International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Certificate Verification and Validation Using Blockchain

C. Vinay Chowdary[1], V. Sudharshan[2], K. Bhargav[3], Ms. Mounika[4] & Ms. Sterlin[5]

[1,2,3] UG Student, [4,5]Guide
School Computer Science and Engineering, Presidency University Bengaluru, Karnataka, India 560069

ABSTRACT—

In order to guarantee the validity and authenticity of credentials given by educational institutions, professional bodies, and other organizations, certificate verification and validation is an essential step. The use of centralized databases, which are prone to fraud, manipulation, and illegal access, is a common component of traditional methods of certificate verification. Block chain technology has come to light as a viable remedy in recent years to improve the security and reliability of certificate verification procedures. An authorized entity issues a certificate to start the certificate verification procedure. The certificate is digitally signed, saved to the block chain, and given a unique cryptographic hash that acts as the certificate's digital fingerprint. Along with pertinent metadata including the issuer, receiver, issue date, and expiration, this hash is maintained on the block chain.

Keywords: Admin, Company, Scanner Module, Upload file, Scan QR code.

I. Introduction

A dynamic, tamper-resistant ecosystem where the validation and verification of certificates transcend traditional limitations. Enter blockchain, the ingenious technological framework that has unveiled a paradigm shift in how we ascertain the authenticity of credentials.

Certificates, whether academic diplomas, professional accreditations, or licenses, have long grappled with issues of counterfeiting, inefficiencies in verification processes, and centralized vulnerabilities. However, the inception of blockchain technology has birthed an innovative solution that redefines trust and reliability.

Imagine certificates being cryptographically sealed into immutable blocks, forming an interconnected chain across a decentralized network of nodes. This blockchain ledger ensures that every credential is time-stamped, linked, and encrypted, creating an incorruptible history of qualifications. Each entry is a testament to its legitimacy, secured by consensus mechanisms that safeguard against alterations or falsifications.

What's groundbreaking is the accessibility and transparency it brings to the table. Through blockchain, stakeholders—employers, educational institutions, or licensing bodies—can effortlessly validate credentials in real-time, eliminating the need for intermediaries or extensive verification procedures. This not only expedites the validation process but also minimizes administrative overheads and fortifies the shield against fraudulent documents.

This transformative approach doesn't just secure certificates; it revolutionizes the very essence of trust in credentialing systems. It propels us toward an era where trust is ingrained in the very fabric of digital verification, empowering individuals and organizations alike to confidently navigate a world where the authenticity of qualifications is unequivocally assured. Blockchain's innovation in certificate verification not only ensures data integrity but also establishes a new standard of trust and reliability in a digital ecosystem.

II. Aim & Objective

The proposed method of certificate verification and validation using block chain introduces a decentralized and transparent approach. Certificates are stored on the block chain, leveraging its immutability and consensus mechanisms. Smart contracts are utilized to automate the verification process, enabling self-executing and tamper-resistant transactions. Verifiers can independently retrieve certificate data from the block chain and validate their authenticity using cryptographic techniques. The distributed nature of the block chain ensures transparency and auditability, reducing reliance on centralized authorities. This method enhances the security, trustworthiness, and efficiency of certificate verification, addressing the limitations of traditional systems and providing a robust solution for various domains, including supply chain, and identity management.

Objectives:

1.Unveiling Universal Trust: Create a blockchain-powered ecosystem that transcends geographical boundaries, ensuring global recognition and trust in verified certificates across industries and regions.

2.Empowering Ownership and Control: Enable individuals to maintain ownership and control over their credentials by providing secure, self-sovereign identity solutions embedded within the blockchain, ensuring privacy and data autonomy.

3.Streamlining Verification Processes: Develop intuitive interfaces and interoperable systems that simplify and accelerate the verification and validation of certificates, reducing bureaucracy and administrative overhead for both institutions and individuals.

