www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 01, January 2025, pp : 721-724

e-ISSN : 2583-1062
Impact Factor : 7.001

BLOCKCHAIN TECHNOLOGY BASED DOCUMENTS VERIFICATION & VALIDATION

Prashant Gumgaonkar[1], Yash Meshram[2], Abhishek Biradar[3], Mayur Kamane[4], Anurag Prajapati[5], Masum Pathan[6]

[1]HOD, Information Technology Department, GWCET, Nagpur, India.

[2,3,4,5,6]Student, Information Technology Department, GWCET, Nagpur, India.

DOI: https://www.doi.org/10.58257/IJPREMS38144

ABSTRACT

In the digital realm, everything is digitized, including certificates of SSL, HSC, and academic certificates, which are provided to students by educational institutions. Maintaining degree certificates can be challenging for students. The organization and institution find the process of verifying and validating certificates to be time-consuming and burdensome. Our project will facilitate the storage of the certificate in the blockchain system, ensuring its security. Initially, the paper certificates are transformed into digital certificates. The disorganized algorithm is employed to produce the hash code value for the certificate. Once the certificates are verified, they are securely stored in the blockchain. These certificates are verified using the mobile application. By implementing blockchain technology, we can enhance the security and efficiency of digital certificate validation.

Keywords: blockchain, digital certificate, hashing, a chaotic algorithm.

1. INTRODUCTION

In 2008, blockchain technology was introduced by Satoshi Nakamoto, marking a revolutionary step in the realm of digital data security. Blockchain is an innovative, decentralized online ledger that facilitates transparent and secure data sharing without the need for intermediaries. This distributed ledger technology (DLT) ensures that information stored within it is immutable, tamper-proof, and accessible only to authorized parties. Over the years, blockchain has transcended its initial application in cryptocurrencies and has become a pivotal tool across various industries, including education, finance, healthcare, and supply chain management.

This project aims to leverage blockchain technology by developing an Android application designed to ensure the secure verification of academic certificates. Today, the authenticity and reliability of graduation certificates and transcripts have become a growing concern. These critical documents, often containing sensitive information, are vulnerable to manipulation and forgery by unauthorized individuals. Furthermore, the ease of accessibility to such information by external parties poses a significant risk to privacy and confidentiality. Consequently, there is an urgent need for an effective and secure system that guarantees the authenticity of these documents, ensuring they originate from credible and authorized sources while eliminating the possibility of counterfeiting.

In recent years, various systems have been proposed to address the challenges associated with e-certificates, particularly for educational institutions. These systems often rely on cloud-based platforms to store digital certificates securely. However, traditional cloud storage systems have their limitations, including susceptibility to hacking and unauthorized access. Blockchain technology emerges as a robust solution to overcome these challenges, offering unparalleled security and reliability. When combined with advanced hashing techniques and cryptographic methods, blockchain becomes an exceptionally potent tool for safeguarding sensitive data, such as academic certificates.

Blockchain's inherent features, such as decentralization, transparency, and immutability, make it an ideal choice for developing a secure certificate verification system. By employing blockchain, the need for continuous manual verification of certificates is significantly reduced. Each certificate issued by an educational institution can be stored as a unique record on the blockchain, complete with a digital signature to ensure authenticity. These records are immutable and can be accessed by authorized parties for verification purposes, thereby eliminating the risk of fraud or forgery.

Digital signatures play a crucial role in enhancing the security of digital documents. These cryptographic tools ensure that the document has not been altered after its creation, thereby maintaining its integrity. Additionally, digital signatures provide authentication by verifying the identity of the issuer and non-repudiation, ensuring that the issuer cannot deny having signed the document. The integration of digital signatures with blockchain technology amplifies the overall security of the system, making it virtually impossible for malicious actors to tamper with or forge academic certificates.

The implementation of blockchain technology in this project addresses several critical issues in the realm of certificate management. Firstly, it ensures the authenticity of certificates by verifying their origin and guaranteeing that they have been issued by a legitimate and authorized institution. Secondly, it enhances the confidentiality of sensitive information

by restricting access to authorized parties only. Thirdly, it provides a transparent and efficient mechanism for storing and verifying certificates, eliminating the need for time-consuming and error-prone manual verification processes.

The Android application developed in this project serves as a user-friendly interface for students, educational institutions, and employers. Students can upload their certificates to the blockchain, ensuring they are securely stored and easily verifiable. Educational institutions can issue digital certificates directly through the application, complete with digital signatures and unique blockchain records. Employers, on the other hand, can use the application to verify the authenticity of certificates quickly and reliably, reducing the risk of hiring candidates with counterfeit qualifications.

One of the key advantages of using blockchain for certificate management is its ability to create a tamper-proof record of each certificate. Every certificate stored on the blockchain is assigned a unique hash, which acts as a digital fingerprint. Any attempt to alter the certificate would result in a mismatch between the original hash and the modified document, immediately flagging the tampering attempt. This feature ensures the integrity of certificates and builds trust among stakeholders, including students, institutions, and employers.

