early blockchain implemen tations like MIT's Blockcerts and UNIC's SHA-256 hashing were not private and lacked user control. New paradigms address decentralized verification without a middleman, with biometric verification and smart contracts coupled to further secure. Platforms like SmartCert and RecordsKeeper used cryptographic signing but were vulnerable to transfer of own ership and offered limited privacy protection. Current work indicates anchoring student identity and certificate hashes to offer authenticity and user-specific control. Such work is stepping stones towards secure, tamper-proof verification systems [14].

2.15

Blockchain technology, originally developed by Satoshi Nakamoto, presented a decentralized and open digital record that has been subsequently used outside cryptocurrency for secure data storage. The development of smart contracts by Ethereum furthered the use of blockchain for decentralized applications, such as document verification. Different studies have shown vulnerabilities in conventional certificate verifica tion systems and the growing number of instances of forgery. Cryptographic hash functions and decentralized storage (e.g., IPFS) have been used to tamper-proof digital certification, as discussed by researchers. Existing research focuses on the use of blockchain with smart contracts to guarantee authenticity, immutability, and real-time verification of academic qualifica tions [15].

2.16

Blockchain's decentralization and immutability have made it an emerging solution to fight academic certificate forgery, which is increasing worldwide. Initial efforts like Blockcerts and MIT's Media Lab concentrated on recipient control but had usability and privacy compromise issues. Universities like the University of Nicosia and OU UK showed practi cal deployments but did not have end-to-end authorization and ownership management. Solutions like SmartCert and RecordsKeeper included cryptographic integrity, but had pri vacy and technical usability issues. The Hyperledger-based framework is unique in combining all the necessary security theme authentication, authorization, ownership, privacy, and confidentiality within a permissioned architecture [16].

2.17

In order to address growing concerns about certificate forgery and verification inefficiencies, blockchain applications in education have emerged. Although they pioneered de centralized, verifiable academic credentials, Blockcerts and MIT's initiatives continue to face privacy and usability issues. While projects like EduCTX, SmartCert, and RecordsKeeper provide certificate verification through a variety of blockchain platforms, they are devoid of features like role-based access and training history traceability. By combining Hyperledger Fabric with regional educational frameworks and a four phase architecture that enhances trust, Vietnam's VECefblock system expanded on these concepts. The system's viability was validated by its performance trials, which also indicated that it could be widely adopted in intricate educational settings [17].

2.18

Researchers are looking into blockchain for safe, impene trable credentialing because of the surge in certificate fraud cases brought on by the quick digitization of education. Although they brought transparency, early blockchain apps like Blockcerts lacked automation and scalability. Since then, inef f iciencies in conventional systems have been addressed by au tomating diploma generation and verification through the use of smart contracts on platforms such as Ethereum. Frameworks like Hyperledger Fabric provide academic institutions with privacy-preserving features and controlled access. For wider adoption, there is increasing interest in combining blockchain with off-chain storage, biometric authentication, and GDPR compliant data models, according to a comprehensive analysis of recent research [18].

2.19

Blockchain technology, which provides decentralized, un changeable, and verifiable academic record systems, is still developing as a strong defense against certificate fraud. New methods were prompted by earlier systems, such as Block certs, which concentrated on generation and validation but lacked modifiability. Smart contract automation, QR-based verification, and SHA-256 hashing for safe certificate tracking are highlighted in recent research. In order to improve real world usability, some systems also investigate hybrid models that facilitate corrections after issuance. To enable scalable, transparent academic verification infrastructures, blockchain education innovations now incorporate secure access control, correction chains, and authentication [19].

2.20

A number of blockchain-based remedies that emphasize immutability, decentralization, and transparency have been put forth to combat academic certificate fraud. Although they were designed to be tamper-resistant, earlier systems such as IPFS based storage and NFT-linked credentials frequently lacked effective search capabilities. Others did not incorporate issuer validation or real-time corrections, but instead used consensus processes and smart contracts to issue and validate certifi cates. Voting-based trusted networks and Bloom Filters were added to recent models to speed up search and verification while lowering false negatives. For scalability and institutional trust, current research now focuses on gas-efficient Ethereum deployment and lightweight, privacy-preserving architectures with hash-only storage [20].

