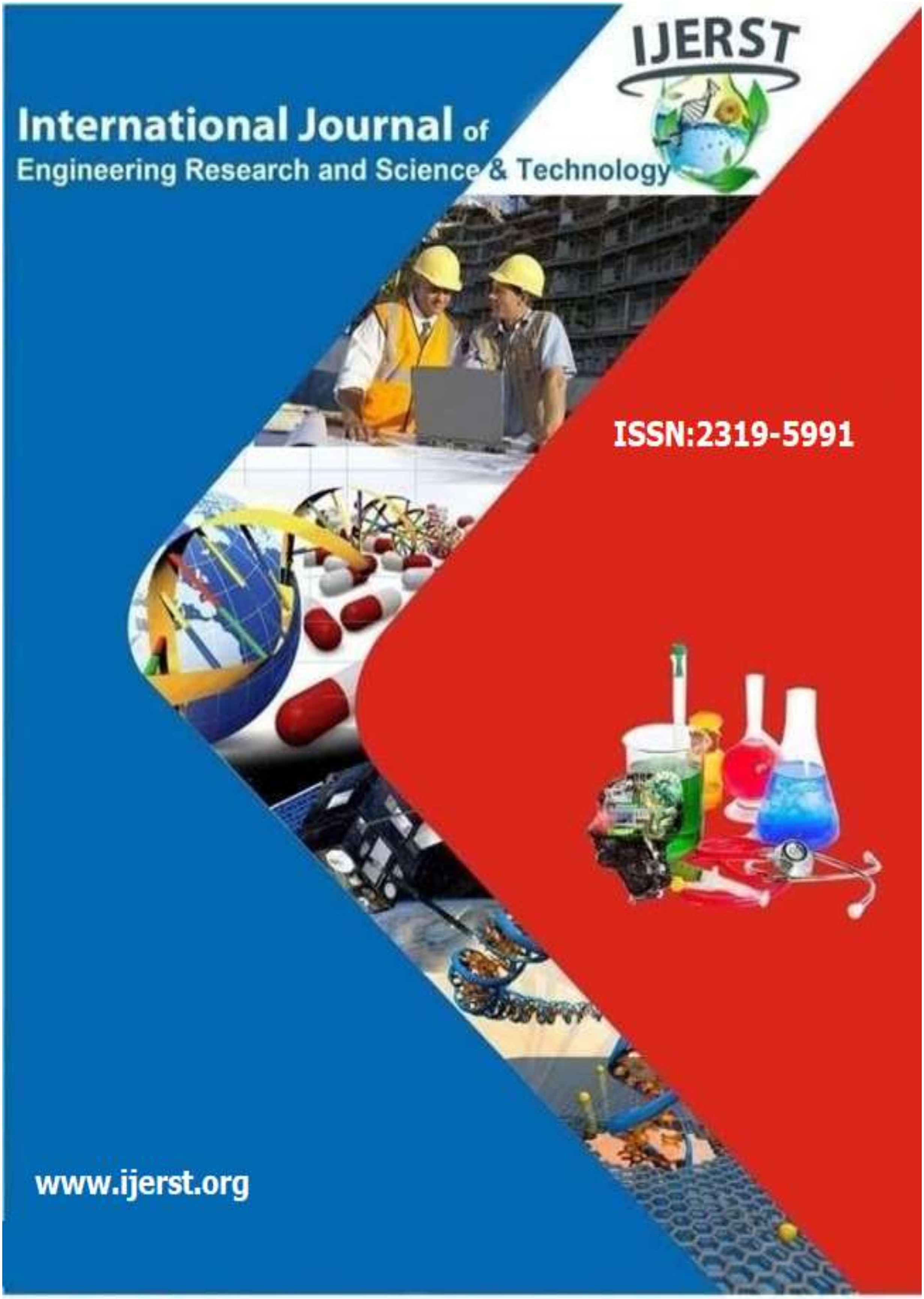
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025



E-mail: editor@ijerst.org or ijerst.editor@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Decentralized Certificate Authentication with Blockchain Technology

C. Gayathri [1]
Assistant professor
Department of CSE(DS)
TKR College of Engineering and Technology

M. Rani [2]
B. Tech (Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
molgararani0809@gmail.com

P. Sai kumar [3]
B. Tech (Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
saikumar.p626@gmail.com

MD Mushaarof [4]
B.Tech(Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
mohammadmushaarof24@gmail.com

