IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Certificate Validation Using Blockchain

Miss. Anjana R. Godase
Department of Computer Science
SKNSCOE Pandharpur
PAHSU University
Maharashtra, India

Miss. Prashila P. Mali
Department of Computer Science
SKNSCOE Pandharpur
PAHSU University
Maharashtra, India

Miss. Pratiksha N. Danake
Department of Computer Science
SKNSCOE Pandharpur
PAHSU University
Maharashtra, India

Miss. Vishakha V. Pawar
Department of Computer Science
SKNSCOE Pandharpur
PAHSU University
Maharashtra, India

Prof. N. M. Sawant
Department of Computer Science
SKNSCOE Pandharpur
PAHSU University
Maharashtra, India

***Abstract*—**In the digital world, everything is digitalized in which the certificates of SSLC, HSC, and academic certificates are digitalized in educational institutions and provided to students. Students are facing difficulties in maintaining their degree certificates. For the organization and institution, verification and validation of certificates are tedious and cumbersome. Our project will help to store the certificate in the blockchain system and provide security. First, the paper certificates are converted into digital certificates. The chaotic algorithm is used to generate the hash code value for the certificate. Then the certificates are stored in the blockchain. These certificates are validated by using the web application. Blockchain technology can provide a more secure and efficient digital certificate validation.

Keywords—blockchain, digital certificate, hashing, a chaotic algorithm

I. INTRODUCTION (*HEADING 1*)

All certificates and transcripts hold information that is easily tampered with illegally by individuals and should not be easily accessible to outside entities. Hence, there is a high need for an efficient mechanism, that can guarantee the information in such certificates is original, which means the document has originated from a reliable and authorized source and is not forged.

Various systems have been designed to secure e-certificates for education institutions and to store them securely in cloud-based systems. Blockchain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also helps in eliminating the need for constant verification of certificates.

II. NEED FOR CERTIFICATE VALIDATION

Certificates are used to verify the authenticity of parties involved in a communication or transaction. Certificate validation is a critical process used in the realm of cybersecurity and secure communication. Certification validation is a fundamental component of ensuring the security and trustworthiness of digital communication and transactions. It plays a crucial role in establishing trust, protecting data, and mitigating various cybersecurity risks. Whether you're browsing the web, sending encrypted emails, or using secure applications, certificate validation helps ensure that you can do so with confidence in the authenticity and security of yourinteractions.

Here are some key reasons why certificate validation is crucial:

- Authentication
- Security
- Data Integrity
- Confidentiality
- Trust Establishment
- Protection Against Man-in-the-Middle Attacks
- Compliance and Security Standards.

III. WHAT IS CERTIFICATE VALIDATION

Certificate validation is the process of verifying the authenticity and legitimacy of the certificate.

IV. NEED OF BLOCKCHAIN

Traditional systems for managing information and transactions often have limitations. Blockchain technology offers a solution by creating a more secure, transparent, and efficient way to track and verify data.

A. Decentralized trust

Unlike traditional systems reliant on central authorities, blockchain utilizes a distributed ledger shared across a network of computers. This shared record fosters trust as everyone has a copy, making it tamper-proof and transparent.

B. Cryptographic Security

Blockchain employs cryptography to safeguard transactions. Each block is linked to the one before it, forming an auditable trail. Any attempt to alter a record would necessitate changing every subsequent block, which is nearly impossible on a secure blockchain network.

C. Potential Cost Reduction

By removing intermediaries, blockchain can streamline processes and reduce verification and record-keeping costs.

D. Increased Efficiency

Transactions on a blockchain can be faster compared to traditional systems as they bypass central authority approvals.

blockchain is a continuously evolving technology with challenges like scalability and energy consumption to address, its potential to revolutionise information management and transaction conduct is undeniable.

LITERATURE REVIEW

1. "Blockchain-Based Certificate Transparency and Revocation Transparency," authored by Wang Z., Lin J., Cai Q., Wang Q., Jing J., and Zha D., published in 2019 in the Financial Cryptography and Data Security conference proceedings by Springer, explores the integration of blockchain technology into certificate transparency and revocation transparency mechanisms. The purpose of this paper is to enhance the security and transparency of digital certificates by leveraging blockchain's immutable ledger properties. By employing blockchain, the paper aims to provide a decentralized and tamper-proof system for verifying the authenticity and revocation status of certificates, thereby mitigating risks associated with certificate fraud and misuse. The research utilises cryptographic algorithms to ensure data integrity and security within the blockchain network, contributing to more reliable certificate management practices.