2.21 Literature survey highlights

Several gaps in existing blockchain-based certificate verification systems. Many early systems, such as Blockcerts and MIT's Media Lab efforts, were concerned with recipient control but sacrificed usability and privacy. The systems in place tended not to have all rounded security elements such as solid authentication, autho rization, and protection of privacy. Furthermore, although plat forms such as EduCTX, SmartCert, and RecordsKeeper were offering certificate verification across different blockchain plat forms, they were not supporting features such as role-based access or training history traceability. Other solutions, includ ing IPFS-based storage and NFT-linked credentials, failed to provide efficient search functions and real-time corrections. Our proposed model addresses these gaps by integrating comprehensive security features and advanced functionalities. It includes role-based access control to provide added security and privacy, protecting certificates from unauthorized issuance and verification by users. The system also features real-time corrections and traceability, enabling easy updates and audit trails of certificate history. Utilizing blockchain technology, our model guarantees immutability and transparency, offering a tamper-proof mechanism for managing certificates. More over, the integration of QR codes and hash-based verification mechanisms provides an additional level of convenience and security, making the verification process fast and reliable. This all-encompassing approach not only increases the security and efficiency of digital certificate management but also the overall user experience.

Chapter 3

SYSTEM SPECIFICATIONS

3.1

- **Framework:** Flask (Python)
- **Database ORM:** SQLAlchemy
- **Session Management:** Flask-Login
- **Blockchain:** Custom blockchain class with:
  - Block creation
  - Transaction linking
  - Proof-of-Work
  - Hash generation
- **Frontend:** HTML, CSS, JavaScript
- **Templating:** Jinja2
- **Form Handling:** Flask-WTF
- **QR Code:** `qrcode` Python library
- **Hosting:** Deployed on a scalable server environment

Design Goals

- Secure
- User-friendly
- Scalable
- Tamper-proof

Chapter 4

SYSTEM DESIGN

4.1

From 4.1, the Blockchain-Based Certificate Verification System begins with user registration and login through the Authentication Block. Certificate information is then issued, saved in a database, and tied to the blockchain. A new transaction is constructed and secured through hashing and proof of work. The system produces a QR code for every certificate to facilitate easy access. It can be verified either with the QR code or with the blockchain hash. This architecture supports secure, tamper-proof, and transparent certificate management.

