IRJCS: International Research Journal of Computer Science
Volume 11, Issue 05, May 2024
ISSN: 2393-9842
https://www.irjcs.com/archives

Create Certificate and Verification System Using Blockchain Technology and Fast Response

Mohammad Sarfarz
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, INDIA
Mohit Raj
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, INDIA
Dr.Vikas Singhal
Head, Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institute),
Greater Noida, INDIA
vikassinghal75@gmail.com

Publication History
Manuscript Reference No: IRJCS/RS/Vol.11/Issue05/MYCS10089
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IRJCS/RS/Vol.11/Issue05/MYCS10089
Received: 02, May 2024 | Revised: 10, May 2024 | Accepted: 18 May 2024 | Published Online: 30, May 2024
http://www.irjcs.com/volumes/Vol11/iss-05/02.MYCS10089.pdf
Article Citation: Mohammad,Mohit,Dr.Vikas(2024). Create Certificate and Verification System Using Blockchain Technology and Fast Response. IRJCS: International Research Journal of Computer Science, Volume 11, Issue 05 of 2024 pages 450-453 **doi:>** https://doi.org/10.26562/irjcs.2024.v1105.02
BibTeX Vikas@2024Create

Abstract: The increase in fake certificates is causing serious problems for people today, especially affecting employment opportunities. Crime has turned into a rapidly growing business, driven by the demand for certification. Law graduates often face problems finding employment due to the number of fake certificates. To solve this problem, many researchers have proposed proof of concept. However, while these systems provide some benefits such as centralized data management, they are vulnerable to theft and hacking. This document introduces a new method to create and verify certificates using blockchain technology and Quick Response (QR) codes. The system is designed using an iterative and incremental model with data flows and the use of events to inform its operation. This application uses Hypertext Preprocessor Pages (PHP) as the frontend and Spring Boot (a Java framework) as the backend. Test results show that the system is not only environmentally safe, but also protects the student's identity from anonymous identification. Fake certificates have become a social problem, especially affecting the employment of law graduates. To solve this problem, researchers have proposed authentication systems, but these systems are often vulnerable to hackers due to centralized servers. This article introduces the creation and authentication of certificates using blockchain technology and QR codes. The system is designed to use discrete and incremental patterns using data flow and events to inform its operation. Choose PHP and Spring Boot for frontend and backend usage respectively. Testing shows that the system is secure and can protect student identities from anonymous verification. The system uses blockchain technology to ensure high security, as the nature of blockchain makes it resistant to tampering and fraud. Each certificate is stored on the blockchain as a block containing all important information such as the certificate holder's name, issuance date and verification date. Security is further strengthened with QR codes, allowing certificates to be easily verified using a smartphone or other QR code scanning device. function. PHP's simplicity and ease of use make it ideal for creating dynamic web pages and performance applications. The combination of these technologies ensures that the system is efficient and effective. Creating proofs and verifications mentioned in this article provides security and solutions to the problem of illegal authentication. Using blockchain technology and QR codes, the system protects graduates and employers from fraud issues such as certificate fraud by providing a reliable way to verify the authenticity of the certificate.

Keywords: Blockchain, Interplanetary File System (IPFS), certificate, generation, proof, QR code

I. INTRODUCTION

The Internet is an important medium for information exchange and provides a broad platform for knowledge transfer. However, despite its widespread use, many users are still hesitant to do business online (Javier, Javier, Oscar, & Manel, 2004). Security issues still exist because the security of many Internet businesses cannot be guaranteed. Research shows that the traditional certification system used by universities around the world is wrong. These systems rely on manual verification processes, which are not useful for organizations with large amounts of data. Schools try to combat cheating and fraud in many ways, but many of the current methods are time- Verifying credentials is an issue of great concern for schools, educational institutions, and employers.