4.Continuous Innovation and Adaptation: Encourage ongoing research and development initiatives to stay at the forefront of technological advancements, continuously enhancing the security, scalability, and efficiency of blockchain-based certificate validation systems.

III. Literature Review:

Blockchain in Certificate Validation

Blockchain technology has garnered considerable attention among researchers for its potential in establishing an immutable and transparent system for certificate validation. Scholars emphasize its capacity to create a secure and decentralized repository for certificates, highlighting the advantages of leveraging distributed ledger technology in this context.

Decentralized Certificate Issuance and Verification: Numerous studies delve into the concept of decentralized certificate issuance, wherein educational institutions or certifying bodies have the capability to directly issue certificates onto a blockchain. These investigations often focus on exploring verification mechanisms that enable anyone to authenticate certificates without dependence on a central authority.

Smart Contracts for Automated Validation:

A prevalent topic in the literature is the integration of smart contracts for automated certificate validation. Scholars extensively explore the implementation of self-executing smart contracts, which streamline the validation process by ensuring predefined criteria are met before certifying a document.

Privacy, Security, and Data Integrity: Privacy and security concerns regarding the storage of sensitive educational credentials on a public blockchain are extensively discussed in scholarly works. Researchers actively explore various encryption techniques, zero-knowledge proofs, and off-chain storage solutions aimed at addressing privacy issues while concurrently preserving the integrity of stored data.

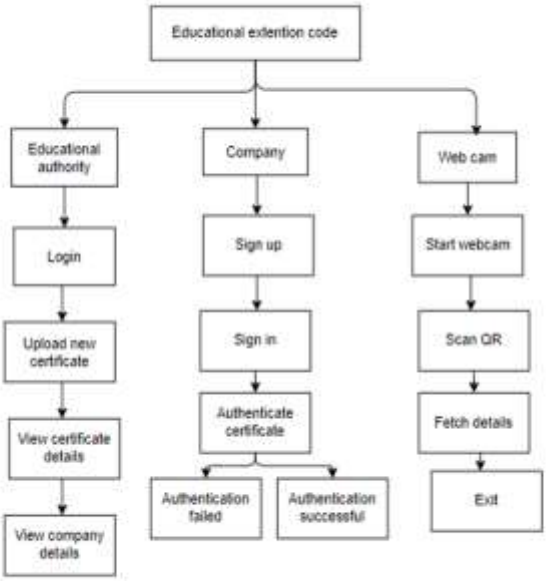
IV. Proposed method

Our project proposes a novel method for certificate verification and validation, leveraging the decentralized and transparent nature of blockchain technology. The process involves the creation and storage of certificates within the blockchain, harnessing its inherent immutability and consensus mechanisms. To streamline verification, smart contracts are employed, enabling automated, tamper-resistant transactions.

One of the key highlights is the independent access that verifiers have to certificate data stored on the blockchain, allowing them to verify authenticity using advanced cryptographic techniques. By eliminating reliance on centralized authorities, this method ensures transparency and auditability through the distributed nature of the blockchain.

The introduction of this approach significantly enhances security, reliability, and efficiency in certificate verification, effectively addressing the shortcomings of conventional systems. Moreover, its robustness extends its applicability across diverse domains such as supply chain management and identity verification.

