iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.65924

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Academic Certificate Authenticity using Blockchain Technology: A Review

Poornima K M[1], Aishwarya K Hirematha[2], Aishwarya K P[3], Anukeerthana M B[4], Eshani C M[5]
Department of CS&E, JNN College of Engineering, Shivamogga, Karnataka, India

Abstract: Blockchain technology has emerged as a significant area of research in recent years, especially in addressing issues like record forgery and inefficiencies in verification processes. This paper explores the application of blockchain in academic certificate authentication, leveraging its immutable, transparent, and decentralized nature to securely issue, store, and verify credentials. The study emphasizes blockchain's potential to revolutionize traditional methods by ensuring authenticity and minimizing fraud.
Keywords: Blockchain, Academic Certificates, Decentralized Systems, Authentication, Hyper Ledger Fabric.

I. INTRODUCTION

In the era of digital transformation, ensuring the authenticity and integrity of academic certificates is critical. Traditional methods, often reliant on centralized authorities, are prone to forgery and inefficiencies. Blockchain technology offers a decentralized solution to these challenges by introducing tamper-proof, transparent, and secure mechanisms for certificate management. This paper delves into the advantages of adopting blockchain for academic certificate authentication and its transformative potential.

II. LITERATURE SURVEY

In this section, various authors have presented various blockchain technologies and smart contract techniques.

In [1], 34 studies on blockchain-based systems for academic certificate verification were made focusing on research published between 2018 and 2022. It categorizes the literature into six key topics: blockchain classification, automated degree generation, security, transparency, adaptability, and enabling technologies. The review emphasizes blockchain's potential to address the persistent issues of degree fraud and inefficient verification by offering a decentralized, tamper-proof solution. It highlights various blockchain systems, such as Ethereum and Hyperledger, used in developing these systems, each with its unique features and challenges. The review also identifies significant gaps, such as the need for standardization, compliance with privacy laws, and better integration with existing educational infrastructures. Future research should focus on developing quantum-resistant cryptographic techniques and enhancing user interfaces. Collaborative efforts among educational institutions, developers, and policymakers are crucial for creating a universally accepted blockchain-based framework.

In [2], the evolution, implementation, and challenges of smart contracts within blockchain ecosystems. Smart contracts represent autonomous, self-executing agreements encoded into digital formats. The paper categorizes contracts into paper, digital, and data-oriented types, highlighting their transition into computable and smart contract forms. Using the SPESC language, the authors suggest embedding legal clauses into smart contracts, bridging conventional legal agreements with digital frameworks. Challenges such as code vulnerabilities, human interpretation errors, and limited relevant use cases are addressed by proposing solutions like decentralization, enhanced supervision, and the standardization of programming languages. The paper also emphasizes the risks posed by automated performance clauses in terms of transaction management and user rights. Future research should focus on broadening smart contract applications across sectors such as finance and governance, while addressing risks through improved design standards and legal adaptability. The study underscores smart contracts' transformative potential in digital transactions

In [3], exploration of the application of the Truffle Suite in developing decentralized applications (DApps) within blockchain environments. It highlights the evolution of blockchain technology into the application phase, which includes advancements such as decentralized systems. The components of the Truffle Suite—Ganache, Truffle, and Drizzle—are discussed, with a focus on their role in simplifying smart contract testing and deployment. The research also demonstrates a use case involving the enhancement of GPIO simulator security using blockchain. Challenges in DApp scalability and real-time configuration are acknowledged, emphasizing the Truffle Suite's utility in addressing these issues. This study underscores blockchain's potential in IoT security and practical DApp development, aiming to achieve a decentralized, transparent, and tamper-proof ecosystem.

In [4], an in-depth analysis of blockchain-based decentralized applications (DApps), categorizing them into four architectures: native client, smart contract, web & contract, and fully decentralized. These applications leverage blockchain's trustless and tamper-resistant features for decentralized operations across industries such as finance (DeFi), gaming (GameFi), and data provenance (NFTs). The study identifies the benefits of DApps, including enhanced security, efficiency, and autonomy, but also highlights challenges like low throughput, scalability, and security risks. Economic issues such as tax evasion and miner manipulation are analyzed, along with security challenges like smart contract vulnerabilities and web-layer attacks. Recent research on formal verification, automated testing, and DApp templates is explored to address these issues. The paper advocates for standardized benchmarks and performance evaluation frameworks to improve DApp usability and scalability. With further advancements, DApps could become crucial to decentralized ecosystems, transforming industries worldwide.

