International Journal for Multidisciplinary Research (IJFMR)

Blockchain Based Certificate Validation System

Abhishek Bhise¹, Chinmay Pardeshi², Mangesh Vajale³, Pratik Bhongale⁴, Sonali Shirke⁵, Mukul Jagtap⁶

^{1,2,3,4,5,6,7}Keystone School of Engineering, Handewadi Chowk, Pune - 412308

Abstract:

Due to the number of increasing graduates per year, there is an increase in the need for verified and easily accessible certificates. This paper describes a way where both of these conditions can be met without any problem. Blockchain technology is used in this project where validation is the topmost priority. Blockchain is a shared database mechanism which allows transparency across the network. Blockchain contains a group of blocks which are linked together by cryptographic hashes. This mechanism makes the data immutable. The database is decentralized so there is no requirement for central authority to store and manage data. Blockchain fulfils the CIA principle which is confidentiality, integrity, availability and authorization. This also reduces the stress of the student keep track of their certificates in case of losing or damaging the certificates. Creating a Fake Certificate in today's world is a very easy task. To counter this problem, blockchain is one of the most reliable solution available. While storing certificates using blockchain, a unique hash code is generated and with this hash code a new QR (Quick Response) code is also generated which will be linked directly to that specific certificate. By scanning the QR code, a person who wants to verify the certificate will be redirected to a website on which the certificate is displayed making it simple and much faster than regular manual techniques.

Keywords: Blockchain, Confidentiality, Integrity, Availability, Authorization, Quick Response, Hash Code

I. INTRODUCTION

The internet is an important medium for exchanging info among greater platforms. Certification and its validation is also an important part of the internet. The security is a very serious issue of the internet. According to research most of the universities still use the traditional manual certificate issuance system which is based on hard copy which has the risk of getting damaged or lost. Students who graduate from any school, college or university gets a certificate. The certificate itself verifies that the student has been in the institution and completed a specific degree period to achieve this certificate. The problem with a physical certificate is that, it can be lost, damaged or tampered with. Hiring Companies validate the authenticity of the certificate by a third-party system or direct contracts with the institute are and which sometimes can take a very long time and also create a problematic situation. If a proper validation is not conducted, any person who forge a fake certificate can get hired. Fake certificates are forged so that many people who want to get their dream job without having the qualification can get hired. Blockchain can be used in this sector where cheap, trustable and easy verification of important verified documents is required. Blockchain is a decentralized and immutable database that has a high potential which is used to record transactions. Blockchain contains a network of data structure which are called blocks connected



E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

with hash values. A block is validated only once when it has been validated by multiple parties. To modify these blocks the malicious user has to modify all the previous blocks connected to it which requires control over more than 50% of the internet which is practically impossible. For example: - Data is stored on multiple servers and if a hacker modifies data at one of the servers, then its hash code will get changed in one server and other servers will be left unchanged and this changed hash code will be detected at verification time which prevents future attacks on the database. If the stored data is unchanged then the hash code doesn't change which tells that the data has not been tampered with and validates the block.

II. PROBLEM STATEMENT

Certificates issued are designed to be legitimate. Forgery of certificate is a serious issue where students get admission using fake certificates and stay unchecked for years until the students himself tells the situation (Example: - Aryan Anand in Lehigh University 2024). Differentiating between fake and original certificate requires a lot of time and money. Due to such cases, a system is needed to minimize the level of certificate forgery. Many systems were created in this attempt using RDBMS (Relational Database Management System) which can be easily hacked nowadays due to the advancement in technology.

Therefore, this study develops and implements a certificate validation system that adapts to the blockchain technology and Quick Response (QR) code to solve the above problem.

III. OBJECTIVE

- This paper proposes a system that reduces management costs, paper costs and completely removes document forgery from the current validation system
- This system follows the CIA principle (Confidentiality, Integrity and Availability)
- To develop a immutable, encrypted, transparent and trackable database system.
- Combining blockchain technology to increase the efficiency of the overall system

IV. LITERATURE SURVEY

Title: Generating E-Certificate and Validation using Blockchain

Authors: Marco Valdi, Murat Yasin Kubilay (JULY 2021)

Overview: This paper is proposed to address the issues of security of certificate information. This Paper also proposes the solution of the issues of reliability and security of certificate revocation information. It also tells us about the current trust model and how the CA (Certificate Authority) have the absolute responsibility to issue correct certificates for the designated subject. A certificate Authority is a trusted third party that issues digital corticates and verifies them using various methods.

Title: Certificate Generation and Verification System Using Blockchain Technology Using Quick Response Code

Authors: Nihu & Vani, Zheng Et Al (May 2022)

Overview: This paper proposes a system using Blockchain technology which generate data hash that connects the current block with the previous forming a long chain of nodes. They also developed a verification system where any organization, institutions, enterprises or anyone concerned would be able to verify the authenticity of the certificate.