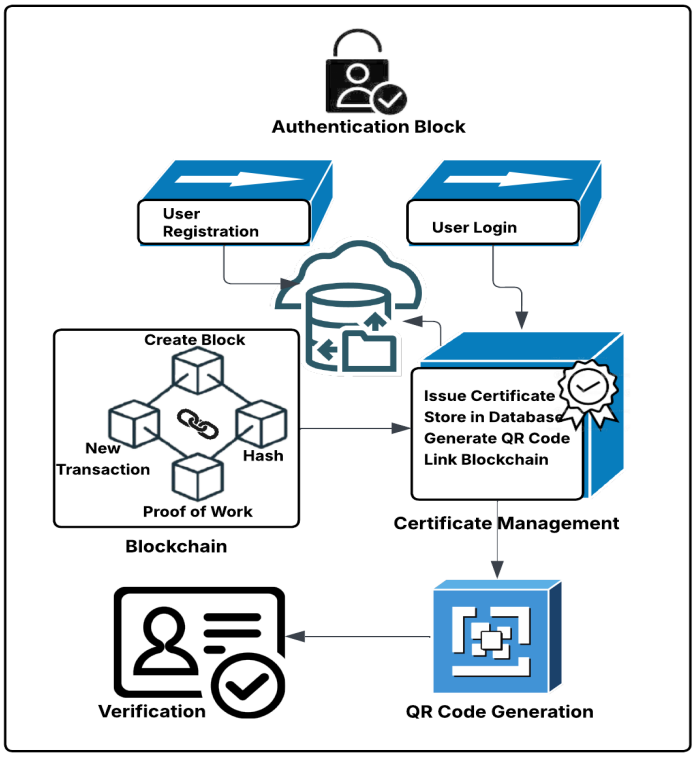

Figure 4.1: Architecture Diagram

Chapter 5

SYSTEM IMPLEMENTATION

5.1 Web Application Design and Implementation

The web application was carefully crafted with Flask, a stable Python web framework, to effectively manage user interaction and data management. SQLAlchemy was utilized for effortless database operations to securely store and retrieve user and certificate information. Flask-Login was implemented to securely manage user sessions. HTML, CSS, and JavaScript were used to craft the frontend for an easy-to-use and respon sive user interface, allowing the application to be easily used by users with different technical backgrounds

5.2 Blockchain Integration

A blockchain class was created specifically to handle the generation of blocks and transactions so that every certificate is stored in an immutable and tamper-proof state. A proof-of work algorithm was used to lock down the blockchain to avoid unauthorized changes. The system was created to produce a unique hash for every certificate, which is stored on the blockchain, with a high degree of security and integrity.

5.3 User Interface Development

User interface was created to be accessible and easy to use. Flask-WTF was implemented to process the submission of user registration, login, and issuance of certificates. The qrcode library was used to create a QR code per certificate, offering a further measure of convenience and security. Dynamic content was created using Jinja2 templates for rendering, so the application responds well and is easy to use

Chapter 6

SYSTEM TESTING

6.1 Testing and Security Assessment

The application was tested extensively to verify that all functionalities were working as expected. This involved testing user registration, login procedures, certificate issuance, and verification processes. Security audits were performed to guard against prevalent vulnerabilities. The utilization of blockchain technology made each certificate identifiable and tamper proof, thereby boosting overall security.

6.2 Deployment

The application was hosted on an appropriate server so that it becomes accessible via the internet. Deployment included setting up the server environment, installing required depen dencies, and making the application scalable under diverse conditions. The application was created with scalability, mean ing it could handle a rise in load and user traffic in the future.

