CERTIFICATE VERIFICATION AND VALIDATION USING BLOCKCHAIN

Chittiprolu Saranya, Chittibomma Sai Sindhu, Ikkurthi Chandi Priya, Dantu Swathi, Anne Dhatri, Dr. A. Kalavathi

Abstract
Everything is digitalized in the digital age, academic certificates which are sent to students and digitalized at educational establishments. Students have difficulty maintaining their degree credentials. Organizations and institutions find it difficult and time-consuming to verify certificates. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. Due to the lack of an effective anti-forgery mechanism, events that cause the graduation certificate to be forged often get noticed. To solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. A blockchain platform is a shared digital ledger that allows users to record transactions and share information securely. The procedure of issuing the digital certificate in this system is as follows. First, the paper certificates are converted into digital certificates. The blockchain technology is used to generate the hash code value for the certificate. Then the certificates are stored in blockchain. The system will create a related QR-code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries.

Keywords: Blockchain, Ethereum, Smart Contracts, Ganache, MetaMask.

1. Introduction
The project "Certificate Verification and Validation Using Blockchain" endeavours to modernize the conventional methods of verifying academic certificates by harnessing the potential of blockchain technology. In today's digital era, the proliferation of counterfeit certificates poses a substantial obstacle for educational institutions, students, and employers. This project addresses this pressing concern by furnishing a secure, transparent, and tamper-proof platform for validating the authenticity of academic credentials. By operating through a decentralized blockchain network, the system ensures that verified student details are securely stored.

Each certificate undergoes encryption and receives a unique identifier before being added to the blockchain. This guarantees the immutability and tamper-resistance of certificate data, thereby serving as a reliable source of truth for all parties involved. One of the standout advantages of this system is its heightened security. Employing blockchain technology ensures that the integrity of certificate data remains intact, significantly mitigating the risk of fraudulent activities. Additionally, the system fosters
transparency and traceability, empowering users to effortlessly verify the legitimacy of certificates. Furthermore, the system streamlines the verification process, enhancing efficiency manifold. Through the utilization of QR codes, companies can promptly scan and validate certificates, obviating the necessity for laborious manual verification techniques. This not only saves time but also alleviates administrative burdens and reduces associated costs.

Moreover, the system champions global accessibility, facilitating seamless verification procedures across diverse geographical locations. Whether it pertains to a student exploring job prospects overseas or an employer verifying the credentials of a potential candidate, the system offers a universally accessible platform for certificate validation. In essence, "Certificate Verification and Validation Using Blockchain" proffers a robust remedy to the pervasive issue of counterfeit certificates in the education sector. By amalgamating the security and transparency of blockchain technology with the efficiency of QR code-based verification, the project endeavors to uphold the integrity and credibility of academic credentials for all stakeholders.

2. Literature Survey

2.1 Advancing Security with Blockchain-based Certificate Transparency:
Blockchain-based certificate transparency solutions enhance security by providing an immutable record of issued certificates and mitigating potential risks associated with the certificate authority system. These systems allow for transparent and decentralized verification of certificates, ensuring the integrity and authenticity of online communications and transactions.

2.2 Decentralized Certificate Revocation Systems:
In the traditional setup, digital certificate revocation systems have struggled with operational challenges, mainly due to the lack of mutual trust, access stability, and data synchronization among certification authorities (CAs). A cutting-edge solution to tackle these issues is the utilization of decentralized certificate revocation systems. Leveraging consortium blockchain technology, these systems facilitate collaborative management of digital certificate revocation lists (CRLs) among multiple CAs, ensuring improved reliability, security, and real-time updates in the certificate ecosystem.

2.3 Enhancing Trust and Security in Certificate Issuance:
The increasing number of fake certificates has become a significant concern, affecting education, employment, and various other sectors. Implementing blockchain technology for certificate issuance and verification ensures tamper-proof, transparent, and secure processes. By utilizing blockchain's decentralization and encryption features, institutions can streamline certificate management and build a trusted ecosystem for validating credentials.