Employers frequently face identity fraud (Musee, 2015), highlighting the need to secure online credentials and credentials less through human influence. Such systems can create and verify certificates by verifying a company's claim to its ownership document (Patrick, Karim, and Kenneth, 2018). But past attempts to solve this problem have failed to match today's fraud methods. It is used in many industries and buildings. Xu et al. (2021) define blockchain as an interactive communication and data management system that eliminates the need for a trusted third party. The decentralized nature of blockchain allows blocks of information to be traded securely, even without trust. It solves the challenges of certificate creation and verification by providing an immutable timeline (Dawi, Jusoh, Stremicks, and Mardani, 2018). Research shows that blockchain technology has great potential for verifying quality certificates. Data protection is now more important than ever due to the recent fast growth of information technology. Whether graduates choose to continue their education or begin looking for employment, they will need a variety of credentials during the interview. But they often find academic certificates and honors missing. Applying for a physical certificate may take a long time because the certificate is issued by another organization person application. For example, requesting an electronic copy saves paper and time. Graduates can easily apply for any certification by providing personal identification information. However, because of this ease of use, phoney degrees, certifications, and licences are becoming more widespread. Schools and businesses are therefore unable to verify the information they get right away [5]. This research created a blockchain-based coupon system in order to address this issue. Various nodes contain various types of data; hence in order to update a certain internal file, multiple nodes must simultaneously request changes. As a result, the system is trustworthy.

II. EXISTING SYSTEM

Current methods of storing and verifying evidence are critical and manual, resulting in evidence delays and poor security. This centralized approach raises concerns about the integrity of information, especially when certificates are distributed to private businesses such as banks. Information in this certificate can easily be changed, deleted or modified without permission, making the certificate vulnerable to hackers and copying. This issue not only affects the integrity of the authentication process, but also the reliability of its own certificates. Additionally, requiring students to present personal identification information at the meeting point demonstrates a lack of secure digital credentials. Relying on manual verification procedures for certificates not only causes delays but also increases the risk of human error. This previous approach is not secure enough to protect credentials from tampering or fraud. Therefore, there is an urgent need to produce evidence and verification safely and efficiently. Blockchain's decentralized nature and cryptographic security features provide a tamper proof and transparent way to store and verify information. By storing credentials on a distributed ledger, blockchain ensures that credentials cannot be changed or deleted without being detected. This provides high security and confidence in the authenticity of the certificate. Besides security benefits, blockchain technology can also be beneficial. Automation of the certificate verification process reduces the time and resources required for manual verification. This ensures that certificate verification is faster and more reliable, benefiting both certificate issuers and recipients. By leveraging the transparency and immutability of blockchain, organizations can demonstrate the integrity of their certification processes and build trust among stakeholders. Revolutionize the way certificates are managed and verified. It brings security, efficiency and transparency into the solution to the inadequacy of the evidence verification process.

III. LITERATURE REVIEW

3.1 Blockchain

The concept of blockchain was originally put out by Satoshi Nakamoto in 2008. Blockchain functions as a transparent, online ledger that facilitates information exchange. Data updates kept in nodes within this system are compressed before being uploaded to other blocks. Different data kinds are separated into distinct blocks so they may be examined directly by an analyst. All nodes share a timestamped blockchain to ensure that input data has not been tampered with. This process is public, transparent and secure. Blockchain 2.0 is centred on the centralization of the whole market, whereas Blockchain 1.0 primarily addressed difficulties with cryptocurrencies and direct payments. Smart contracts transfer assets, create value and offer an alternative to Bitcoin. Its decentralized structure eliminates the need for intermediaries, reduces costs and increases security. Blockchain's transparency ensures that all transactions are visible to participants, thus increasing trust and accountability. Scalability, power consumption and management issues are some of the issues that need to be addressed for widespread use. However, with ongoing research and development, blockchain continues to evolve, providing new solutions to complex problems.

3.2 Ethereum

Several derivative applications are supported by Ethereum, an open, distributed platform that is Turing complete [10]. Ethereum is used in the construction of governmental organisations. Ethereum will function as a worldwide computing system if the Bitcoin blockchain is viewed as a global payment system. Furthermore, Ethereum is an open platform that resembles Google's Android. It offers a framework that enables developers to create applications. These developers work with Ethereum to construct and maintain the infrastructure. The key features of Ethereum are as follows: Immutable: Third parties are unable to alter any data, and the blockchain remains unaffected by server or computer failure. 1) The Virtual Machine for Ethereum (EVM). A programmable blockchain is EVM. In contrast to Bitcoin, which provides a fixed system, the EVM enables programmers to train the EVM to execute programmes using a level language called Solidity [11]. Solidity's smart contract must be completed before it can be translated into a bytecode contract that the EVM can understand. This is done via a compiler known as solc. The Ethereum blockchain receives the assembled instructions after that. This brings the procedure to a close.