Chapter 7

RESULTS AND ANALYSIS

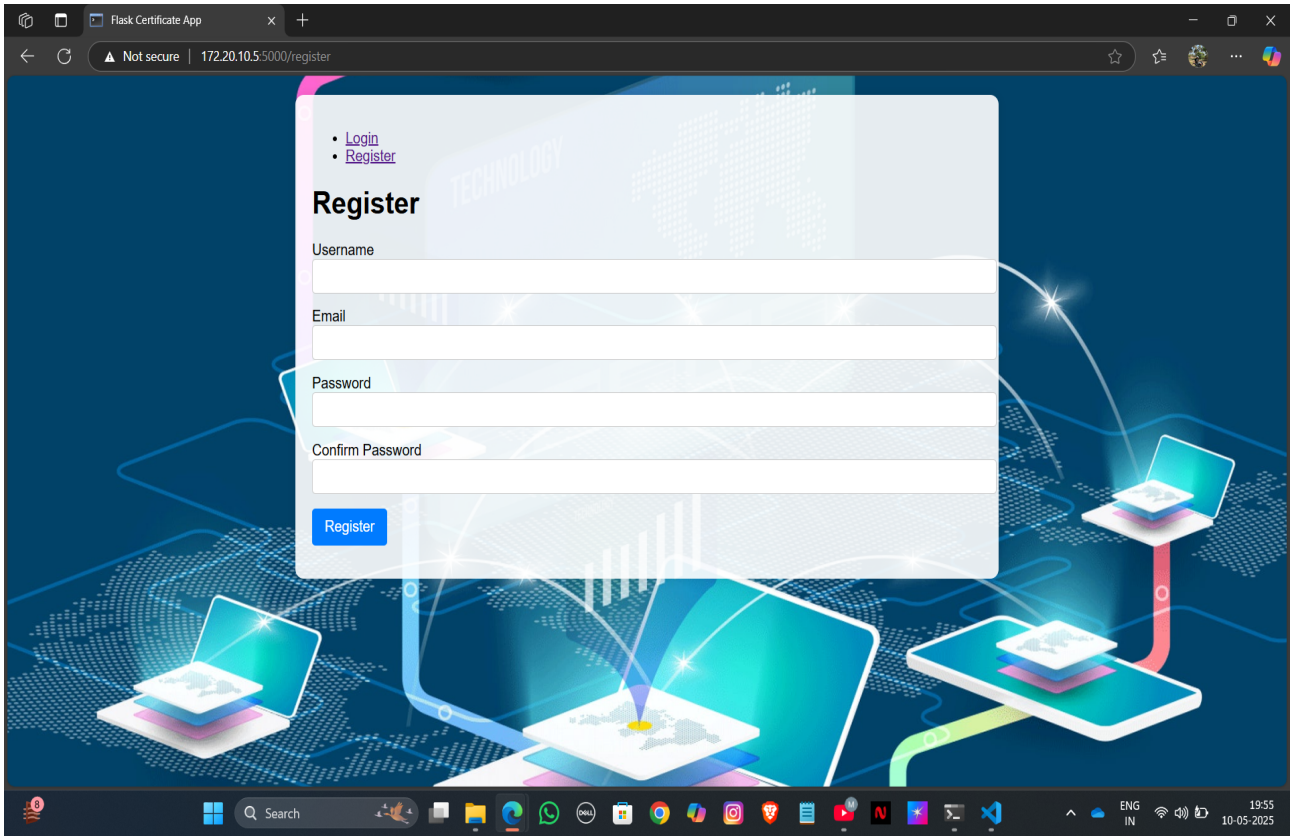

Figure 7.1: User Registration Page

Fig 7.1 New users can register securely by providing a username, email, and password for accessing the certificate system.

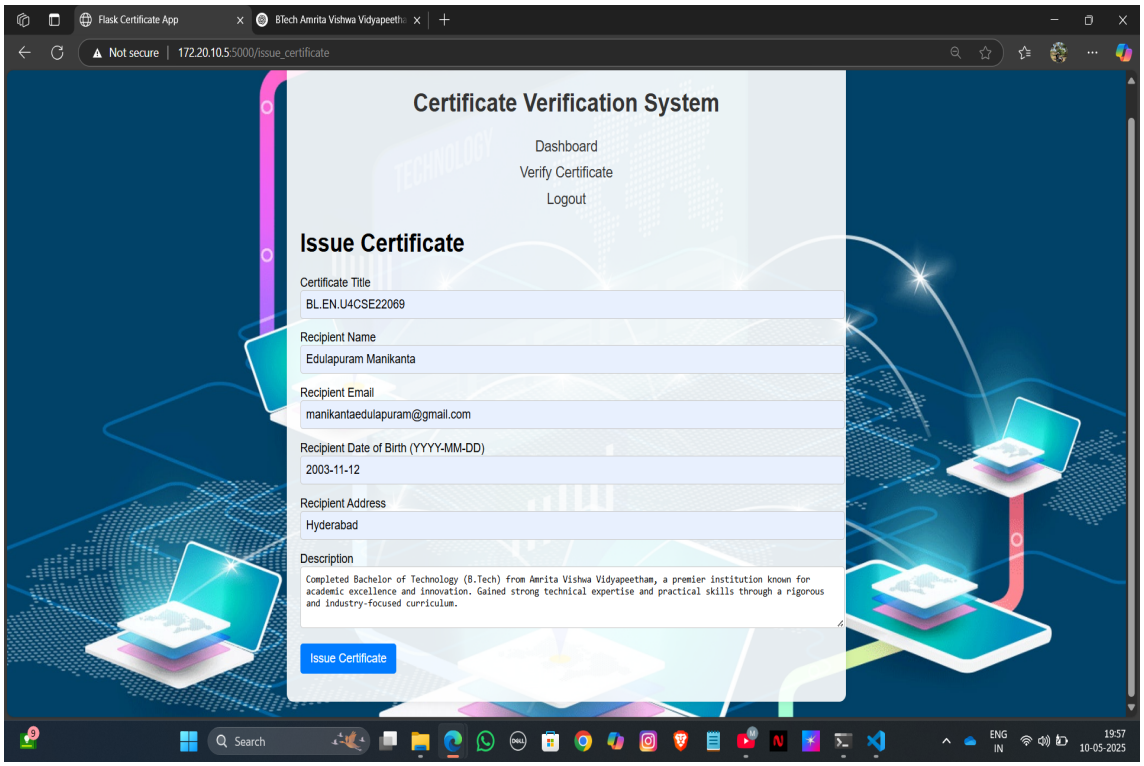

Figure 7.2: Issue Certificate Page

Fig 7.2 Allows authenticated users to input recipient details and generate a blockchain-secured digital certificate.