Title: Blockchain-Based Certificate Authentication System with Enabling Correction



Author: Jayesh Dongare, Omar Sale (March 2023)

Overview: This paper was issued to criticize the problem related to the current system of certification. It also solves this issue of certification by proposing a system that not only verifies but also generates new certificates. The proposed project eliminates the current limitations of technology by using Blockchain Technology.

V. PROPOSED SYSTEM

We propose a system where students can enter the details of their certificates. We also allow institutions to enter the details of the od students that were issued certificates for completing a specific degree from the institution. This certificate is converted into digital copies of the original certificate which are verified by the admin or an image processing system. After the certificate has been verified by the admin, it is stored in the blockchain system where the certificate becomes immutable and immune to any modification that can be done by malicious users. After the certificate is stored in the blockchain system, a QR code is generated with a timestamp. If any person who scans the QR code can easily be redirected to the website where the certificate is displayed securely.

VI. SYSTEM ARCHITECTURE



VII. IMPLEMENTATION

To establish a blockchain based certificate validation system a comprehensive analysis of system's requirements is needed. This included the specific types of certificates to be validated as well as the issuers, recipients, validators and the desired security requirements. Following this a suitable platform for blockchain can be selected such as Ethereum.

In the development phase, smart contracts are created for management of the certificate validation process. Smart Contracts includes the structure and rules for the certificates for issuance and validation. A login system will be created where the institutions and students store their credentials with the help of decentralized identifiers and verifiable credentials.



International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 • Website: <u>www.ijfmr.com</u> • Email: editor@ijfmr.com

Certificate are verified and digitally signed by the respective admin where each certificate is assigned a unique identifier. The next step involves the setup of a private blockchain network with node configuration and network security. Admin is granted the permission to access the data and verify it before uploading it into the blockchain network.

User friendly interface is created for validation system with the help of APIs the system becomes robust in operations. Permission access control mechanisms restrict actions based on user roles.

Testing such as unit testing, integration testing and end-to-end testing will be conducted to verify the functionality, security and performance of the system. Upon successful testing, system will be deployed on the blockchain network to check its compatibility with other components.

The final stage involves setting up monitoring tools and maintenance tools for regular updates and checking for any vulnerabilities, making the system robust and efficient for blockchain based certificate validation system

VIII. CONCLUSION

This paper proposes about the generation and verification of certificates using Blockchain Technology. This project is based on blockchain technology and also the addition of QR Code is used to overcome various weaknesses related to the previous systems. In this system, Students as well as institutions can upload certificates in the blockchain system which will be verified by an admin or by an image processing system for automation. After verification, these certificates are stored and no modifications can be made. This feature helps us to create a system in which all the transactions and processes are transparent and immutable. In our project, we added a QR (Quick Response) Code feature which decreases the time required to search for the certificates. The certificate generates a hash code and a timestamp which creates uniqueness and also increases security for certificates.

IX. REFERENCES

- 1. "Blockchain-based Certificate Validation System" by A. K. Singh et al. (2018) This paper proposes a blockchain-based framework for certificate validation, which ensures the authenticity and integrity of certificates.
- 2. "A Secure Certificate Validation System using Blockchain Technology" by S. S. Iyer et al. (2019) -This study discusses the implementation of a blockchain-based certificate validation system, which provides a tamper-proof and transparent way of certificate validation.
- 3. "Blockchain-based Certificate Validation for IoT Devices" by J. Kim et al. (2020) This paper explores the application of blockchain
- 4. "Decentralized Certificate Validation System using Blockchain" by R. Gupta et al. (2021) This paper introduces a decentralized approach to certificate validation by utilizing blockchain technology, which addresses issues of centralization and improves trust in certificate issuance.
- 5. "Leveraging Blockchain for Digital Credentialing" by M. Perez and T. Wang (2022) This research discusses the broader implications of blockchain technology in the realm of digital credentialing, emphasizing its potential for creating secure, verifiable credentials that can be shared across platforms.
- 6. "Evaluation of Blockchain-based Certificate Validation" by L. Chen et al. (2023) This paper reviews various blockchain models for certificate validation, analyzing their performance, security



features, and scalability issues in practical applications.

- 7. "Smart Contracts for Certificate Validation" by K. Leung and D. Patel (2023) This study looks at the use of smart contracts within blockchain systems to automate the certificate validation process, ensuring immediate verification and reduced administrative overhead.
- 8. "A Comparative Study of Blockchain-based Authentication Systems" by F. Ahmed and S. Khan (2023) This paper compares various blockchain-based authentication and certificate validation methodologies, aiming to identify best practices and frameworks for implementation.