In [5], a comprehensive analysis of the development, challenges, and applications of smart contracts in blockchain ecosystems over the last decade. Smart contracts are defined as self-executing agreements that leverage blockchain's decentralized architecture to automate and enforce contract terms. The transformative impact on industries such as finance, supply chains, and intellectual property management, offering benefits like reduced transaction fees, increased transparency, and automation. However, it also identifies significant challenges, including coding vulnerabilities, scalability limitations, and the "oracle problem," which complicates interactions with off-chain data. The study examines popular platforms like Ethereum, Hyperledger Fabric, and Stellar, evaluating their suitability for smart contract deployment. Future research directions include enhancing security, scalability, and regulatory frameworks to address existing barriers. The paper concludes by underscoring the pivotal role of smart contracts in advancing blockchain technology, paving the way for more efficient and transparent decentralized applications.

In [6], the implementation of a Hyperledger Fabric-based cross-border fund transfer application offers a secure, efficient, and transparent solution for cross-border payments. The platform facilitates direct transactions between financial institutions, significantly reducing delays and costs associated with traditional methods. Transparency and accountability are enhanced through fund tracking and transaction visibility, which boosts confidence and mitigates fraudulent activities. However, the system's implementation poses challenges, such as the need for interoperability across financial systems, collaboration with regulatory bodies, and scalability concerns as transaction volumes increase. Continuous development and optimization are required to ensure sustainability and address these challenges.

In [7], the adoption of Hyperledger Fabric as a blockchain platform for healthcare applications provides a patient-centric, interoperable system to address challenges in health data management. By leveraging a permissioned blockchain framework, this system ensures data confidentiality, privacy, and access control. The modular architecture of Hyperledger enables integration with existing systems while offering scalability and flexibility. Key advantages include secure data sharing, reduction in fraud through immutable records, and enhanced patient control over their medical data. However, challenges persist, such as the need for compliance with privacy regulations like GDPR and the complexity of ensuring transaction scalability. Despite these hurdles, the system shows promise for transforming healthcare delivery by enabling transparent, secure, and efficient data exchanges.

In [8], a decentralized system to address challenges in verifying educational certificates, leveraging Hyperledger Fabric and IPFS technologies. The methodology involves using Hyperledger Fabric for maintaining a secure, immutable ledger and IPFS for decentralized file storage, ensuring integrity and accessibility. The system operates in two stages: certificate issuance, where universities securely issue and store certificates on the blockchain, and certificate verification, enabling easy retrieval and validation of certificates using a unique ID. Advantages include enhanced transparency, security, and efficiency, reducing costs and effort associated with traditional methods, while providing robust protection against forgery. However, the study acknowledges limitations like unexplored network scalability and varying transaction loads, suggesting further work on expanding the network to include more organizations and channels. Future research could explore interoperability and integrate advanced technologies like AI to enhance system capabilities.

In [9], the exploration of blockchain-based pharmaceutical supply chain management system implemented using Hyperledger Fabric and Sawtooth frameworks. Integration of cryptographic logging, smart contracts for automation, and a query service for streamlined data retrieval. TrackChain addresses challenges such as interoperability and resource optimization, employing cross-chain and transfer-chain technologies for seamless operation. The study highlights Sawtooth's advantages in resource efficiency, scalability, and parallel transaction handling, making it more suitable for resource-constrained scenarios compared to Fabric, which demonstrates higher CPU utilization. While the system ensures enhanced transparency, security, and traceability, challenges such as resource-intensive components like validators and consensus algorithms remain. Future directions include developing cross-blockchain connectivity protocols and extending stakeholder participation for improved interoperability and supply chain efficiency.