T. Saikumar Reddy [5]
B. Tech (Scholar)
Department of CSE(DS)
TKR College of Engineering and Technology
saisaikumar0551@gmail.com

ABSTRACT

Certificate authentication has typically depended on central authorities, which can lead to security issues like forgery, data tampering, and vulnerabilities that stem from a single point of failure. In this paper, we introduce a decentralized method for certificate authentication through blockchain technology, which helps provide security, transparency, and a permanent record. By using smart contracts and cryptographic hashing, this system removes the need for middlemen, allowing organizations to securely create, manage, and confirm certificates. The blockchain acts as a secure ledger, making sure that certificates are protected from tampering and can always be verified.

This method builds trust in digital credentials, cuts down on fraud, and makes the authentication process easier for employers, schools, and other organizations. With blockchain, we reduce administrative burdens and stop unauthorized changes, which streamlines how we handle certificates. Also, the decentralized setup means that it can be accessed and used by a variety of institutions and industries around the globe. Through our prototype and analysis, we show that blockchain-based certificate authentication is feasible, secure, and efficient in real-life situations. Our results point to how blockchain technology could transform how we verify digital credentials, opening new possibilities for a safer and more decentralized future in education and the job market.

Keywords: Blockchain, Decentralized Authentication, Certificate Verification, Smart Contracts, Cryptographic Hashing, Digital Credentials, Tamper-Proof Records, Distributed Ledger Technology, Trustless Verification, Secure Credential Management.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

I . INTRODUCTION

In our increasingly digital world, it's essential to verify academic and professional credentials to ensure authenticity in hiring, education, and licensing. Traditional systems for certificate authentication often depend on centralized authorities like universities, certification agencies, and third-party verifiers. These centralized methods come with numerous challenges, such as the risk of document forgery, data breaches, sluggish administrative processes, and high operational costs. The manual verification of certificates can be slow and prone to human error, making it tough for organizations to efficiently validate credentials on a scale.

Given the surge in fraudulent activities—like fake degrees and altered documents, there is a pressing need for a robust, transparent, and tamper-proof solution. Blockchain technology presents a compelling alternative by enabling a decentralized approach to certificate authentication. By recording certificate data on a distributed ledger, blockchain ensures immutability, security, and accessibility. Once a certificate is recorded, it cannot be changed or deleted, minimizing the risk of fraud. Moreover, blockchain allows for instant verification, enabling employers and educational institutions to retrieve authenticated credentials directly from the network.

Smart contracts further streamline the process of certificate issuance and validation. These self-executing programs run based on predefined conditions, ensuring that certificates are issued and verified without needing intermediaries. This reduces reliance on central authorities, lowers administrative burdens, and simplifies the verification process. Additionally, cryptographic hashing techniques maintain data integrity and confidentiality, safeguarding against unauthorized alterations to stored credentials.

Another significant benefit of blockchain-based certificate authentication is its global accessibility and interoperability. Traditional verification can involve complicated cross-border coordination, which often leads to delays and extra costs. With blockchain, certificates can be verified instantly from anywhere in the world, enhancing efficiency for employers, universities, and professional organizations. This is especially advantageous for international students, job seekers, and companies with a global footprint.

This paper delves into the potential of blockchain technology for decentralized certificate authentication, examining its feasibility, implementation, and the benefits it offers. It presents a comprehensive analysis of the system's architecture, security features, and concrete applications in credential verification. By showcasing the merits of a decentralized approach, the study illustrates how blockchain can transform the issuance, storage, and verification of academic and professional certificates, paving the way for a secure and fraud-resistant digital credentialing future.

II. RELATED WORK

Numerous studies and projects have delved into leveraging blockchain technology for ensuring secure and decentralized certificate authentication. Conventional methods of verifying credentials depend on centralized authorities, which expose them to risks like fraud, data breaches, and inefficiencies. This has led researchers to propose a range of blockchain-based solutions that exploit the immutability, transparency, and security characteristics of distributed ledger technology.

One of the trailblazing initiatives in this field is the Block certificates project by the MIT Media Lab. It established an open-source standard for the

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

issuance and verification of blockchain-based certificates. With Block certificates, institutions can create cryptographically signed certificates and record their hashes on a blockchain, empowering recipients to demonstrate authenticity without relying on third-party verification. This system boosts security and eliminates the chances of certificate forgery, presenting a dependable alternative to traditional paper credentials.

