https://doi.org/10.46335/IJIES.2024.9.6.12 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 49-54

International Journal of Innovations in Engineering and Science, www.ijies.net

Online Blockchain Based Certificate Generation And Verification System

Pravthi Bawankule[1], Priyanka Sarode[2], Pratham Mahajan[3], Dr. Kapil Gupta[4]

[4]Assistant Professor, [1,2,3,] Students Department of Computer Engineering
St. Vincent Pallotti College of Engineering and Technology ,Nagpur, Maharashtra, India

kgupta@stvincentngp.edu.in

***Received on**: 5 May,2024* ***Revised on**: 29 June,2024* ***Published on**: 01 July ,2024*

Abstract- *In today's digital age, the rise of fake certificates presents a major obstacle for educational institutions and employers alike. As we move towards a paperless certification system, the importance of secure and tamper-proof verification methods cannot be overstated. This study proposes the development of an Online Blockchain-Based Certificate Generation and Verification System to tackle this challenge head-on. By harnessing the decentralized and immutable characteristics of blockchain technology, the system aims to establish a secure and transparent platform for both generating and validating certificates. Through the use of smart contracts, our system automates the issuance and verification processes, eliminating the need for reliance on centralized authorities and significantly reducing the risk of fraud. The system consists of two primary components: Certificate Generation and Certificate Verification. The Certificate Generation module is responsible for creating and issuing certificates, while the Certificate Verification module empowers users to verify certificates by either uploading a certificate PDF or entering a certificate ID. Key features of our proposed system include the integration of Solidity smart contracts for managing and storing certificate details on the Ethereum blockchain, seamless integration with IPFS for decentralized and secure file storage of certificate PDFs, and authentication via Firebase. This research endeavors to streamline the certificate generation and validation process, all while upholding the integrity and authenticity of certificates through the inherent security measures of blockchain technology. Our proposed system serves as a robust solution to combat fraudulent activities and instill trust in digital certification processes, paving the way for a more reliable and efficient certification ecosystem.*

I –INTRODUCTION

In today's digital world, fake certificates are causing big problems for people, companies, and society. These fake certificates look real, but they're not. They can be used to cheat and trick others into thinking someone has qualifications they don't really have. This hurts everyone involved and damages the reputation of schools and businesses.

Even though we're moving more towards digital ways of doing things, many certificates are still on paper. This makes it easy for people to make fake ones or change real ones. Plus, it's slow and hard to check if a paper certificate is real or fake. Schools and businesses really need a better way to manage certificates. They need a system that can handle lots of certificates, make sure they're all real, and do it quickly. That's where block chain comes in.

The project offers a block chain-based solution for the creation and verification of digital certificates. Credentials (UID, CANDIDATE_NAME,

https://doi.org/10.46335/IJIES.2024.9.6.12 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 49-54

International Journal of Innovations in Engineering and Science, www.ijies.net

COURSE_NAME, ORG_NAME, IPFS_HASH) are stored in the blockchain. First, create a certificate pdf using the Pinata service and save it in IPFS. The resulting IPFS hash is then stored on the blockchain along with other data. Blockchain is like a super-secure digital record book. It keeps track of things in a way that can't be changed or messed with. This makes it perfect for managing certificates because it means we can trust that they're real.

This research is all about creating a new system for managing certificates using blockchain. We want to make it easy for schools and businesses to issue, store, and check certificates. By using blockchain, we can make sure that certificates are secure, transparent, and trustworthy. The goals of this project are to make a system that's easy to use, keeps certificate data safe, lets people check certificates quickly, follows all the rules about keeping data safe, and stops fraud and cheating.

II -LITERATURE SURVEY

The paper addresses the issue of document verification complexity and forgery of graduation certificates. It proposes a digital certificate system based on blockchain technology to combat certificate counterfeiting. The system utilizes blockchain's immutable nature to ensure anti-counterfeit measures and verifiability. The process involves generating an electronic file of the certificate, calculating its hash value, and storing it in the blockchain. The paper highlights security themes required for document verification and identifies gaps in existing blockchain-based certificate verification systems. Blockchain-based digital certificates enhance security and verifiability, addressing the challenges of document forgery. The paper emphasizes the importance of incorporating blockchain technology to prevent fraudulent activities related to certificate authentication [1].

The paper discusses the prevalence of certificate forgery due to the lack of effective anti-forgery mechanisms. It proposes a digital certificate validation system based on blockchain technology. The system monitors not only degree certification but also the individual's entire personality and behavioral

activities using a unique-based monitoring process. Keywords include blockchain, hyperledger, digital certificate, and hashing. The paper highlights the need for blockchain-based certificate validation systems to prevent certificate forgery. It emphasizes the comprehensive monitoring of individuals' activities to enhance the credibility of certificates[2].

This overview provides insights into the fundamentals of blockchain technology and its potential applications. It discusses the decentralized and immutable nature of blockchain, highlighting its role in recording transactions securely. While not directly related to certificate management, this paper offers valuable background information on blockchain, which is integral to understanding the proposed systems.[3]

Various blockchain platforms and protocols, including Ethereum and Hyperledger, have been utilized to create secure credentials. These platforms offer transparency, immutability, and strong security features, making them suitable for certificate management systems.

The reviewed literature highlights the growing interest in leveraging blockchain technology to address the challenges of certificate management. While existing research provides valuable insights and solutions, further exploration is needed to enhance the security, scalability, and usability of blockchain-based certificate verification systems. Collaborative efforts between academia, industry, and government are essential to develop robust solutions that ensure the integrity and authenticity of digital certificates in today's digital age.

III- OBJECTIVE

The primary objective of this project is to develop and implement a blockchain-based certificate generation and verification system with the following goals:

Create a User-Friendly Interface: Design and develop an intuitive and user-friendly interface for issuing and storing certificates securely on the blockchain. The interface should be accessible to all stakeholders, including certificate issuers, recipients, and verifiers, ensuring ease of use and seamless navigation[4].

Implement Strong Smart Contracts and Encryption: Utilize robust smart contracts and encryption techniques to safeguard the integrity and confidentiality of certificate data stored on the blockchain. By leveraging cryptographic algorithms and decentralized confirmation mechanisms, the system aims to prevent tampering and unauthorized access to certificate information.

https://doi.org/10.46335/IJIES.2024.9.6.12 e-ISSN: 2456-3463
Vol. 9, No. 6, 2024, PP. 49-54

Establish Accessible Verification Process: Establish a transparent and accessible verification process for real-time validation of certificates. Certificate verifiers should be able to verify the accuracy and authenticity of certificate data efficiently, either by uploading the certificate file or entering the unique identifier associated with the certificate.

Ensure Compliance with Data Protection Laws: Ensure compliance with relevant data protection laws and industry standards governing the handling and storage of sensitive information. By adhering to regulatory requirements, the system will maintain the privacy and security of certificate data while upholding the trust and confidence of stakeholders.

Conduct Audits for Vulnerability Prevention: Conduct regular audits and security assessments to identify and address vulnerabilities and potential threats to the certificate management system. By proactively monitoring and mitigating risks, the system aims to prevent fraudulent activities and maintain the integrity of certificate issuance and verification processes.

IV-PROPOSED METHODOLOGY

This system introduces an innovative approach to certificate management, utilizing blockchain technology to ensure the security and integrity of digital certificates. Within this framework, the system operates through two main components: Certificate Generation and Certificate Verification.

In the Certificate Generation process, institutes or authorities are empowered to generate and issue certificates securely. This process begins with the creation of the certificate itself, which involves compiling essential information such as the candidate's details, course name, and organization name. Once the certificate data is prepared, it is converted into a PDF format using the Pinata service. Pinata facilitates the secure storage of the certificate PDF on the Interplanetary File System (IPFS), a decentralized and immutable storage network. The resulting IPFS hash, representing the unique identifier of the certificate, is then stored on the blockchain along with other pertinent data. This ensures that the certificate's authenticity and integrity are preserved through cryptographic means and distributed ledger technology[5].

On the other hand, the Certificate Verification process enables stakeholders to validate the authenticity of certificates efficiently. Verifiers, such as employers or educational institutions, have two options for verifying certificates within the system. They can either upload the certificate PDF directly for verification or input the certificate ID provided by the candidate. In both cases, the system retrieves the corresponding certificate information from the blockchain, cross-referencing it with the original data to verify authenticity in real-time. This streamlined verification process enhances trust and transparency, mitigating the risks associated with fraudulent activities and ensuring the credibility of digital certificates.

Overall, the proposed approach harnesses the power of blockchain technology to create a transparent, secure, and efficient system for managing digital certificates. By integrating cryptographic algorithms, decentralized storage, and smart contract functionality, the system offers a reliable platform for issuing, storing, and verifying certificates across diverse domains. This innovative approach not only enhances the credibility of the certification process but also fosters trust among stakeholders, reinforcing the integrity of digital credentials.

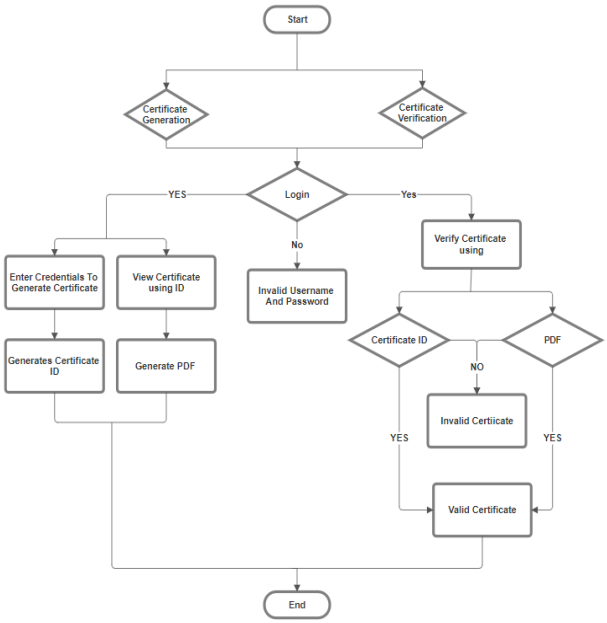

Fig 1.1 System Flow Diagram

V - RELATED WORK

This system introduces a ground-breaking method for managing certificates, utilizing the power of blockchain technology to guarantee the integrity and security of

https://doi.org/10.46335/IJIES.2024.9.6.12 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 49-54

International Journal of Innovations in Engineering and Science, www.ijies.net

digital certificates. By leveraging blockchain, the system establishes a transparent and immutable platform for creating, storing, and verifying certificates, effectively reducing the potential for fraudulent authentication and document tampering. This adoption of blockchain not only boosts the reliability of certificates but also simplifies the verification process, making operations more efficient for institutions and organizations alike[6].

The user interface stands as the central hub for user interaction within the system. When users access the platform, they are greeted with an intuitive interface that clearly distinguishes between two key roles: Certificate Generation and Certificate Verification. These roles are presented with descriptive features and functionalities, ensuring that users can navigate to their desired tasks seamlessly. The interface design is crafted to prioritize intuitive navigation and accessibility across different devices, aiming to elevate the overall user experience.

Certificate Generation Module:

The certificate generation process begins with institutes or certificate authorities accessing the system. Users are then prompted to input essential details such as candidate name, organization name, course name, and unique identification numbers required for certificate creation. Leveraging predefined templates and formats, the system dynamically generates a certificate in PDF format based on the provided information. To ensure the integrity and security of the generated certificate, cryptographic hashing algorithms are employed to create a unique fingerprint of the certificate content. Subsequently, the certificate PDF is securely stored on IPFS using Pinata, a trusted service for decentralized file storage, ensuring tamper-proof and immutable storage. Additionally, pertinent certificate data, including the IPFS hash, is recorded on the blockchain, establishing a permanent and transparent record of certificate issuance.

Certificate Verification Module:

Similar to the certificate generation process, users accessing the certificate verification module are presented with a straightforward interface. The module offers multiple verification options to accommodate different user preferences and scenarios.

Users have the option to verify certificates either by uploading a PDF document or by inputting the certificate ID[7].

Verify Certificate using PDF

The system's certificate verification module conducts thorough validation checks to ensure the authenticity and integrity of certificates. Users have the option to verify certificates by uploading a PDF document. During this process, the system meticulously analyzes the uploaded document, extracting crucial details such as candidate name, organization name, course particulars, and unique identification numbers. It then cross-references this extracted information with the corresponding data stored on the blockchain. If the extracted details precisely match the blockchain records, the certificate is considered valid, and the verification process is successfully completed. However, if any disparities or irregularities arise between the uploaded PDF and the blockchain data, the system promptly identifies the certificate as tampered or invalid, prompting users to exercise caution.

Verify Certificate using Certificate ID

Users can also opt to verify certificates by inputting the certificate ID. In this process, the system meticulously validates the accuracy and completeness of the provided ID. It conducts stringent checks to ensure that the length of the inputted ID matches the expected length and that the ID corresponds to records stored on the blockchain. If the provided ID meets these criteria and matches the blockchain data, the certificate is verified as authentic, and the verification process is successfully completed. However, if the inputted ID deviates from the expected length or if it fails to match any records on the blockchain, the system rejects the verification attempt, signaling that the certificate ID is either invalid or incomplete. By implementing these proactive verification measures, the system ensures that only genuine and unaltered certificates are considered valid, thereby upholding the integrity and reliability of the certification process.

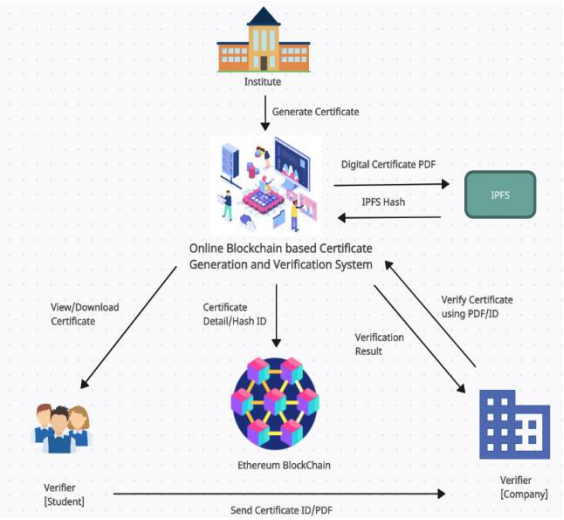

Fig 1.2 Online Blockchain Based Certificate Generation and Verification System Overview

https://doi.org/10.46335/IJIES.2024.9.6.12 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 49-54

International Journal of Innovations in Engineering and Science, www.ijies.net

VI -TECHNOLOGIES USED

1. Blockchain Technology:

Blockchain serves as the cornerstone technology of the system, providing a decentralized and immutable ledger for storing certificate data securely. Specifically, the system leverages the Ethereum blockchain for its robustness and support for smart contracts. Ethereum's smart contract functionality enables the execution of automated certificate issuance and verification processes, enhancing efficiency and transparency[8].

2. IPFS (Interplanetary File System):

The Interplanetary File System (IPFS) is employed for decentralized storage of certificate PDF files. By utilizing IPFS, the system enhances data integrity and availability through distributed file storage. This decentralized approach ensures that certificate documents are resilient to single points of failure and remain accessible even in the event of network disruptions.

3. Firebase Authentication:

Firebase Authentication is integrated into the system for user authentication and authorization. This technology provides secure login mechanisms using email/password authentication, ensuring that only authorized users can access the certificate generation and verification functionalities. Firebase Authentication offers robust security features, including multi-factor authentication and OAuth-based authentication options.

4. Pinata:

Pinata serves as the storage solution for uploading certificate PDFs to IPFS. It facilitates fast and secure uploads while ensuring data integrity through cryptographic hashing. Pinata's platform offers seamless integration with IPFS, enabling efficient storage and retrieval of certificate documents. Additionally, Pinata provides APIs and SDKs for easy integration into the system's backend infrastructure.

5. Truffle Suite:

The Truffle Suite is employed for smart contract development, testing, and deployment on the Ethereum blockchain. This comprehensive suite of tools includes Truffle for smart contract compilation and deployment, Ganache for local blockchain testing, and Drizzle for frontend integration. Truffle's development environment streamlines the smart contract development lifecycle, enabling developers to write, test, and deploy smart contracts with ease.

6. Node.js:

Node.js is employed for backend development and server-side logic implementation. As a lightweight and efficient JavaScript runtime environment, Node.js enables developers to build scalable and performant server-side applications. Node.js's event-driven architecture and non-blocking I/O model make it well-suited for handling concurrent requests and managing backend services in real time.

7. Python:

Python is used for scripting and backend logic implementation within the system. Renowned for its simplicity and versatility, Python provides a wide range of libraries and frameworks for building robust backend services. With its clean syntax and extensive ecosystem, Python enables developers to implement complex business logic and data processing tasks efficiently.

VII. CONCLUSION

The Online Blockchain Based Certificate Generation Validation System offers a transformative solution to the challenges associated with traditional certificate management processes. By harnessing the power of blockchain technology, the system ensures the integrity, transparency, and security of digital certificates, thereby enhancing trust and reliability in certification processes.

Through the utilization of Ethereum blockchain, IPFS, Firebase Authentication, Pinata, Truffle Suite, Node.js, and Python, the system provides a robust and scalable platform for generating, storing, and verifying certificates. These technologies collectively contribute to the seamless operation of the system, facilitating efficient certificate management workflows and enhancing user experience[9].

Furthermore, the user-friendly interface of the system simplifies certificate generation and verification processes, enabling users to interact with the platform intuitively. By integrating stringent validation checks and verification protocols, the system ensures that only authentic and unaltered certificates are deemed valid, thereby safeguarding the integrity of the certification process[10].

Overall, the adoption of blockchain technology in certificate management holds immense potential to revolutionize the way certificates are issued, stored, and verified. By embracing innovation and leveraging cutting-edge technologies, the Online Blockchain Based Certificate Generation Validation System paves the way for a more transparent, secure, and efficient certification ecosystem, benefiting institutions, organizations, and individuals.

https://doi.org/10.46335/IJIES.2024.9.6.12 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 49-54

REFERENCES

[1] *Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.*

[2] *Chen, G. (n.d.). Development and Application of Smart Contracts.*

[3] *Hargude, R. N. (2021). Verification and Validation of Certificate Using Blockhchain.*

[4] *Jiin-Chiou, N.-Y. L.-H. (2018). Blockchain and Smart Contract for Digital Certificate.*

[5] *Maharshi Shah, P. K. (2019). Tamper Proof Birth Certificate Using Blockchain Technology.*

[6] *Mougayar, W. (2016). The Business Blockchain:Promise,Pratice, and Application of the Next Internet Technology. Wiley.*

[7] *Priya, S. &. (n.d.). Online Certificate Validation Using Blockchain.*

[8] *Ravi, S. L. (2021). Certificate Verification using Blockchain and Generation of Transcript.*

[9] *Saleh, O. S. (2020). Blockchain based framework for educational certificates verification . Iraq.*

[10] Zibin Zheng, S. X.-N. (2017). *An Overview of Blockchain Technology:Architecture,Consensus,and future Trends.*