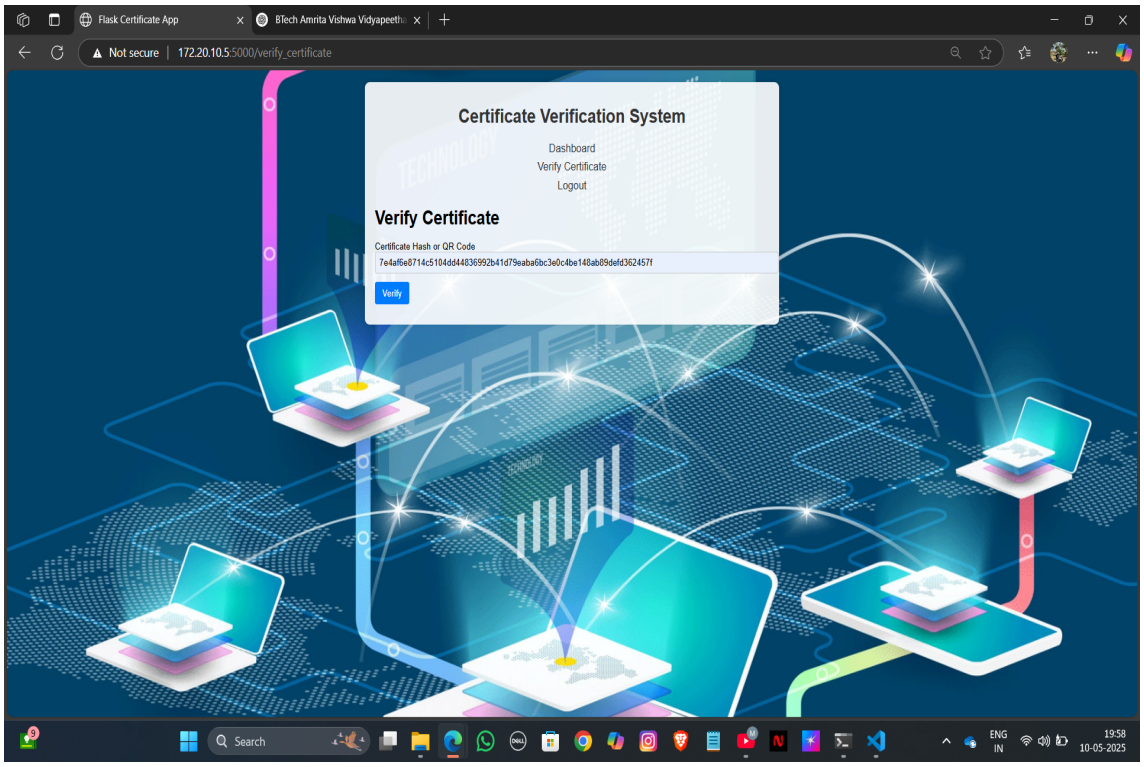

Figure 7.3: Verify Certificate Page

Fig 7.3 Enables users to verify the authenticity of a certificate using its unique blockchain hash or QR code.

