International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 3, 2025

Certificate Verification And Validation Using Blockchain

[1] Miryala Rajesh Kumar[2] Dr Kiran B.M[3] Dr Mr. G.Prasad
Sphoorthy Engineering College Hyderabad.

***ABSTRACT**: Everything in the digital world is digital, including academic, HSC, and SSLC certificates that are given to students in educational institutions. It's challenging for students to keep their degree diplomas. Verification and validation of certifications are time-consuming and difficult for the organization and institution. Our initiative will contribute to security and certificate storage in the blockchain system. Initially, digital certificates are created from the paper ones. The hash code value for the certificate is generated using the chaotic algorithm. The certificates are then stored on the blockchain. And the mobile application is used to validate these certificates. We can offer a more secure and effective digital certificate validation by utilizing blockchain technology.*

I. INTRODUCTION

First presented by Satoshi Nakamoto in 2008, blockchain technology is a cutting-edge form of online ledger that makes transparent and decentralized data sharing possible. The idea behind this project is to create an Android application that offers safe certificate verification. Transcripts and graduation certificates nowadays frequently include private information that is easily accessible to unauthorized parties or manipulated with. Therefore, a strong system that guarantees the integrity and authenticity of such documents—confirming that they come from a reliable and approved source and haven't been altered or falsified—is desperately needed.

There are a number of methods in place to protect educational institutions' e-certificates and keep them in cloud-based settings, but there are still many obstacles to overcome. The goal of this project is to use blockchain technology to provide a decentralized, impenetrable system for certificate validity and verification. Because fake or altered papers are so common, confirming the validity of certificates remains a significant challenge in domains such as education, training, compliance, and product certification. Through the utilization of blockchain's fundamental characteristics—security, transparency, and immutability—this project seeks to resolve these problems and create a reliable certificate authentication system. Authorized institutions, certifying bodies, and regulatory agencies will be able to issue digital certificates that are cryptographically signed and kept on a blockchain network thanks to the proposed method. A distinct digital fingerprint, or hash, will be assigned to every certificate, guaranteeing its integrity and allowing for real-time verification by any stakeholder. By entering the certificate ID through a public verification portal or scanning a QR code, people or organizations can confirm the legitimacy of a certificate. The system will obtain and show its original data from the blockchain if the certificate is legitimate.

PROBLEM DEFINITION

Verifying credentials, including degrees, professional training records, compliance clearances, and product certifications, has become a critical problem for businesses all over the world in the digital age. Conventional methods of granting and confirming these credentials are usually laborious, centralized, and vulnerable to fraud, forgeries, and illegal changes. When fake credentials are not discovered, institutions and employers face serious financial and reputational risks. This is because counterfeit certificates can be made and circulated with frightening simplicity using easily accessible design tools.

II. LITERATURE SURVEY

Statistics from Taiwan's Ministry of Education indicate that about a million students graduate annually. Some decide to continue their education at postsecondary institutions or domestic or foreign high schools, while others are ready to start working. While studying, students gather a variety of relevant documents, including diplomas, transcripts, and certificates of success, all of which are vital when applying to schools or jobs. Nowadays, when schools grant diplomas or honors, simply the names of the schools and students are usually noted. Sometimes incidents of fake graduation diplomas are discovered since there is no reliable way to stop forgeries. A digital certificate system built on blockchain technology is suggested as a solution to this problem. It is possible to make digital certificates tamper-resistant and readily verifiable by utilizing the immutability of the blockchain.

The following is the procedure for issuing a digital certificate in this system: The first step is to create an electronic copy of the paper certificate and store it in a database with the relevant data. Next, the system determines the electronic file's hash value. The blockchain has this hash value. Inquiry string and accompanying QR code are created and

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 3, 2025

attached to the paper certificate, enabling prompt authenticity verification.

AUTHORS :

D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay,

ABSTARCT:

certificate validation process within SSL/TLS.