3.3 Smart Contracts

Nick Szabo originally presented smart contracts in the early 1990s. He clarified that computers can control transaction circumstances thanks to smart contracts. With the popularity of blockchain, smart contracts are also becoming increasingly popular. The central component of Ethereum, a blockchain platform founded in 2015, is smart contracts. "Digital contracts written in source code and executed by computers, integration of proofs into the blockchain" is what smart contracts are defined as [6]. Smart contracts can be created using the Ethereum blockchain. Developers can add arbitrary instructions to smart contracts according to their needs to build various applications, including interactions with other contracts; Additionally, smart contracts placed on the blockchain are copied everywhere to prevent the contracts from being tampered with. By running computers and related services over Ethereum, human error can be minimized and conflicts between these contracts can be avoided. Applications for cryptocurrencies and voting [7] both make use of smart contracts. An illustration of how developers may quickly implement smart contracts for bitcoin trading is provided in Figure 3. Solidity, Serpent, and LLL are the primary high languages utilised in the creation of smart contracts [12]. At the moment, the majority of developers encode instructions into bytecode and create smart contracts for EVM execution using Solidity. When developers create smart contracts, they are paid in some way.

Figure 1. Purpose of smart contract

IV. MODULES

4.1 User Interface

The user interface used in this project includes NetBeans and Android Studio. Developed an integration environment (IDE) using NetBeans for server communication. To construct an Ethereum client for Android that is suitable for testing and development, utilise Android Studio. It increases the efficiency of Ethereum app development by utilisingEthereum's to replicate precise user behaviour. Additionally, Testrup has all of the normal protocol call (RPC) capabilities and operations, including events, and may carry out extra activities to make development easier. 10 characters plus two transcripts, university certificates, government certificates, etc. Install multiple certificates such as These certificates will be verified by the relevant authorities before being uploaded. For example, if you upload a school certificate, the system checks the certificate number against the school's server to ensure its authenticity. Approved credentials are stored on the server, unconfirmed credentials are discarded. In this system, each certificate number is considered as a block. To ensure security, a hash code is created for each block. Users can choose to increase the number of QR codes according to their needs. One of the main advantages of this model is that users can share QR codes with others when necessary. when the user's cellphone number receives an OTP for verification. The user can examine his certificate upon successful authentication. Should the third party attempt to scan the QR code more than once, the authorised user will get the third party's location through an authorised link. Authorized users can choose to allow or deny access to others using this link.

V. LITERATURE SURVEY

This technology was chosen for its integrity, encryption, traceability, and data synchronization capabilities. The system increases efficiency at every level by using blockchain resources. It reduces paper usage, reduces administrative costs, prevents data corruption, and provides accurate and reliable digital evidence. A new Public Key Infrastructure (PKI) paradigm that uses blockchain-based authentication "The existing trust model depends on certification authorities (CAs) to provide people legitimate credentials. However, CAs can be compromised, resulting in the issuance of fake but valid certificates .bad security or disregard for the Certificate of Operations (CPS) and Privacy Policy (CP), EmanueleFrontoni, Luca Spalazzi (2017) "Certificate Authentication through Public Ledgers and Blockchain" This project aims to solve the trust and security problems of certificates from the first file. removed. It eliminates any malfunctions and is easy to use using existing open platforms. This project involves creating and implementing a system that transfers hashes of local data to the blockchain. However, it faces many problems and effective application methods that will protect its originality and reputation have not yet emerged. As stated under Revocation and Certificate Transparency.

The global certificate blockchain, which is solely appendable, houses the information that the project controls regarding certificates and revocations. Achieving limited granularity removal transparency and certificate transparency is its aim. The certificate management system often faces issues such as lack of transparency, vulnerability to fraud, and inefficiency. Blockchain provides decentralization, security and transparency to these issues. Each certificate is stored in a block that links to the previous block, forming a chain. This blockchain ensures that once a certificate is issued it cannot be changed or tampered with. This immutability of blockchain makes it ideal for storing sensitive information such as credentials. in code. Smart contracts can be used to complete the verification process without the need for human intervention. This not only speeds up the verification process, but also reduces the risk of errors and fraud. Since blockchain is a distributed ledger, each transaction is recorded and verified by multiple sources in the network. This ensures that the information stored on the blockchain is accurate and reliable. Users can verify the authenticity of their credentials simply by scanning the blockchain, eliminating the need for a third-party service. Every block in the blockchain is encrypted, making it nearly impossible for hackers to intercept data. This ensures that credentials stored on the blockchain are protected from unauthorized access. Blockchain can help eliminate fraud, reduce costs, and simplify the authentication management process by providing solutions, security, and transparency.