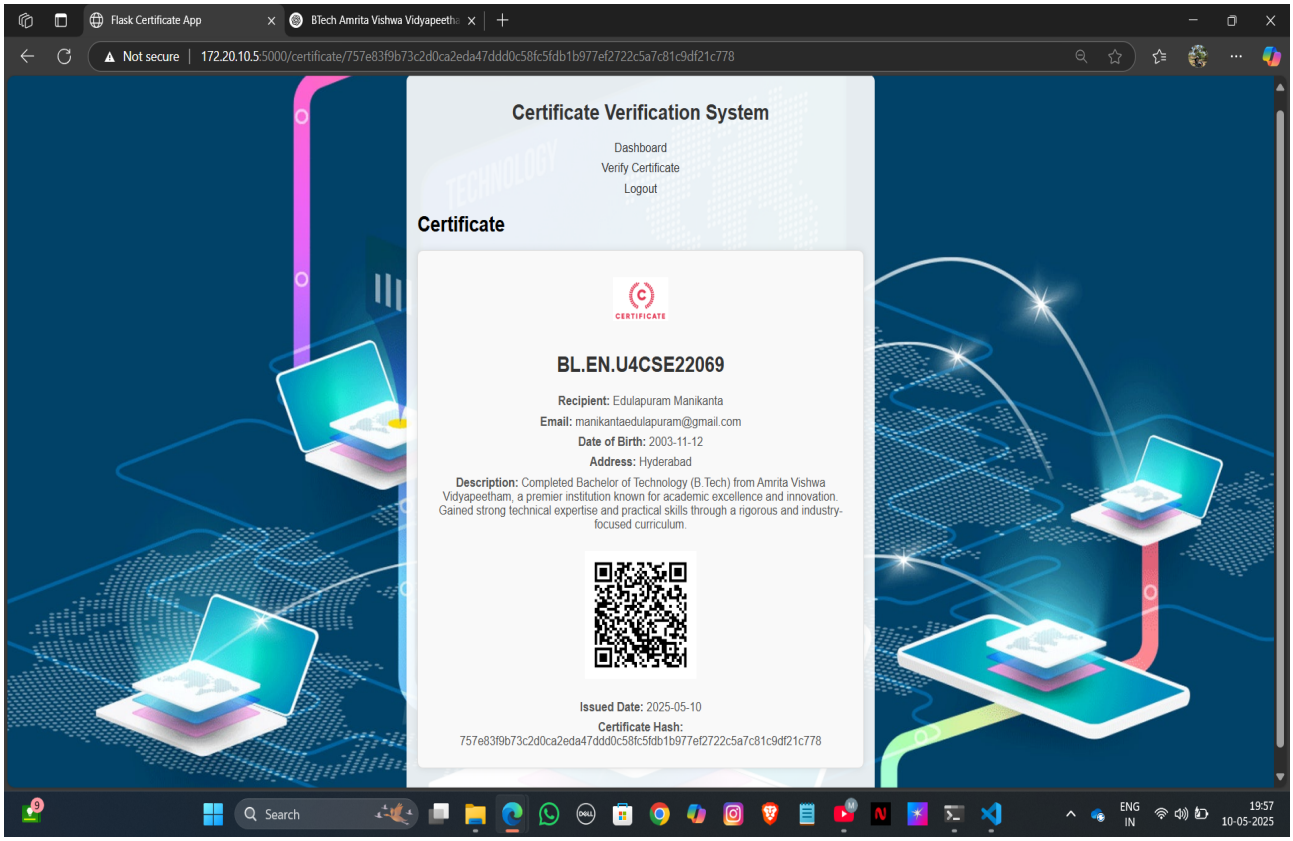

Figure 7.4: Verified Certificate Display Page

Fig 7.4 Displays a verified graduate certificate with recipient details, QR code, and certificate hash, confirming B.Tech completion from Amrita Vishwa Vidyapeetham.

7.1

The web application demonstrated stable performance, ef fortlessly managing user input and data operations. Flask sup plied a solid backend, while SQLAlchemy provided effective database operations. Authentication of users was effortless, and the frontend design was user-friendly, rendering the ap plication usable to users with differing technical capabilities. The responsiveness of the application and ease of use were tested using users, thus confirming readiness for deployment. The use of blockchain technology greatly improved the se curity and integrity of the certificate management system. Each certificate was stored on the blockchain with a distinct hash, providing immutability and tamper-proof storage. The proof of-work algorithm successfully locked down the blockchain, making unauthorized changes impossible. The uniqueness of the QR codes created for each certificate provided an added level of security and convenience, enabling easy and rapid verification. The deployment was done on an appropriate server, making the application available via the internet. The deployment went through server environment configuration and required depen dency setup, leading to efficient and stable functioning. The scalability of the application was tested to ensure that it can take in higher load and user demand with time. Deployment also entailed extensive testing to verify that the application performs effectively under different scenarios, reinforcing its reliability and performance.