2. Aisong Zhang and Xinxin Ma authored the research paper titled "Decentralized Digital Certificate Revocation System Based on Blockchain," published in the Journal of Physics: Conference Series, Volume 1069, presented at the 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) held from June 22–24, 2018, in Suzhou. The purpose of this research paper is to propose a decentralized system for digital certificate revocation utilizing blockchain technology. By employing blockchain, the system aims to enhance the security and efficiency of certificate revocation processes. The authors likely explored various consensus algorithms and cryptographic techniques to design a reliable and tamper-resistant system. The results of the research are expected to demonstrate the feasibility and effectiveness of using blockchain for digital certificate revocation, potentially leading to improved trust and reliability in digital transactions and communications.

3. "Certificate Validation through Public Ledgers and Blockchains" was authored by Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi, published in the Proceedings of the First Italian Conference on Cybersecurity. The purpose of this paper is to explore the utilization of public ledgers and blockchains for certificate validation, aiming to enhance security and trust in digital transactions. By leveraging blockchain technology, the authors propose a system capable of securely verifying the authenticity of certificates without relying on centralized authorities. The result of this research is the development of a decentralized certificate validation mechanism, ensuring tamper-proof and transparent verification processes. The algorithm employed in this study likely involves cryptographic techniques such as hashing and digital signatures to ensure the integrity and authenticity of certificates stored on the blockchain.

4. "Certificate Verification System using Blockchain" was authored by Nitin Kumavat, Swapnil Mengade, Dishant Desai, and Jesal Varolia from the Computer Engineering Department of Mumbai University. The purpose of the paper is to propose a system leveraging blockchain technology for verifying certificates, aiming to enhance security, transparency, and efficiency in the verification process. The system utilizes blockchain's decentralized and immutable nature to store certificate data securely, preventing tampering and unauthorized modifications. Through the implementation of algorithms like cryptographic hashing and possibly consensus mechanisms such as Proof of Work or Proof of Stake, the system ensures the integrity and authenticity of certificates, enabling reliable verification by stakeholders such as employers, educational institutions, and other relevant parties.

5. "Blockchain and Smart Contract for Digital Document Verification" was authored by S. Sunitha Kumari and D. Saveetha from the Department of Information Technology at SRM Institute of Science and Technology. The purpose of this paper is to explore the utilization of blockchain technology and smart contracts for digital document verification, aiming to enhance security, transparency, and efficiency in the verification process. The study investigates how blockchain and smart contracts can streamline document verification procedures by providing immutable records and automated verification protocols. The paper likely employs various blockchain algorithms such as proof of work (PoW) or proof of stake (PoS) to ensure the integrity and consensus of the decentralized network. The expected result is an improved, tamper-resistant system for verifying digital documents, reducing fraud and errors while enhancing trust and reliability in verification processes.

PROBLEM DEFINITION

The traditional methods of certificate validation and verification suffer from issues related to document forgery, centralized authority vulnerabilities, and inefficiencies. To address these challenges, there is a pressing need for a

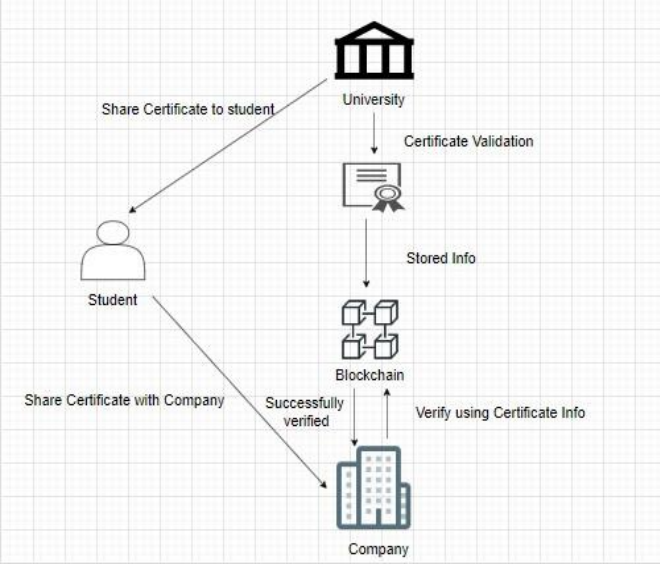
secure, decentralized, and tamper-proof certificate validation system that leverages blockchain technology. This system should provide a reliable means of verifying the authenticity and validity of certificates across various industries and institutions, ensuring trust, transparency, and ease of verification for all stakeholders involved.

In this certificate validation using blockchain, we involve the validation and resolution of challenges associated with leveraging blockchain technology to enhance the validation process of certificates.

Ensuring that certificates stored on the blockchain are authentic and issued by legitimate authorities, thereby maintaining trust in the validation process.

Designs user-friendly interfaces and workflows for certificate validation on blockchain platforms, minimizing complexity and enhancing accessibility for stakeholders.

METHODOLOGY



The process begins with the issuance of certificates by legitimate authorities or certification bodies. Each certificate is associated with a unique digital identifier and relevant information about the credential holder.

1. Certificate Issuance by Institutions: Institutions responsible for issuing certificates digitally encode the credentials along with relevant information about the certificate holder. Each certificate is assigned a unique digital identifier.

2. Blockchain Integration by Institute: The institute integrates blockchain technology into its certificate issuance process. Certificate data, including the unique identifier and credential details, is securely recorded on a blockchain network.

3. Institute and Company Registration: Companies and institutes register on the blockchain platform to access certificate verification services. Their identities are verified, and they are granted access to the blockchain platform's validation functionalities.

4. Certificate Verification by Employers: When an employer needs to verify a candidate's credentials, they access the blockchain platform. They retrieve the certificate data from the blockchain by searching for the unique identifier associated with the candidate's credential.

5. The blockchain-based certificate validation system: Is designed to be scalable to accommodate a large volume of certificates. Interoperability with existing systems and standards ensures seamless integration with the employer's verification processes.

By implementing this methodology, institutions can streamline the certificate validation process, ensuring authenticity and enhancing trust between certificate holders and employers.

RESULTS

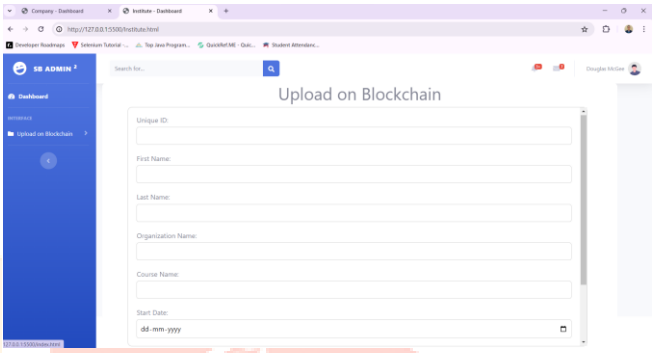


Fig. Data uploading to blockchain

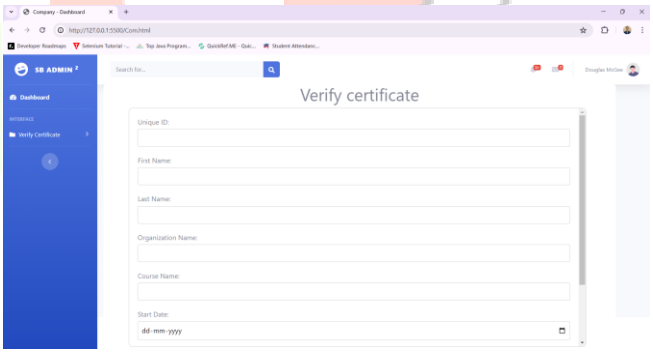


Fig. verify certificate

ACKNOWLEDGEMENT

We would like to express our deep sense of gratitude to our guide Prof. N. M. Sawant for their invaluable help and guidance for the duration of the project. We are highly indebted to Prof. S. V. Pingale, HOD for constantly encouraging us by giving critics on our work. We express gratitude towards Prof. R. S. Yewale, Project Coordinator for providing the support and giving his valuable time, indispensable support and his priceless suggestions.

We also express gratitude towards our all teaching and non-teaching staff, family members and our Friends for encouraging us with their valuable suggestions and motivating us from time to time.

REFERENCES

[1] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[2] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[4] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, "Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.

[5] S.Sunitha Kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology

[6] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Con tract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[7] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, Univer sity Utara Malaysia, Kedah, Malaysia.

[9] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/ 10.1109/ATC.2018.8587428.

[10] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Tech□nology" International Journal of Recent Technology and Engineering (IJRT