In [10], the adoption of blockchain-enabled smart contracts across various industries, emphasizing their capacity to automate agreements without relying on intermediaries. Smart contracts are highlighted as a transformative tool providing speed, accuracy, cost-effectiveness, and improved agreement in transactions. Applications span healthcare, supply chains, and energy management, showcasing their potential to revolutionize traditional processes. The study addresses challenges such as coding vulnerabilities, regulatory hurdles, and performance barriers, recommending strategies like code reviews, encryption, and Layer 2 solutions to mitigate risks. Moreover, it discusses the scalability of smart contracts and their impact on decentralization and transparency. By eliminating intermediaries, smart contracts reduce operational costs and enhance security, while their automated nature minimizes human errors. Despite the outlined challenges, the paper stresses the significant potential of blockchain and smart contracts to foster innovation and streamline operations in various fields, making them pivotal to the future of decentralized ecosystems.

In [11], the growing threat of quantum computing to current blockchain systems by presenting a quantum-resistant smart contract framework. Conventional cryptographic algorithms, such as elliptic curve cryptography, are vulnerable to quantum attacks, necessitating more secure alternatives. The researchers implement lattice-based cryptography, known for its robustness against quantum threats, to enhance the digital signatures used in smart contracts. Additionally, the study proposes a peer-to-peer (P2P) network structure featuring an identity agent layer to enable secure cross-chain communication between different blockchain systems. This approach not only strengthens security but also facilitates interoperability, a critical challenge in modern blockchain ecosystems. Performance reviews conducted in a simulated Bitcoin transaction environment reveal that the proposed system maintains performance and scalability while providing robust protection against quantum attacks. This innovation ensures the long-term reliability and security of blockchain applications, making them resilient to emerging computational threats.

In [12], a novel approach to detecting deepfakes using blockchain technology. It leverages blockchain's transparency and immutability to store hash values of authentic media files, enabling verification against potentially manipulated content. The researchers utilize deep learning models, such as Convolutional Neural Networks (CNNs), for feature extraction and classification of deepfake media. The system ensures secure, decentralized storage and tracking of media authenticity, addressing the growing threats posed by deepfake technologies. To enhance detection accuracy, the authors integrate blockchain with AI-based techniques for real-time media validation. Their evaluation validated a detection accuracy exceeding 97%, highlighting the system's robustness. Challenges such as scalability, resource utilization, and real-time processing were addressed using optimized blockchain protocols. This study offers a promising framework for deploying secure, efficient, and scalable solutions to combat the growing misuse of deepfake technology in areas such as media, forensics, and cybersecurity.

Table 1: Summarization of various authors

Authors	Title	Research Focus	Observations
A. Rustemi et al. (2023)	A Systematic Literature assessment on Blockchain-based totally structures for Academic Certificate Verification	34 studies on blockchain-based academic certificate verification and highlights decentralization as a solution to fraud.	Addresses gaps in standardization and privacy law compliance.
T. Mao and J. Chen (2023)	Clever Contract in Blockchain	Evolution and challenges of implementing smart contracts in blockchain ecosystems.	Transformative applications and solutions to vulnerabilities.
Rajat Verma, Namrata Dhanda, Vishal Nagar (2023)	Application of Truffle Suite in a Blockchain Environment	Use of the Truffle Suite to develop decentralized applications (DApps) within a blockchain environment.	Utility of Truffle Suite in simplifying smart contract deployment while addressing challenges like scalability and configuration.
P. Zheng et al. (2023)	Blockchain-based totally Decentralized application: A Survey	Decentralized applications (DApps) with a focus on security, scalability, and economic considerations.	Advocates for standardized benchmarks to enhance adoption.
H. Taherdoost (2023)	Smart Contracts in Blockchain generation: A essential overview	Comprehensive review of smart contracts in blockchain technology.	Development, applications, and challenges of smart contracts over the past decade.