V. Flow chart:



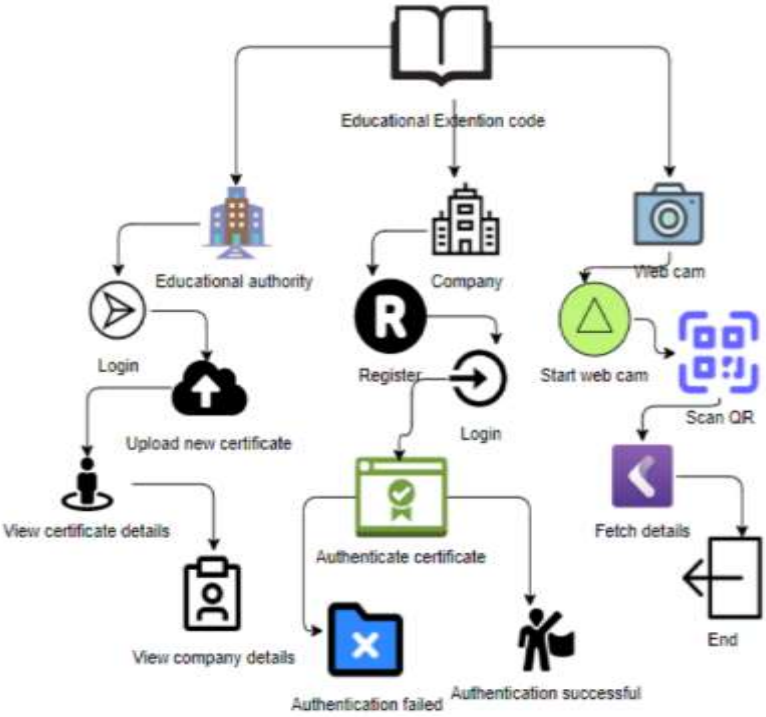
VI. Modules:

Admin Dashboard: The educational authority serves as the system administrator, accessing the platform with credentials 'admin' and 'admin'. Upon login, the admin uploads student information and certificates. These details are securely stored on the Blockchain, associating each certificate with a unique hash code, known as a digital signature. Additionally, a QR code is generated based on this hash code and affixed to the student's certificate. This QR code serves as a portal to retrieve information from the Blockchain; its successful scan validates the certificate's authenticity.

Company login: Users representing companies can create accounts, accessing the platform's interface. Upon login, they have the capability to scan and upload certificates. The system generates a digital signature that is cross-verified with the signatures stored in the Blockchain. If the certificate is genuine, an identical signature is generated, confirming the certificate's authenticity.

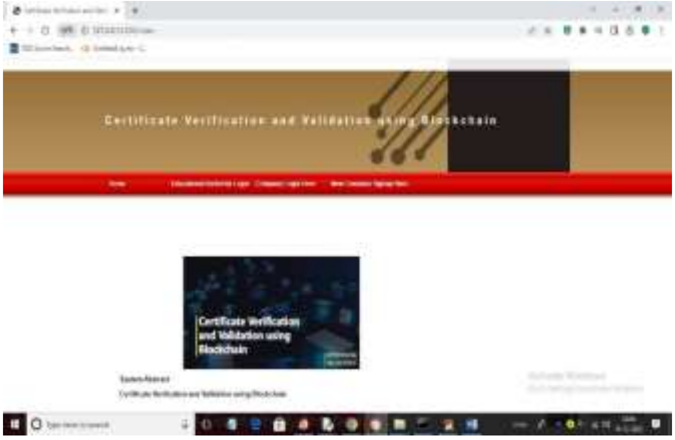
Scanner module: This module is an independent tool utilized by educational institutions and companies. It facilitates the scanning of QR codes affixed to certificates. By scanning these codes, pertinent details are retrieved from the Blockchain, ensuring quick and reliable validation of certificates.

VII.ARCHITECTURE

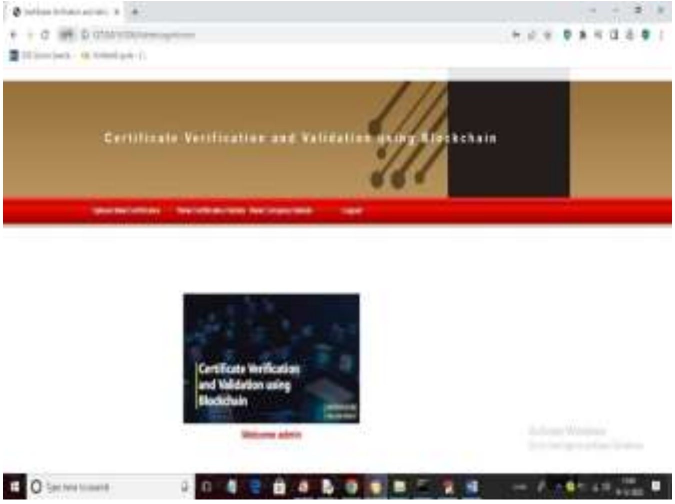


VIII. Results

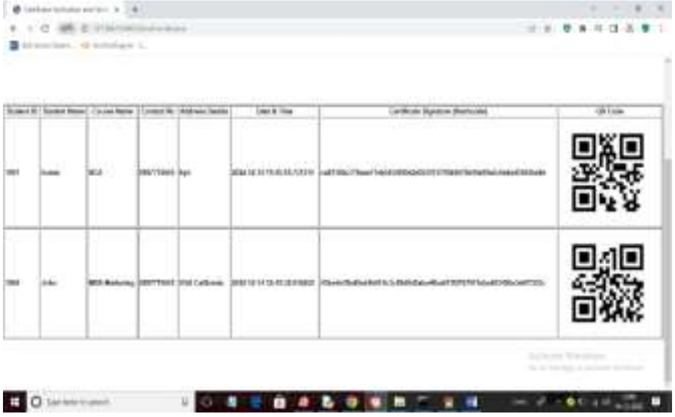
Home page:


Certificate Verification and Validation using Blockchain
Home
Certificate Verification and Validation using Blockchain
System Abstract

Admin page:


Certificate Verification and Validation using Blockchain
Logout
Certificate Verification and Validation using Blockchain
Welcome admin

Certificate details:



Student ID	Student Name	Course Name	Contact No	Address Details	Date & Time	Certificate Signature (Hashcode)	QR Code
[illegible]	[illegible]	BCA	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	MBA Marketing	[illegible]	[illegible]	[illegible]	[illegible]	

IX. CONCLUSION:

In the convergence of technology and education, Blockchain integration for certificate verification marks a revolutionary leap. The admin's pivotal role in securely linking student credentials to Blockchain through digital signatures and QR codes establishes a new trust paradigm. Simultaneously, corporate access ensures validation through Blockchain's stored data, amplifying reliability. The standalone Scanner Module simplifies access, offering seamless QR code scans for instant Blockchain certified information. This transformative ecosystem, fortified by Blockchain's integrity, reshapes certificate validation. Its multifaceted approach across admin, corporate, and scanner modules heralds a future rooted in tech-driven trust. This fusion of reliability and transparency paves the way for a new era in certificate authentication, underlining the potential of Blockchain in education.

REFERENCES

[1] Ali, A., et al. (2021). Blockchain-Based Certification Systems: A Systematic Literature Review. Sensors.

[2] Vignesh, V., et al. (2019). Blockchain-Based Certificate Verification System for Internet of Things. In 2019 10th International Conference on Computing, Communication and Networking Technologies IEEE.

[3] Stukach, V., et al. (2019). Decentralized Blockchain-Based Certificate Validation for Learning Objects. In 2019 International Conference on Information Technology and Systems (ICITS) IEEE.

[4] Alam, M. M., et al. (2019). A Blockchain-Based Secure Certificate Verification System. In 2019 4th International Conference on Networking, Systems and Security (NSysS).

[5] Bello, R. A., et al. (2019). Blockchain-Based Certification System for the Internet of Things. In 2019 IEEE 7th International Conference on Future Internet of Things and Cloud (FiCloud) IEEE.

[6] Bello, R. A., et al. (2020). Blockchain-Based Certificate Verification System for IoT. International Journal of Advanced Science and Technology.

[7] Islam, S. M. R., et al. (2020). Blockchain-Based Certificate Verification and Validation in IoT Systems: A Review. Journal of Information Processing Systems.