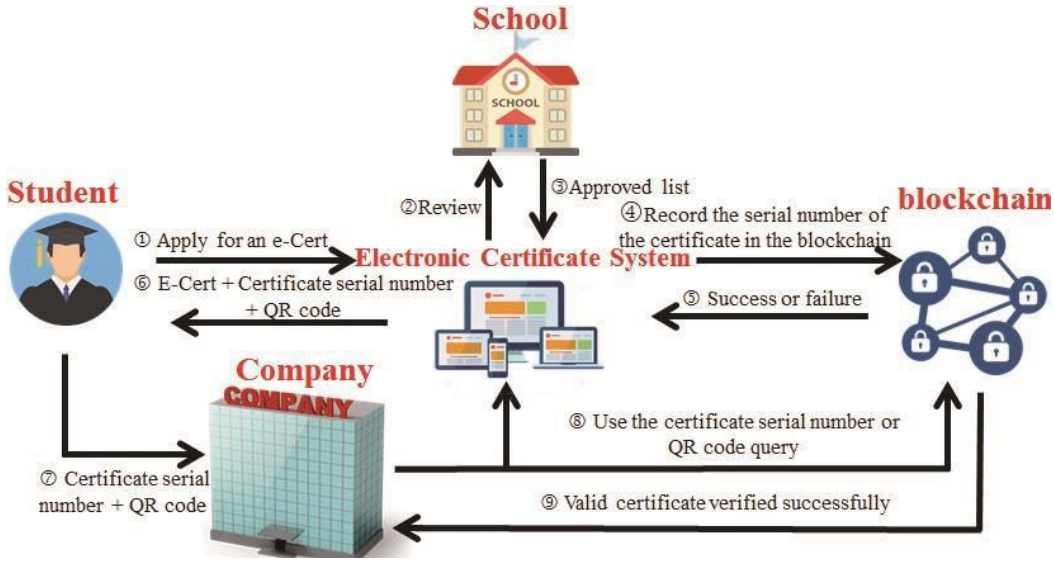
VI. RESEARCH METHODS

6.1 System Design

Authentication system using technology. The application has been specifically designed and implemented on the Ethereum platform using the Ethereum Virtual Machine (EVM). The system appeals to three main user groups: schools or accrediting bodies, students and authorities. Schools or accredited organizations access the system, allowing them to view the information. When students meet the necessary conditions, a certificate is issued by the system. After students receive their certificates, they can check their certificates. The operating procedures of the system established by this organization are detailed as follows: entering data about the students in the system. The student's number is automatically entered into the blockchain by the system. All documents are clearly verified by the certification system. Each graduate will also receive a tracking number and an electronic copy of the certificate. > The company sends the query and if the phone number is verified, the system is immediately informed. Companies can use the QR code to determine whether the certificate has been falsified or tampered with. The use of blockchain technology increases the security and reliability of the certification process and reduces the risk of fraud and fraud. Additionally, the system increases efficiency by digitizing the certificate issuance process and providing a reliable verification process.

6.2 Operation

When users arrive at the registration page, they click "register now," enter their personal data, and then get an email confirming their registration. Units of Certification Following the inputting of a graduate's data, the system creates an electronic certificate with a QR Code and numbers the certificate.



VII. CONCLUSION

This study examines the process of creating certificates and proofs and issuing certification certificates using blockchain technology and rapid response. The goal is to mitigate many of the weaknesses associated with existing systems. This ensures that the process is transparent and cannot be changed. Additionally, the risk of students losing their identity information is reduced. By integrating QR codes, the system further reduces the possibility of data tampering, thus increasing reliability) middle. This binary storage method maintains data integrity and transparency. One of the characteristics of blockchain technology is data security. Blockchain functions as a sizable, publicly available online database that stores and verifies identical data. Using a blockchain-based system lessens the likelihood of authentication. The system's automated certificate issuance and certificate application processes are open and transparent. As a result, a business or organisations may quickly request data from the system. To put it briefly, the system not only guarantees the security and correctness of the data, but it also provides a strong means of safeguarding the certificate's integrity.