Furthermore, blockchain technology enables secure and decentralized storage of certificates. Unlike traditional centralized storage systems, where data is stored in a single location and is vulnerable to hacking, blockchain distributes data across a network of nodes. This decentralized architecture makes it nearly impossible for hackers to compromise the system, as they would need to gain control of the majority of nodes in the network—a highly unlikely scenario.

The combination of blockchain technology and digital signatures also ensures compliance with global data protection regulations, such as the General Data Protection Regulation (GDPR). By restricting access to authorized parties and providing a transparent mechanism for data handling, this system aligns with the principles of data privacy and security, offering peace of mind to users.

In conclusion, this project highlights the transformative potential of blockchain technology in addressing the challenges associated with certificate verification and management. By developing an Android application that integrates blockchain and digital signature technologies, we aim to create a secure, reliable, and efficient system for managing academic certificates. This solution not only reduces the risk of forgery but also enhances the overall security, validity, and confidentiality of these critical documents. As blockchain technology continues to evolve, its application in the education sector is poised to revolutionize the way academic credentials are issued, stored, and verified, setting a new standard for trust and transparency.

2. LITERATURE SURVEY

Jin-Chiou et al. [1] developed software aimed at addressing the issue of forged certificates. Graduation certificates, due to their lack of anti-forgery mechanisms, are prone to counterfeiting. To counter this, they designed a decentralized application leveraging Ethereum blockchain technology. The process involves generating a digital version of the paper certificate and storing its hashed value in the blockchain. While the system ensures certificate authenticity and reduces the reliance on paper, it requires a separate scanning application to validate the certificate, necessitating a smartphone and an active internet connection.

Ze Wang et al. [2] proposed a system for certificate transparency and revocation using blockchain technology. In this approach, a Certificate Authority (CA) digitally signs certificates, and the revocation status is published by the CA in public logs, allowing for transparent monitoring of its operations. The system was implemented with Firefox and Nginx, offering trust in the process. However, certificate validation suffers from delays, and users may experience a misleading sense of security.

Madala et al. [3] utilized the Hyperledger Fabric blockchain platform to issue certificates. Here, the Certificate Authorities (CAs) can issue certificates only after receiving approval from domain owners. The system incorporates Google's Certificate Transparency (CT) technique, designed to prevent unauthorized SSL/TLS certificates from being issued. Despite its innovative approach, this system faces challenges with scalability and low transaction throughput.

Aisong Zhang et al. [4] introduced a consortium blockchain-based system that employs a secret sharing scheme to validate digital certificates. This method safeguards both user information and property while managing certificate revocation through collaboration among CAs. The trustworthiness of the Certificate Revocation List (CRL) in this system is higher compared to traditional methods. Certificate verification involves decrypting the signature using the public key and comparing the resulting hash with that of the original message. If the values match, the certificate is deemed untampered. However, the system still leaves room for a false sense of security.

Macro Baldi et al. [5] designed a system for certificate validation using public ledgers and blockchain. In this approach, CRLs are distributed via a private blockchain and shared among CAs, which are responsible for both issuing certificates and maintaining CRLs. This setup ensures authentication and certificate revocation list availability at all times. However, the ecosystem remains vulnerable due to its fragility and susceptibility to compromise.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 01, January 2025, pp : 721-724
e-ISSN : 2583-1062
Impact Factor : 7.001

3. OBJECTIVES

- **Enhanced Security with Blockchain**
  Utilize the immutable nature of blockchain technology to ensure robust security for digital certificates. The unmodifiable property of the blockchain prevents unauthorized alterations, safeguarding the authenticity of the certificates.
- **Transparency and Confidentiality**
  Ensure a balance between transparency and confidentiality. Each transaction within the blockchain network is visible to authorized peers, providing a clear audit trail while protecting sensitive data from unauthorized access.
- **Offline Functionality**
  Design the application to function seamlessly in offline mode, allowing users to validate certificates without requiring an active internet connection. This feature ensures accessibility in areas with limited connectivity.
- **Rapid Certificate Validation**
  Implement mechanisms for swift and efficient certificate verification. The validation process is streamlined to minimize delays, offering users a smooth and hassle-free experience.
- **Accurate and Reliable Information**
  Provide users with trustworthy and precise data regarding the authenticity of digital certificates. The system aims to eliminate discrepancies and ensure reliability in certificate verification.
- **User-Friendly System**
  Develop an intuitive and user-friendly interface to cater to both technical and non-technical users. This approach ensures that the application is accessible to a broader audience.
  By addressing these objectives, the project seeks to create a secure, transparent, and efficient solution for validating digital certificates.

4. PROPOSED MODEL

Methodology

The proposed system aims to convert academic and sports certificates into digital certificates using sampling and quantization techniques. Each certificate is assigned a hash value, generated using a chaotic algorithm, which is then stored within a blockchain. A block comprises the hash value, timestamp, and the hash of the previous block, forming a chain of interconnected blocks. Institutions can register student details, including name and email ID, through the application interface, and these details are stored in the database. Certificates issued by the registrar are added to the blockchain through the application. Employers or verifiers can validate these certificates by entering the student's information.