Blockchain technology offers unprecedented opportunities for enhancing certificate verification and validation processes, revolutionizing traditional approaches to certification management. By leveraging blockchain-based certificate transparency mechanisms and decentralized revocation systems, organizations can ensure the authenticity and integrity of academic credentials, mitigating the risks associated with counterfeit certificates and fraudulent activities. Through continued research and innovation in this field, blockchain-based solutions have the potential to redefine certificate authentication in the digital age, fostering greater trust and confidence in certification processes.
3. Proposed System

We introduce the utilization of Blockchain technology to address the challenge of ensuring the authenticity and integrity of academic certificates. Blockchain, renowned for its immutable nature and tamper-resistant properties, serves as an ideal platform for securely storing certificate data.

- Certificate Storage on Blockchain: When a certificate is issued to a student, the admin user initiates the process by storing a digital copy of the certificate on the Blockchain. This digital copy undergoes hashing and encryption processes to ensure its integrity and security.

- Digital Signature Generation: Following the storage of the certificate on the Blockchain, a digital signature is generated for the certificate data. This digital signature acts as a unique identifier and provides assurance of the certificate's authenticity.

- QR Code Generation and Affixing: Subsequently, a QR code is generated using the digital signature of the certificate. This QR code encapsulates the digital signature and serves as a tangible link to the Blockchain-stored certificate data. The QR code is then affixed to the student's certificate.

- Verification Process: When external entities, such as companies or institutions, need to verify the certificate, they can easily scan the QR code using a QR code scanner. The scanner decodes the QR code and extracts the embedded digital signature.

- Validation from Blockchain: The extracted digital signature is then used to query the Blockchain. If the digital signature exists on the Blockchain, it confirms the validity and authenticity of the certificate. The certificate details associated with the digital signature are retrieved from the Blockchain and presented to the verifying party.

- Successful Certificate Validation: If the QR code exists on the Blockchain and the digital signature matches, the certificate validation is deemed successful. The verifying party can confidently trust the authenticity of the certificate, as it has undergone secure storage and validation on the Blockchain.

System design is an interdisciplinary engineering activity that enables the realization of successful systems. This system may be defined as an integrated set of components that accomplish a defined objective. The process of systems design includes defining software and hardware architecture, modules, interfaces, and data to enable a system to satisfy a set of well-specified operational requirements.

Figure: System Architecture
4. Modules

1. User Authentication and Authorization:
   - Implement secure login mechanisms for both students and companies.
   - Authenticate users based on their credentials and roles.
   - Authorize access to specific functionalities based on user roles and permissions.

2. Student Details Upload and QR Code Generation:
   - Enable students to upload their academic details securely.
   - Generate QR codes containing unique identifiers for each certificate.
   - Associate QR codes with verified student details stored on the blockchain.

![Certificate Verification and Validation using Blockchain](image)

Figure: Certificate details

3. Company Login:
   - Provide secure login for companies to access the verification system.
   - Authenticate companies based on their credentials.
   - Grant access to certificate verification functionalities upon successful login.

4. Validation of Certificates:
   - Allow companies to scan QR codes to verify the authenticity of certificates.
   - Validate certificates by querying the blockchain for corresponding student details.
   - Display verified academic credentials to the verifying party.

5. Scan QR Code:
   - Authorized users can scan QR codes to retrieve product details instantly.
   - QR code scanning enables quick and convenient access to product information.
5. **Future Recommendation and Conclusion**

Data security is the foundation of blockchain technology. Blockchain is a large, open access online ledger where every node stores and verifies the same data. The possibility of certificate fraud can be reduced using blockchain based methods. The certificate application process and the automatic certificate feeding process in the system are open and transparent. The company or organization can request information about the certificate from the system. In summary, this system ensures the accuracy and security of information.

**Blockchain Certificate Generation:**
- Develop a feature to generate digital certificates directly on the blockchain using smart contracts.
- Implement mechanisms to ensure the authenticity and immutability of generated certificates.

**Enhanced Verification Mechanisms:**
- Implement advanced verification mechanisms, such as cryptographic hashing and digital signatures, to further enhance the security and trustworthiness of certificates.
- Explore the use of zero-knowledge proofs to allow certificate verification without revealing sensitive information.

6. **References**