In this paper, we introduce a novel system called CTB that leverages advancements in blockchain technology to address the limitations of the current CA ecosystem. CTB ensures that a CA cannot issue a certificate for a dom Trustworthy public key distribution for web domains, usually handled by X.509 certificates, is essential to the security of web communication via SSL/TLS protocols. The trusted third parties in charge of providing these certificates are known as Certificate Authorities (CAs). Notwithstanding its vital function, the CA ecosystem is essentially delicate and vulnerable to intrusion. Initiatives like Google's Certificate Transparency project and associated studies have responded by promoting public, append-only logs of all certificates issued by CAs in an effort to increase CA accountability. The conventional X.509 protocol is intended to be enhanced by these transparency techniques.

without the domain owner's express approval, removing the possibility of an illegitimate certificate being issued. Another long-standing issue in the ecosystem is addressed by CTB's strong certificate revocation mechanism. We demonstrate a CTB implementation using IBM's Hyperledger Fabric blockchain technology. The smart contract for the system is entirely created in Go and is provided here for reference.

METHODOLOGY

WORKING PROCESS

Blockchain is a distributed, decentralized database. The system created for this study has the following operational workflow:

1. Schools input student data into the system and award degree certificates. The serial number of every learner is then automatically recorded on the blockchain by the system.
2. To guarantee authenticity and accuracy, the certificate system verifies data.

3. Schools award graduates electronic certificates, or e-certificates, that contain a special QR code in place of conventional paper certificates. In addition, graduates get a digital copy of their certificate and an inquiry number.

4. Graduates can show their serial number or an e-certificate with the QR code to potential employers when they seek for jobs.

III. SYSTEM STUDY

3TECHNICAL FEASIBILI

By evaluating the system's technical needs, this analysis determines whether it is technically feasible. It is crucial that the system doesn't overtax the client's current technical resources, as this could result in unnecessary burdens. In order to ensure successful implementation, the system should be built to function effectively with the resources at hand, requiring little to no modifications.

ECONOMICAL FEASIBILITY

By evaluating the system's technical needs, this analysis determines whether it is technically feasible. It is crucial that the system doesn't overtax the client's current technical resources, as this could result in unnecessary burdens. In order to ensure successful implementation, the system should be built to function effectively with the resources at hand, requiring little to no modifications.

.

TECHNICAL FEASIBILI

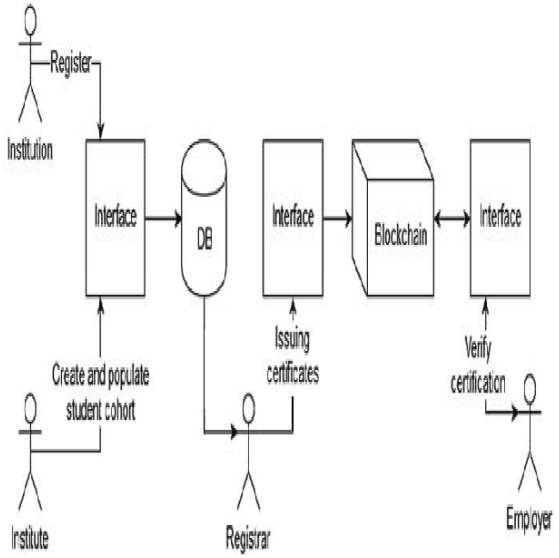
By analyzing the system's technological needs, this study seeks to determine the technical viability. The client may become burdened if the designed system places undue demands on the technical resources already in place. As a result, the system should only necessitate minor or no modifications to the existing infrastructure, guaranteeing that its deployment stays simple and economical.

SOCIAL FEASIBILITY

This study's main goal is to assess users' acceptance of the system. Giving users comprehensive training is an essential step in this procedure to guarantee they can utilize the system effectively. It is crucial that users start to see the system as a useful tool rather than as something to be feared. The methods employed to inform and acquaint users with the system have a significant impact on their acceptance. Gaining their trust is essential since it enables them to provide constructive criticism, which is critical considering that they are the system's main users.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 3, 2025

IV. SYSTEM ARCHITECTURE



V. SOFTWARE REQUIREMENTS:

.Hardware specifications:

• Pentium IV 2.4 GHz system
.
• 40 GB of hard disk space.