Digital Certificate Creation

Student certificates are transformed into digital format using an analog-to-digital conversion method. Both academic and sports certificates issued by institutions are uploaded to the system. Through the conversion process, each certificate is represented in binary form (0s and 1s). The system uses a 2D function to map each pixel value of the digital certificate. Administrators can log in through the admin interface to upload certificates. Once uploaded, certificates are digitized via sampling and quantization. The interface includes options to register students or upload certificates through "Add Student" and "Add Certificate" buttons.

Hash Code Generation

The chaotic algorithm generates a unique hash value for each digital certificate. This algorithm accepts inputs of varying sizes and produces fixed-size outputs. It uses a predefined mapping scheme, parameters, and initial conditions to ensure collision resistance. The same conditions are used during verification to ensure consistency. Compared to SHA-1, chaotic hash functions offer higher resistance to collisions, providing enhanced security.

Digital Certificate Validation

Validation involves verifying the stored certificates in the blockchain by matching hash values. The hash value comparison ensures that no tampering has occurred. Employers or verifiers can log in to the application using their credentials, select the certificate type, and initiate the validation process. If the certificate is genuine, the system will display a success message. If tampering or modifications are detected, the system will flag the certificate as invalid or altered.

Working of the Application

The application consists of three primary sections: the admin login, student and certificate management, and the verifier page. Administrators can log in using their credentials to add student information and upload certificates. Using "Add Student" and "Add Certificate" options, the system registers students and uploads their documents. Verifiers can access

the verifier interface with their login details, select the type of certificate, and validate it by providing the student's login ID. The system displays a success message for authentic certificates and an error message for tampered or invalid ones.

5. CONCLUSION

This paper introduces a blockchain-based approach to combat the growing issue of certificate forgery. Data security is a fundamental necessity in digital systems, and blockchain technology, with its immutable and decentralized nature, provides a robust solution for safeguarding sensitive information. By utilizing blockchain's unmodifiable property, this system significantly reduces the possibility of certificate tampering or forgery, ensuring authenticity and reliability.

The proposed application enables users to seamlessly view and validate digital certificates, making the verification process straightforward and efficient. It guarantees data accuracy by utilizing advanced hashing algorithms and blockchain mechanisms, ensuring that certificates remain unaltered and trustworthy.

Furthermore, the system simplifies certificate management for both administrators and verifiers, offering a user-friendly platform for handling digital certificates. By integrating security, accuracy, and ease of use, this solution addresses the challenges of traditional certificate systems and sets a strong foundation for secure digital certificate management in the future.

6. REFERENCES

[1] M. Aldwairi, M. Badra, and R. Borghol, "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," 2023.

[2] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. A. Azad, and N. Mansoor, "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," 2023.

[3] M. Rahman, M. T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-based certificate authentication system with enabling correction," 2023.

[4] Y. Abu Hammoudeh, M. Qatawneh, O. Abualghanam, and M. Almaiah, "Digital Certificate Validation Using Blockchain: A Survey," in Proceedings of the 2023 International Conference on Information Technology (ICIT), 2023.

[5] A. Geethakumari and C. Sweethapreethi, "Educational Certificate Verification Using Blockchain Based Framework," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, pp. 560-566, 2021.

[6] M. Toorani and C. Gehrmann, "A Decentralized Dynamic PKI based on Blockchain," arXiv preprint arXiv:2012.15351, 2020.

[7] H. Kinkelin, R. von Seck, C. Rudolf, and G. Carle, "Hardening X.509 Certificate Issuance using Distributed Ledger Technology," arXiv preprint arXiv:2004.07063, 2020.

[8] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and Smart Contract for Digital Certificate," in Proceedings of the IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1046-1051.

[9] L. S. B. S. Hossain, M. I. Ali, and D. S. R. Ghosh, "Blockchain-Based Digital Certificate Management System," International Journal of Computer Science and Network Security, vol. 18, no. 7, pp. 121-127, 2018.

[10] J. Kang, S. G. Lee, and S. Lee, "A Blockchain-Based Approach for Certificate Validation and Verification," Journal of Information Security and Applications, vol. 43, pp. 44-52, 2018.

[11] A. B. A. S. Hossain and M. H. Younus, "Blockchain Technology for Certificate Validation: A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 8, no. 10, pp. 70-73, 2018.

[12] P. J. S. Shi and J. L. He, "Digital Certificate Verification Using Blockchain Technology," IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3124-3132, 2020.

[13] V. L. C. Gunasekara and M. C. R. Wijesekera, "Blockchain-Enabled Digital Certificate Management System for Educational Institutions," International Journal of Computer Applications, vol. 182, no. 5, pp. 35-42, 2019.

[14] K. A. J. Sundararajan and S. Srinivasan, "Blockchain for Digital Certificates: A Proof of Concept," Journal of Blockchain Research, vol. 7, pp. 99-109, 2019.

[15] B. K. Ahuja and D. W. L. Liu, "Blockchain-Based Secure Digital Certificate System," International Journal of Computer Science and Engineering, vol. 34, no. 1, pp. 74-80, 2019.