A. Rengarajan, K. C. A. Parashar (2023)	Hyperledger Fabric Based Blockchain Cross-Border Fund Transfer Application	Development of a Hyperledger Fabric-based platform for secure, efficient, transparent cross-border fund transfers.	Reduction in delays and costs and enhancement in transparency.
P., K. N., S. K. W., B. P. D. (2023)	Private Blockchain in the Field of Health Services	Usage of Hyperledger Fabric, a private blockchain, for secure and interoperable healthcare applications.	Hyperledger Fabric being the suitable blockchain to address medical fraud and to ensure secure management of patient data.
R. A. Jaafar, S. N. Alsaad (2023)	Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric	Developing a decentralized system using Hyperledger Fabric and IPFS for secure educational certificate verification.	Transparency, security, and efficiency enhancement. Future focus on interoperability and integrating AI.
C. M. N. Sudha, J. V. N. J. (2023)	TrackChain: Hyperledger based pharmaceutical supply chain – Resource utilization perspective	Exploration of blockchain-based pharmaceutical supply chain Hyperledger Fabric and Sawtooth for improved efficiency and interoperability.	Resource optimization and transparency but faces challenges in scalability, resource-intensive components.
A. Prasad, P. B., D. G., S. K. S. (2023)	Blockchain – Enabled Smart Contracts	Adoption of blockchain-enabled smart contracts across industries.	Transformative potential of smart contracts in healthcare, supply chains, and energy management.
X. Zheng (2024)	studies on Blockchain clever contract technology primarily based on resistance to quantum computing assaults	Quantum-resistant smart contract framework utilizing lattice-based cryptography.	Lattice-based cryptography for digital signatures and proposes a P2P network with an identity agent layer for cross-chain communication.
Khaled Salah (2024)	Deepfake Detection by way of using Blockchain era	Integration of blockchain with AI to secure and validate media authenticity in real-time.	A robust framework for combating deep-fake technology.