Chapter 8

CONCLUSION AND FUTURE SCOPE

8.1

In conclusion,the Blockchain-Based Certificate Verification System efficiently overcomes the limitations of conventional paper-based certificates by taking advantage of the decen tralized and immutable features of blockchain technology. The system offers a safe, tamper-proof way of issuing and authenticating digital certificates, guaranteeing the authenticity and integrity of professional and academic credentials. With the inclusion of user-friendly functionalities like hash-based verification and QR codes, the app simplifies the verification process and presents it in a friendly manner, making it convenient and easy to use for users with different technical skills. The system's scalability and powerful security attributes guarantee that the system is reliable and flexible to meet growing demands. In general, this project shows the great potential of blockchain technology in improving the security, transparency, and efficiency of digital certificate management, providing a reliable solution for academic and professional use. Future efforts may be directed at expanding the system's functionality, for example, automatic certificate renewal and interfacing with other systems for even wider usage.

References

[1] O. Ghazali and O. S. Saleh, "A graduation certificate verification model via utilization of the blockchain technology," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 3-2, pp. 29–34, 2018.

[2] B. M. Nguyen, T.-C. Dao, and B.-L. Do, "Towards a blockchain-based certificate authentication system in vietnam," *PeerJ Computer Science*, vol. 6, p. e266, 2020.

[3] G. Balamurugan and K. K. A. Sahayaraj, "A blockchain based certificate authentication system," in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, 2023.

[4] N. Nadeem *et al.*, "Hybrid blockchain-based academic credential verification system (b-acvs)," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 43991–44019, 2023.

[5] A. Das *et al.*, "Securing supply chains: Blockchain's shield against counterfeit products," in *Proceedings of 6th International Conference*, vol. 19, 2024.

[6] S. H. Said *et al.*, "A comprehensive blockchain-based system for educational qualifications management and verification to counter forgery," *IEEE Access*, 2025.

[7] A. Padmavathi *et al.*, "Blockchain-based carbon offset tracking system for sustainable product management," in *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, IEEE, 2024.

[8] A. Vangala *et al.*, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15824–15838, 2020.

[9] S. Rasool *et al.*, "Docschain: Blockchain-based iot solution for verification of degree documents," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, pp. 827–837, 2020.

[10] P. E. Gundgurti *et al.*, "Smart and secure certificate validation system through blockchain," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, IEEE, 2020.

[11] A. Bedi *et al.*, "A novel blockchain supported hybrid authentication and handshake algorithm for smart grid," *IEEE Access*, 2024.

[12] P. P. Bokariya and D. Motwani, "Decentralization of credential verification system using blockchain," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 10, no. 11, 2021.

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

[14] A. Chowdhary, S. Agrawal, and B. Rudra, "Blockchain based framework for student identity and educational certificate verification," in *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, 2021.

[15] M. C. Rao *et al.*, "Verification and validation of certificate using blockchain," *Turkish Journal of Computer and Mathematics Education*, vol. 14, no. 3, pp. 1211–1216, 2023.

[16] Z. Wang *et al.*, "Blockchain-based certificate transparency and revocation transparency," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 681–697, 2020.

[17] N. Gopal and V. V. Prakash, "Survey on blockchain based digital certificate system," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 11, 2018.

[18] A. Rustemi *et al.*, "A systematic literature review on blockchain-based systems for academic certificate verification," *IEEE Access*, vol. 11, pp. 64679–64696, 2023.

[19] M. M. Rahman *et al.*, "Blockchain-based certificate authentication system with enabling correction." https://arxiv.org/abs/2302.03877, 2023. arXiv preprint arXiv:2302.03877.

[20] M. Fartitchou *et al.*, "Blockmedc: Blockchain smart contracts for securing moroccan higher education digital certificates," *IEEE Access*, 2025.