Another noteworthy endeavor is Sony Global Education's credentialing system, designed to facilitate the secure and tamper-proof issuance of academic certificates. By using blockchain, Sony enables the storage and verification of academic records, allowing for seamless sharing of credentials among students, educational institutions, and employers. This initiative underscores the practical integration of blockchain in education and its potential for widespread adoption.

Various government-backed projects have also investigated blockchain for credential verification. A prime example is the Maltese government, which implemented a blockchain-based system for issuing academic certificates to students. This project aims to combat credential fraud while streamlining verification processes for employers and universities globally. In a similar vein, the Indian government’s National Blockchain Project has explored using blockchain to securely store and authenticate digital certificates issued by educational institutions.

III. METHODODLOGY

The blockchain-based certificate authentication system is built on a well-defined framework aimed at providing secure, transparent, and decentralized credential verification. The component design features a decentralized architecture that highlights key players, including issuing authorities (like universities and certification organizations), a blockchain network responsible for storing certificate hashes, smart contracts for automating processes, certificate holders (which may be students or professionals), and verifiers (such as employers and academic institutions). This setup effectively removes the need for intermediaries, thereby minimizing fraud and cutting down on administrative burdens.

Selecting the right blockchain is critical for the system's overall effectiveness. Public blockchains like Ethereum and Polygon support decentralization, while private blockchains such as Hyperledger Fabric provide controlled access alongside improved scalability. The choice of consensus mechanism—be it Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT)—also affects how efficiently transactions are validated. Factors such as cost and performance, including gas fees and transaction speeds, heavily influence which blockchain is the best fit for real-world applications.

The certificate issuance process starts with the issuing authority creating a digital certificate that includes vital information. This certificate is then hashed using a cryptographic algorithm (like SHA-256). This resultant hash, along with essential metadata, gets recorded onto the blockchain via a smart contract, ensuring that it remains immutable. The certificate holder is given a unique certificate ID or QR code for verification purposes. The verification process entails fetching the hash from the blockchain, recalculating it from the issued certificate, and comparing the two. A successful match indicates the certificate's authenticity; if not, it raises suspicions of tampering or fraud.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Smart contracts are integral to the automation of certificate issuance, verification, and revocation. These self-executing programs guarantee that only authorized organizations can issue certificates, facilitate immediate verification, and allow for revocation in instances of academic misconduct or errors. To bolster security and privacy, the system implements cryptographic hashing to thwart tampering efforts, utilizes Zero-Knowledge Proofs (ZKPs) for validation without compromising sensitive information, employs role-based access control to regulate permissions, and incorporates data encryption to safeguard off-chain storage.

By incorporating these methodologies, the blockchain-based certificate authentication system provides a secure, scalable, and efficient solution compared to traditional centralized verification methods. It effectively assures the authenticity of digital credentials while diminishing fraud, heightening privacy, and making global access possible.

IV. IMPLEMENTATION DETAILS

The decentralized certificate authentication system employs blockchain technology and encompasses several key elements, such as blockchain setup, smart contract creation, certificate issuance, verification methods, and user interface design. This system is crafted to provide secure, unchangeable, and efficient certificate authentication while reducing the need for third-party intermediaries.

The journey begins with establishing a suitable blockchain network to securely store certificate hashes. A public blockchain (like Ethereum, Polygon, or Binance Smart Chain) offers transparency and immutability, while a private blockchain (such as Hyperledger Fabric or Quorum) allows for controlled access and scalability. This blockchain network is made up of multiple nodes tasked with validating transactions and maintaining the integrity of the ledger.

After the network is set up, smart contracts are deployed to streamline the processes of certificate issuance, verification, and revocation. These smart contracts are coded in Solidity (for Ethereum-based networks) or Chaincode (for Hyperledger Fabric,

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

managing crucial operations like registering certificates, retrieving stored hashes for verification, and updating or revoking records as needed.

The certificate issuance process kicks off when an institution generates a digital certificate in formats such as JSON, XML, or PDF, containing student details, course information, and the issuance date. A cryptographic hashing algorithm (e.g., SHA-256) is utilized to create a unique hash of the certificate, which is then logged onto the blockchain through a smart contract. Instead of storing the entire certificate, only the hash and minimal metadata (including certificate ID and institution details) are saved to enhance blockchain efficiency. The recipient receives a certificate ID or QR code, which can be utilized for verification purposes.

For certificate verification, the verifier scans the QR code or inputs the certificate ID into the verification portal. The system retrieves the stored hash from the blockchain and compares it to the hash of the certificate being presented. If both hashes align, the certificate is verified as authentic; if not, it is flagged as fraudulent or tampered with. This trustless verification process removes the necessity for third-party validation and enables global access to credentials in real time.

The system's front-end is crafted as a web-based portal utilizing either React.js or Angular, paired with web3.js or ethers.js to enable seamless blockchain interactions. The user interface is designed with features that allow institutions to issue and manage certificates, students to securely store

and share their credentials, and employers to easily search and verify the authenticity of certificates. To maintain scalability and cost efficiency, we are using off-chain storage solutions like IPFS (Interplanetary File System) or cloud-based services to hold complete certificate details, while only the hashes are kept on-chain. Furthermore, Layer-2 scaling solutions such as Polygon or Optimistic Rollups are employed to lower transaction costs and enhance processing speed.

The necessity for a secure and decentralized certificate authentication system has gained significant recognition in both academia and industry. Traditional methods for issuing and verifying certificates rely on centralized authorities, making them vulnerable to forgery, data breaches, and inefficiencies. In this section, we will review existing approaches and studies related to certificate authentication, blockchain-based credential verification, and associated technologies.

Numerous studies have highlighted the shortcomings of traditional certificate verification systems. Research conducted by Patel et al. (2020) indicates that these centralized verification methods necessitate manual checks by institutions or third parties, which can lead to delays, high administrative costs, and increased susceptibility to fraud. Furthermore, centralized databases that store certificates face risks of hacking or manipulation,

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

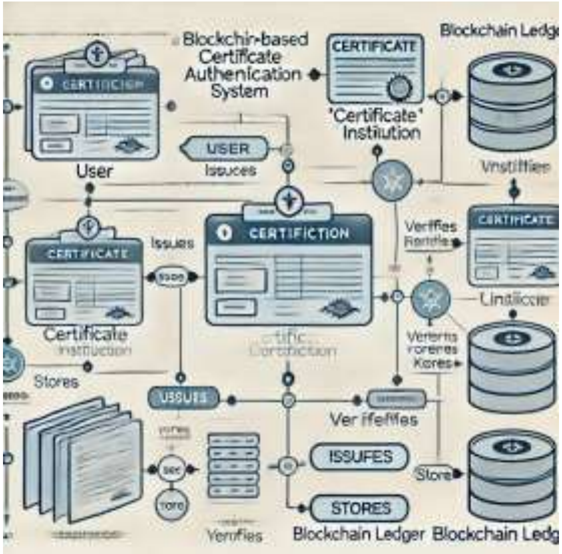
potentially resulting in the loss of critical academic records. To tackle these issues, researchers have suggested adopting blockchain-based solutions for the issuance and verification of academic credentials in a way that is tamper-proof.

Blockchain technology has attracted considerable attention in the field of digital credentials and identity management. A study by Sharma and Gupta (2021) introduced a public blockchain-based solution for secure degree verification, where certificates are stored as cryptographic hashes on the blockchain, ensuring immutability and transparency. The study emphasizes the benefits of utilizing Ethereum smart contracts to automate the authentication process, effectively removing the need for intermediaries. However, it also acknowledges challenges associated with high transaction fees and scalability issues in public blockchains. In response to these limitations, researchers have explored private and consortium blockchains, such as Hyperledger Fabric, which provide controlled access and improved efficiency.

In summary, the literature review indicates that blockchain technology offers a secure, transparent, and efficient alternative to traditional certificate authentication methods. While public blockchains foster decentralization and trust, private blockchains present scalability and cost benefits. Emerging technologies like ZKPs, decentralized identity (DID), and IPFS-based storage further enhance security and privacy. Nevertheless, challenges like high computational costs, network scalability, and regulatory compliance continue to be subjects of active research. The proposed system builds upon these findings by integrating smart contracts, cryptographic hashing, and decentralized storage to create a robust certificate authentication framework that is fraud-resistant, globally accessible, and highly scalable.

V. PROPOSED SYSTEM

The proposed blockchain-based certificate authentication system is designed to address the shortcomings of traditional centralized methods, offering a secure, decentralized, and tamper-proof solution for issuing and verifying digital certificates. Conventional certificate authentication typically depends on centralized entities like universities and certification organizations, which can be prone to fraud, data manipulation, and inefficiencies.



Our system harnesses the power of blockchain technology to guarantee that academic and professional certificates are immutable, verifiable, and globally accessible, without the need for intermediaries.

In this framework, educational institutions and certification bodies serve as the issuing authorities responsible for generating digital certificates. Rather than placing the entire certificate on the blockchain, we create a cryptographic hash of the certificate using secure hashing algorithms such as SHA-256. This hash, together with minimal metadata like the issuing institution's details and a timestamp, is recorded on the blockchain via smart contracts. The actual certificate can be stored off-chain using InterPlanetary File System (IPFS) or other decentralized storage solutions, which helps to maintain data privacy and adhere to regulations like GDPR. After a certificate is issued, the recipient (student or professional) receives a unique certificate ID or QR code, which can be easily shared with employers, institutions, or other entities needing to authenticate the certificate.

For the certificate verification process, verifiers, including employers and academic institutions, can scan the QR code or input the certificate ID into a verification portal. The system retrieves the stored hash from the blockchain and compares it to the hash of the provided certificate. If the hashes

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

match, the certificate is deemed authentic and untampered. Any discrepancies will flag the certificate as fraudulent or modified. The immutability of blockchain records ensures that certificates cannot be forged or altered post-issuance.

This system is developed using platforms like Ethereum, Hyperledger Fabric, or Polygon, chosen based on scalability and privacy needs. Smart contracts streamline the processes of certificate issuance, verification, and revocation, fostering trust while removing the possibility of human error. Additionally, we implement role-based access control (RBAC) to prevent unauthorized alterations, and leverage zero-knowledge proofs (ZKPs) to enhance privacy, allowing for verification without the need to reveal sensitive data.

By embracing this blockchain-based decentralized system, educational institutions, employers, and certification bodies can establish a more secure, transparent, and efficient method for managing digital credentials. This solution helps reduce administrative burdens, mitigates fraud risks, and provides an uncomplicated, globally accessible way to authenticate certificates.

VI. LITERATURE SURVEY

The necessity for a secure and decentralized certificate authentication system has gained significant recognition in both academia and industry. Traditional methods for issuing and verifying certificates rely on centralized authorities, making them vulnerable to forgery, data breaches, and inefficiencies. In this section, we will review existing approaches and studies related to certificate authentication, blockchain-based credential verification, and associated technologies.

Numerous studies have highlighted the shortcomings of traditional certificate verification systems. Research conducted by Patel et al. (2020) indicates that these centralized verification methods necessitate manual checks by institutions or third parties, which can lead to delays, high administrative costs, and increased susceptibility to fraud. Furthermore, centralized databases that store certificates face risks of hacking or manipulation, potentially resulting in the loss of critical academic records. To tackle these issues, researchers have suggested adopting blockchain-based solutions for the issuance and verification of academic credentials in a way that is tamper-proof.

Blockchain technology has attracted considerable attention in the field of digital credentials and identity management. A study by Sharma and Gupta (2021) introduced a public blockchain-based solution for secure degree verification, where certificates are stored as cryptographic hashes on the blockchain, ensuring immutability and transparency. The study emphasizes the benefits of utilizing Ethereum smart contracts to automate the authentication process, effectively removing the

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

need for intermediaries. However, it also acknowledges challenges associated with high transaction fees and scalability issues in public blockchains. In response to these limitations, researchers have explored private and consortium blockchains, such as Hyperledger Fabric, which provide controlled access and improved efficiency.

In summary, the literature review indicates that blockchain technology offers a secure, transparent, and efficient alternative to traditional certificate authentication methods. While public blockchains foster decentralization and trust, private blockchains present scalability and cost benefits. Emerging technologies like ZKPs, decentralized identity (DID), and IPFS-based storage further enhance security and privacy. Nevertheless, challenges like high computational costs, network scalability, and regulatory compliance continue to be subjects of active research. The proposed system builds upon these findings by integrating smart contracts, cryptographic hashing, and decentralized storage to create a robust certificate authentication framework that is fraud-resistant, globally accessible, and highly scalable.

VII.CONCLUSION AND FUTURE WORK

Incorporating blockchain technology for certificate authentication offers a groundbreaking approach to the limitations of traditional centralized verification systems. Conventional methods are often plagued by problems like certificate forgery, misplaced credentials, reliance on third-party verification, and administrative inefficiencies. With the decentralized and immutable characteristics of blockchain, the system proposed here guarantees secure, tamper-proof, and globally accessible certificate authentication. Utilizing cryptographic hashing, smart contracts, and decentralized storage options such as IPFS enables the issuance and verification of certificates independently, thereby reducing fraud and promoting transparency. Educational institutions can authenticate digital certificates on a blockchain network, providing instant validation for employers, universities, and other relevant parties. The trustless design of the system ensures that once a certificate is recorded, it is immutable, making it perfect for lifelong credential management. Additionally, Layer-2 scaling solutions like Polygon and Optimistic Rollups facilitate efficient transaction processes, lowering costs and enhancing scalability for broader acceptance. The adoption of Zero-Knowledge Proofs (ZKPs) and Decentralized Identity (DID) frameworks also boost privacy by allowing credential verification without disclosing sensitive information, thereby ensuring compliance with privacy laws like GDPR.

Nonetheless, blockchain-based certificate authentication must address certain challenges before achieving large-scale implementation. A primary concern is transaction costs on public blockchains, particularly on networks like Ethereum, where high gas fees can hinder adoption. While Layer-2 solutions help alleviate this issue, further enhancements are necessary to improve affordability and efficiency. Additionally, legal and regulatory recognition poses a significant hurdle, as many governments and educational institutions have yet to formally accept blockchain-based certificates as valid credentials. There is also a lack of technical understanding and institutional willingness to adopt these innovations, as many universities and employers continue to prefer traditional verification methods due to familiarity and ease of use. Furthermore, the use of private and consortium blockchains creates trust dependencies, as centralized control resides with a select group of authorized institutions, potentially limiting the level of transparency when compared to fully decentralized public blockchains.

For future endeavors, there are several significant enhancements that can be pursued to improve efficiency, security, and widespread acceptance of blockchain-based certificate authentication systems. To start, investigating interoperability between various blockchain networks could facilitate seamless cross-chain verification, so institutions utilizing different blockchain platforms can universally authenticate certificates. Exploring solutions such as Polkadot, Cosmos, and Chain-link might promote interoperability and data exchange across diverse blockchain ecosystems.

ACKNOWLEDGMENTS

I would like to extend my heartfelt gratitude to Mrs. B. Tejaswini, my mentor at TKR College of Engineering Technology, for her unwavering

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

guidance, expertise, and continuous support throughout the course of this research. Her insightful feedback, constructive criticism, and dedication were pivotal to the successful completion of this project.

REFERENCES

[1]. B. K. Chaurasia, ‘‘Blockchain enabled MediVault for healthcare system,’’ Multimedia Tools Appl., vol. 2024, pp. 1–21, Jun. 2024.

[2].A.K.Sharma,B.K.Chaurasia,andV.Singh,‘‘Bloc kchain-basedfeedback system using NFT in e-commerce,’’ Iran J. Comput. Sci., vol. 7, no. 3, pp. 579–587, Sep. 2024.

[3] S. A. Sultana, C. Rupa, R. P. Malleswari, and T. R. Gadekallu, ‘‘IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field,’’ Information, vol. 14, no.8,p.446,Aug.2023.

[4] T. de Souza-Daw and R. Ross, ‘‘Fraud in higher education: A system for detection and prevention,’’ J. Eng., Design Technol., vol. 21, no. 3, pp. 637–654, May 2023, doi: 10.1108/JEDT-12-2020-0504.

[5] A. Tariq, H. B. Haq, and S. T. Ali, ‘‘Cerberus: A blockchain-based accreditation and degree verification system,’’ IEEE Trans. Computat. Social Syst., vol. 10, no. 4, pp. 1503–1514, Aug. 2022.

[6] C.-S. Hsu, S.-F. Tu, and P.-C. Chiu, ‘‘Design of an e-diploma system based on consortium blockchain and facial recognition,’’ Educ. Inf. Technol., vol. 27, no. 4, pp. 5495–5519, May 2022, doi10.1007/s10639-021-10840-5.

[7] G. Ramakrishnan, M. Rehan, and G. Sujatha, ‘‘Solidity vulnerability scanner,’’ in Proc. Int. Conf. Data Sci., Agents Artif. Intell. (ICD SAAI), Chennai, India, vol. 1, Dec. 2022, pp. 1–5, doi: 10.1109/ICD SAAI55433.2022.10028877.

[8] P. Gugnani, W. W. Godfrey, and D. Sadhya, ‘‘Ethereum based smart contract for event management system,’’ in Proc. IEEE 6th Conf. Inf. Commun. Technol. (CICT), Gwalior, India, Nov. 2022,pp.1–5,doi: 10.1109/CICT56698.2022.9997939.

[9] S. Lin, Z. Li, S. Zhao, H. Zhao, Y. Li, and S. Wang, ‘‘Design and implementation of blockchain-based college education integrity system,’’ in Proc. IEEE 5th Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE), Dalian, China, Sep. 2022, pp. 276–281, doi: 10.1109/ICIS CAE55891.2022.9927601.

[10] M. Jurgelaitis, L. Ceponiene, and R. Butkiene, ‘‘Solidity code generation from UML state machines in model-driven smart contract development,’’ IEEE Access, vol. 10, pp. 33465–33481, 2022, doi: 10.1109/ACCESS.2022.3162227.

[11] M. Saim, M. Mamoon, I. Shah, and A. Samad, ‘‘E-voting via upgradable smart contracts on blockchain,’’ in Proc. Int. Conf. Futuristic Technol. (INCOFT), Belgaum, India, Nov. 2022, pp. 1–6, doi: 10.1109/INCOFT55651.2022.10094482.

[12] U. Rahardja, A. N. Hidayanto, P. O. H. Putra, and M. Hardini, ‘‘Immutable ubiquitous digital certificate authentication using blockchain protocol,’’ J. Appl. Res. Technol., vol. 19, no. 4, pp. 308–321,Aug.2021.

[13] D. Maji, R. S. Lamkoti, H. Shetty, and B. Gondhalekar, ‘‘Certificate verification using blockchain and generation of transcript,’’ Int. J. Eng. Res. Technol., vol. 10, no. 3, pp. 1–6, Apr. 2021.

[14] F. M. Enescu, N. Bizon, and V. M. Ionescu, ‘‘Blockchain technology protects diplomas against fraud,’’ in Proc. 13th Int. Conf. Electron., Comput. Artif. Intell. (ECAI), Pitesti, Romania, Jul. 2021, pp. 1–6, doi: 10.1109/ECAI52376.2021.9515107.

[15] Meyliana, Surjandy, E. Fernando, C. Cassandra, H. A. Eka Widjaja, Y. U. Chandra, and H. Prabowo, ‘‘A blockchain technology-based for university Student enrollment process,’’ in Proc. 6th Int. Conf. Comput. Eng. Design (ICCED), Sukabumi, Indonesia, Oct. 2020, pp. 1–4, doi: 10.1109/ICCED51276.2020.9415856.

[16] D. Čeke and S. Kunosić, ‘‘Smart Contracts as a diploma anti-forgery system in higher education—A pilot project,’’ in Proc. 43rd Int. Conv. Inf., Commun. Electron. Technol. (MIPRO), Opatija, Croatia, 2020, pp. 1662–1667, doi: 10.23919/MIPRO48935.2020.9245391.

[17] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, ‘‘Blockchain-based medical records secure storage and medical service framework,’’ J. Med. Syst., vol. 43, no. 1, pp. 1–9, Jan. 2019.

[18] 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.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

[19] T. Aste, P. Tasca, and T. Di Matteo, ‘‘Blockchain technologies: The foreseeable impact on society and industry,’’ Computer, vol. 50, no. 9, pp.18–28,2017.

[20] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, ‘‘Public key authentication and key agreement in IoT devices with minimal airtime consumption,’’ IEEE Embedded Syst. Lett., vol. 9, no.1,pp.1–4,Mar.2017.

[21] C.-S. Park, ‘‘A secure and efficient ECQV implicit certificate issuance protocol for the Internet of Things applications,’’ IEEE Sensors J., vol. 17, no. 7, pp. 2215–2223, Apr. 2017.

[22] K.Christidis and M. Devetsikiotis, ‘‘Blockchains and smart contracts for the Internet of Things,’’ IEEE Access, vol. 4, pp. 2292–2303, 2016.

[23] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, ‘‘Key management protocol with implicit certificates for IoT systems,’’ in Proc. Workshop IoT Challenges Mobile Ind. Syst., May 2015, pp. 37–42.