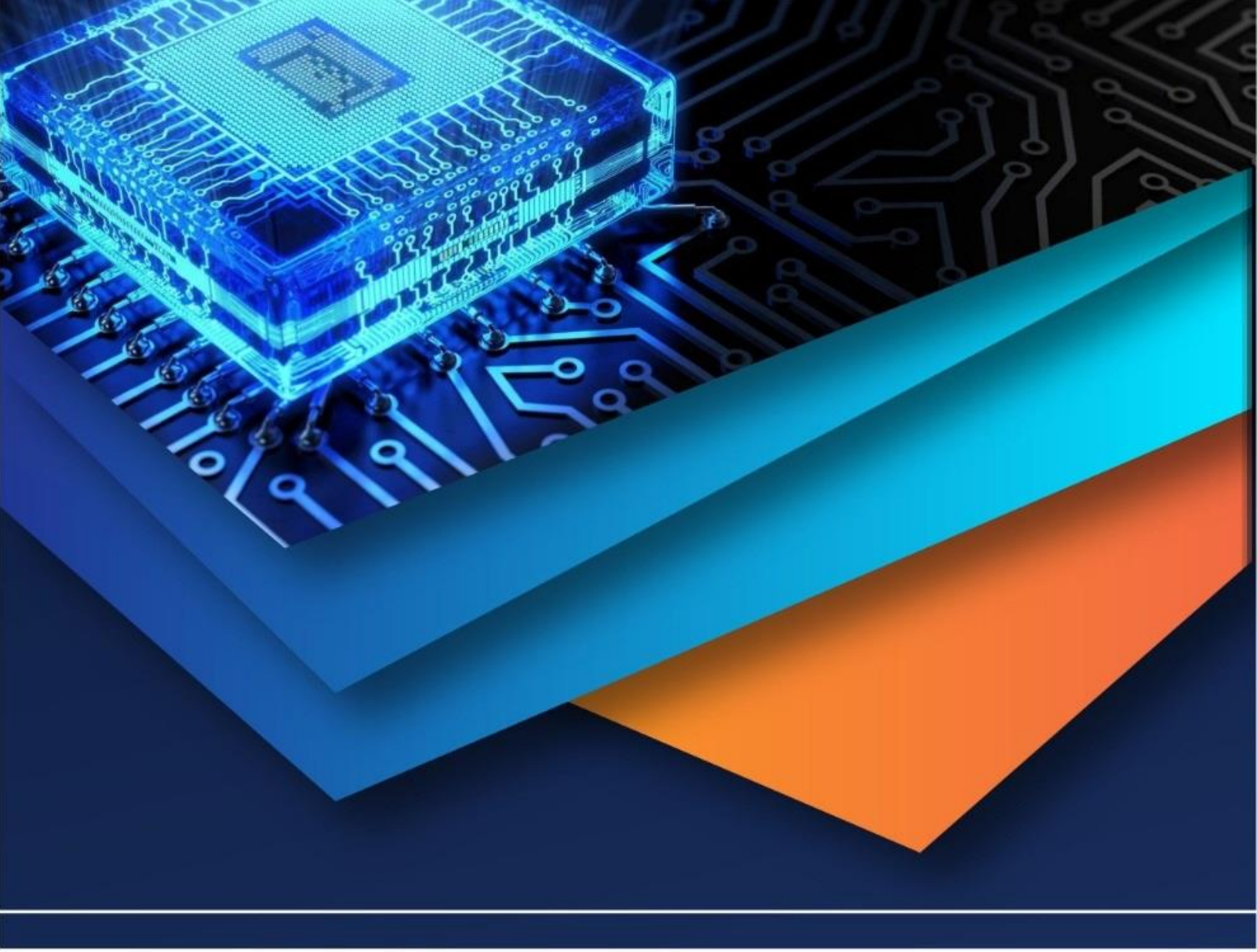
III. CONCLUSION

The integration of blockchain technology in academic certificate authentication offers a robust solution to persistent challenges such as document fraud and inefficiencies in verification processes. The decentralized, tamper-proof nature of blockchain ensures transparency and reliability. Future research should focus on standardization and enhanced interoperability to encourage widespread adoption across educational institutions.

REFERENCES

[1] Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature assessment on Blockchain-based totally structures for Academic Certificate Verification," IEEE get admission to, vol. 11, pp. 64679-64685, 2023.
[2] T. Mao and J. Chen, "Clever Contract in Blockchain," proceedings of ICBBEM 2022, AHIS 5, pp. 868–875, 2023.
[3] R. Verma, N. Dhanda, and V. Nagar, “Application of Truffle Suite in a Blockchain Environment,” in Proc. 3rd Int. Conf. Comput., Commun., Cyber-Security, 2023, pp. 693–701.
[4] P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, "Blockchain-based totally Decentralized application: A Survey," IEEE Open journal of the computer Society, pp. 1–10, 2023.
[5] H. Taherdoost, "Smart Contracts in Blockchain generation: A essential overview," information, vol. 14, no. 117, pp. 1–19, 2023.
[6] Rengarajan A., and Adithya Parashar K. C., "Hyperledger Fabric Based Blockchain Cross-Border Fund Transfer Application," Int. J. Adv. Res. Comput. Commun. Eng., vol. 12, no. 3, pp. 24-28, Mar. 2023.
[7] Purwono, Khoirun Nisa, Sony Kartika Wibisono, and Bala Putra Dewa, "Private Blockchain in the Field of Health Services," J. Adv. Health Inform. Res., vol. 1, no. 1, pp. 10-15, Apr. 2023.
[8] R. A. Jaafar and S. N. Alsaad, "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric," TEM Journal, vol. 12, no. 4, pp. 2385–2395, Nov. 2023.

[9] C. M. Naga Sudha and Jesu Vedha Nayahi J., "TrackChain: Hyperledger based pharmaceutical supply chain – Resource utilization perspective," Heliyon, vol. 10, no. 1, pp. e23250, Dec. 2023.
[10] A. Prasad, P. B, D. G, and S. okay. S, "Blockchain – Enabled Smart Contracts," international magazine of Advances in Engineering architecture technology and generation (IJAEAST), vol. 1, no. 6, pp. 12–20, 2023.
[11] X. Zheng, "studies on Blockchain clever contract technology primarily based on resistance to quantum computing assaults," PLOS ONE, vol. 19, no. five, pp. 1-22, 2024.
[12] Khaled Salah,Khalifa University "Deepfake Detection by way of using Blockchain era," 2024



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY