



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Issuing and Verifying Digital Certificate with Blockchain

Rushabh Ahire, Samarth Pawar, Harshal Salunke, Aditya Jadhav, Mrs Priti Balu Kudal

Student of Third Year, Department of Computer Engineering, Guru Gobind Singh Polytechnic

Maharashtra, India

Student of Third Year, Department of Computer Engineering, Guru Gobind Singh Polytechnic

Maharashtra, India

Student of Third Year, Department of Computer Engineering, Guru Gobind Singh Polytechnic

Maharashtra, India

Student of Third Year, Department of Computer Engineering, Guru Gobind Singh Polytechnic

Maharashtra, India

Sr. Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic

Maharashtra, India

ABSTRACT: Today The creation of fake certificates becomes easier. Tracking these certificates and validating their authenticity manually becomes a tedious job. To make the data more secure and safe, everything needs to be digitalized with the principle of Confidentiality, Reliability, and Availability. All of these can be achieved with a technology named Blockchain. Using blockchain technology is proposed to store the genuine certificates in digital form and verify them firmly whenever needed without delay. Makes sure that the certificates, once verified, can be present online.

KEYWORDS: Blockchain, Hyperledger, Digital Certificate, Hashing

I. INTRODUCTION

The “Issuing and Verifying Digital Certificate system is based on Blockchain technology, designed to create a secure and tamper-proof way of issuing and verifying certificates using blockchain technology. The system uses IPFS and Pinata to store the certificates, which are broken into small pieces and distributed across the network, making it difficult for anyone to tamper with or alter the certificate.

The system includes a web-based interface that allows students to request for certificates and institutions to verify their requests and issue certificates securely. Once the certificate is issued, the institution can upload it to IPFS using Pinata, which provides a user-friendly interface for managing and distributing files on the IPFS network.

The certificate is then stored on IPFS and can be accessed by the student using the IPFS hash.

To ensure the authenticity of the certificate, the system sends the certificate details to the student via email, and the student can download the certificate using the IPFS hash. The system also includes a web app for verifying the authenticity of certificates, which allows employers, educational institutions, and other interested parties to verify the certificate using the IPFS hash.

The system stores student requests in Firebase, a cloud-based platform that provides a range of tools and services for developing and managing mobile and web applications. This allows institutions to easily manage and track student requests, as well as access analytics and usage tracking data to monitor and optimize the performance of the system.

Overall, the “Issuing and Verifying Digital Certificate” system is a powerful tool for creating secure and efficient systems for certificate issuance and verification. By using blockchain technology and IPFS, the system provides a tamperproof and distributed way of storing certificates, improving the accuracy and reliability of certificate verification. The system's use of Pinata and Firebase simplifies the development and management of the system, while the web-based interface and email notifications streamline the certificate issuance and verification process for students and institutions. The system has potential applications across a wide range of industries, including education, healthcare, government, and professional certifications, and demonstrates the power and potential of blockchain technology beyond cryptocurrency.

II. PROBLEM STATEMENT

In traditional systems, certificates are typically issued in paper form and can be easily forged or tampered with. This makes it difficult for employers and educational institutions to verify the authenticity of certificates, leading to inefficiencies and potential fraud. By using blockchain technology, certificates can be stored in a tamper-proof and transparent manner, providing a secure and efficient way to issue and verify certificates.

PROJECT SCOPE

This research focuses on the practice currently in place at the learning institutions. The first face of usage of this system will involve degree certificate in learning institutions that issue certificates after completion of the degree course. This will enable to test the usage of the system and also discover flaws that might be encountered in the system. As part of future work, the digitization of the academic certificates this system will be scaled up to other industries like Government institutions, health and Insurance to create verifiable tamper proof documents.

III. GOALS AND OBJECTIVES

- The aim of this study is to develop and implement a Issuing and Verifying digital certificate
- System using Blockchain technology to be used by learning institutions to issue
- Verifiable academic certificates to students this will stop fraud.
- Understanding Blockchain technology and its capabilities.
- Review of the current solutions for the issuing and maintenance of academic certificates.
- Create a digital immutable and easily verifiable way the academic certificates of students who obtain academic qualifications from the University.

IV. LITERATURE SURVEY

A. *The Jiin-Chiou Chen, Narn-Yih Lee, Chien hi, and Yi-Hua Chen “Blockchain and Smart Contract for Digital Certificate”*

[1] In order to solve the problem of certificate forgery, the digital certificate system based on blockchain technology would be proposed. Due to the unmodifiable property of blockchain, the digital certificate with anticounterfeit and verifiability could be made. The procedure given for issuing the digital certificate in this system is as follows. Firstly, the generation of an electronic file of a paper certificate accompanying other related data will be done into the database, also calculation of the electronic file for its hash value will be done. Finally, the hash value will be stored into the block in the chain system. A QRcode and inquiry string code related to the certificate will be generated by the system to affix to the paper certificate. A demand unit will be provided to verify the authenticity of the paper certificate by scanning through mobile phones or by website inquiries.

B. *Padmavati E Gundgurti , Kranthi Alluri , Poornima E Gundgurti , Sai Harika K and Vaishnavi G “Smart and Secure Certificate Validation System through Blockchain”*

[2] In this paper, the problems that arise due to counterfeiting the Certificates and a platform to overcome the mentioned problem are stated. To implement the platform the concept of Blockchain issued. An incontestable advantage of Blockchain is it will make the platform decentralized. The platform is designed to store the Certificates in the block and generate a hash on the request of the student. Once the Certificates are stored in the block they become impossible to fix or to modify by anybody. Putting the information in the block will also remove doubt about the knowledge of the employee. An overview of our platform and its functionalities is presented.

C. *Muniba Memon , Umair Ahmed Bajwa , Asad Ikhlas and Syed Shahbaz Hussain “Blockchain beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications”*

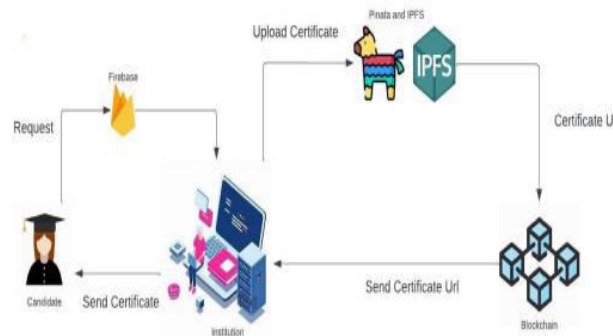
[3] In this paper, in the world of internet of things, social media, and cloud computing, blockchain is the latest addition to the technology. The swift development of blockchain and its respected applications has made it a force to be recognized. But the scope of blockchain is not limited to bitcoin or the cryptocurrencies implementation. This paper enlightens the stipulation of blockchain beyond the bitcoin. Furthermore, this paper reveals the insights of blockchain technology concepts, evolution, mechanisms and challenges based on literature review. This paper identified the complications or challenges in implementation of blockchain technology in real-world applications. Secure implementation of blockchain technology on small scale applications is the key problem that still need to be addressed.

The proposed consensus mechanism would be useful for secure implementation of the blockchain on small-scale application or projects.

D. Santosh Pandey, Gopal ojha, Rohit Kumar and Bikesh Shresha “BlockSIM: A practical simulation tool for optimal network design, stability and planning”

[4] In this paper they have introduced a BlockSIM, which is a comprehensive and open source blockchain system simulation tool. It can assist blockchain architects for better evaluation of the performance of planned private blockchain networks by running scenarios and deciding the optimal system parameters suited for their purposes. They have compared the results of their simulation with real blockchain networks and demonstrated that BlockSIM can be used effectively by architects of blockchain systems to plan and implement scalable, stable and resilient blockchain networks. Also a demonstration via a real life example is provided stating how the architects can apply BlockSIM to plan and design real-world blockchain systems.

V. SYSTEM ARCHITECTURE



VI. FUNCTIONAL & NON-FUNCTIONAL REQUIREMENTS

Functional requirements:

- Allow user registration with necessary details.
- Implement a straightforward identity verification process.
- Automatically generate digital certificates post-verification.
- Utilize smart contracts for automated certificate issuance.
- Enable decentralized control over digital identity.
- Record certificate transactions on the blockchain.
- Design an intuitive interface for real-time certificate verification.
- Allow users to request and verify certificate revocation.

Non-functional requirements:

- Implement robust encryption for data security.
- Design for scalability to accommodate a growing user base.
- Ensure quick responses and optimize data retrieval for performance.
- Adhere to established blockchain standards and provide APIs.
- Design a user-friendly interface with multilingual support.
- Adhere to legal and regulatory standards, regularly updating compliance measures.
- Ensure high availability, implement redundancy, and minimize downtime.
- Prioritize privacy by minimizing unnecessary data storage.
- Generate detailed logs for transactions and restrict access to authorized personnel.
- Design adaptability to changes in blockchain technology, regularly updating for compatibility.

VII. CONCLUSION

In conclusion, blockchain technology provides a secure, transparent, and tamper-proof way to issue and verify certificates. By using blockchain technology, traditional certificate issuing systems can be transformed into decentralized, efficient, and cost-effective systems that are accessible to all parties involved, including employers, educational institutions, and individuals. While there are challenges in implementing blockchain based certificate issuing and verification systems, the benefits they offer in terms of security, transparency, and efficiency make them a promising solution for the future of certificate issuance and verification.

VIII. FUTURE SCOPE

The future scope for issuing and verifying certificates using blockchain technology is significant, as the technology continues to evolve and mature. Here are some of the potential future developments for this technology:

1. **Interoperability:** One of the potential future developments for blockchain-based certificate issuance and verification is interoperability between different blockchain networks. This would enable certificates to be transferred and verified across different blockchain networks, making the process more efficient and streamlined.
2. **Smart Contracts:** Another potential future development is the use of smart contracts to automate the certificate issuance and verification process. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This would eliminate the need for intermediaries and streamline the process even further.
3. **Multi-Factor Authentication:** Blockchain-based certificate issuance and verification could also benefit from the use of multi-factor authentication. This would involve using multiple sources of verification, such as biometric data, to confirm the identity of the certificate holder. This would enhance the security of the process and reduce the risk of fraud.
4. **Integration with Internet of Things (IoT):** Another potential future development is the integration of blockchain-based certificate issuance and verification with the Internet of Things (IoT). This would enable certificates to be verified automatically in real-time, based on data collected from IoT devices.
5. **Standardization:** Standardization of the blockchain-based certificate issuance and verification process could also be a potential future development. This would ensure that all parties involved in the process, such as issuers, verifiers, and certificate holders, follow a common set of standards and protocols, making the process more efficient and reliable.
6. **Adoption in Emerging Markets:** Blockchain-based certificate issuance and verification could also see significant adoption in emerging markets, where traditional methods of verification may be less reliable or efficient. The technology could help to improve access to education, employment, and other opportunities by providing a secure and reliable method for verifying credentials.

REFERENCES

Appendix B:- Bibliography (References from Links, Books)

- [1] Certif-ID : <https://certif-id.com/solutions/certificates/>
- [2] Blockcerts : <https://www.blockcerts.org/>
- [3] Ijraset : <https://www.ijraset.com/research-paper/system-for-academic-certificates-verification-using-blockchain>
- [4] Researchgate: https://www.researchgate.net/figure/Digital-Certificate-verification-process-using-Blockchain_fig4_351356935



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details