The RAM size is 512 Mb.

Software specifications:

• Windows serves as the operating system.
• Python is the coding language.

VI. TESTING

By methodically examining a work product for any potential flaws or weaknesses, testing seeks to identify errors. To assure dependability, it entails evaluating the functionality of individual parts, subassemblies, assemblies, or the whole product. Software is tested to make sure it satisfies user expectations and needs and doesn't malfunction in ways that are unacceptable. There are several test kinds, each intended to meet particular testing requirements.

Types of Testing

UNITTESTING

To ensure that a program's underlying logic operates correctly and that inputs produce the desired results, unit testing entails developing test cases. This procedure guarantees that all internal code pathways and decision branches are extensively evaluated. Unit testing, which is done after a unit is finished but before it is integrated with other program components, concentrates on individual software components. It is an invasive and structural testing method that depends on understanding the specifics of the unit's implementation. Unit tests are intended to perform granular checks on certain parts, business procedures, applications, or system configurations. By doing this, they attest that each distinct business process execution path functions in accordance with specified specifications, with clearly defined inputs and anticipated outcomes.

INTEGRATIONTESTING

To determine if integrated software components function as a single program, integration tests are used. This kind of testing concentrates on the interactions between several modules, highlighting the outcomes displayed in fields or displays as opposed to specific features. Integration tests make sure that the components work together correctly and consistently, while unit tests make sure that each part works as intended when used separately. Integration testing's main objective is to find potential problems that may occur from component interaction, problems that may not be apparent when testing modules separately.

SYSTEMTEST

System testing guarantees that all requirements are met by the integrated software system. It tests a configuration to guarantee results that are known and predictable. Configuration-oriented system integration testing is one type of system testing. The foundation of system testing is process descriptions and flows, with a focus on pre-driven process connections and integration points.

WHITEBOXTESTING

System testing ensures the integrated software system satisfies all requirements. To provide known and predictable results, it checks a configuration. One sort of system testing is configuration-oriented system integration testing.

Process flows and descriptions, with an emphasis on pre-driven process links and integration points, form the basis of system testing.

V. CONCLUSION AND FUTURE WORK

In this research, we proposed a blockchain-based approach to the problem of certificate forging. Data security is essential, and using blockchain technology's immutability improves defenses against unwanted changes and drastically lowers the possibility of falsified certifications. Users can see and validate certificates with our suggested application, guaranteeing information security and correctness. It also makes it easier for users to manage digital certificates.
We intend to concentrate on increasing the system's speed and scalability in subsequent studies in order to gradually improve the user experience.

REFERENCES

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, "Smart Contract and Blockchain for Digital Certificate," IEEE International Conference on Applied System Invention (ICASI), 2018.
[2] Blockchain-Based Certificate and Revocation Transparency, Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019). Financial Cryptography and Data Security, edited by Zohar A. et al. FC. Computer Science Lecture Notes, volume 10958. Heidelberg, Berlin, Springer.
10.1109/ICDMW.2018.00018 D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 71-80.
[4] "Decentralized Digital Certificate Revocation System Based on Blockchain" by Aisong Zhang and Xinxin Ma
The fifth Marco Baldi, Daniele Sciarroni, Giuseppe Gottardi, Emanuele Frontoni, Franco Chiaraluce, and Luca Spalazzi Using Blockchain and Public Ledgers to Validate Certificates The First Italian Conference on Cybersecurity Proceedings.

[6] Nitin Kumavat, Dishant Desai, Swapnil Mengade, and Jesal Varolia, "Certificate Verification System using Blockchain," Department of Computer Engineering, Mumbai University.
[7] S. Sunithakumari and D. Saveetha, "Smart Contracts and Blockchain for Digital Document Verification," Department of Information Technology, SRM Institute of Science and Technology.
[8] Mohammedsan Rana, Omars Saleh, and Osmanghazali, "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, Kedah, Malaysia; University Utara Malaysia.