Digital Certificate Verification using Blockchain

Prof. Priyanka Abhale[1], Anjali Chikate[2], Shubhada Jadhav[3], Irshad Shaikh[4], Rutuja Bhole[5]

ALARD COLLEGE OF ENGINEERING & MANAGEMENT
(ALARD Knowledge Park, Survey No. 50, Marunji, Near Rajiv Gandhi IT Park, Hinjewadi, Pune-411057)
Approved by AICTE. Recognized by DTE. NAAC Accredited. Affiliated to SPPU (Pune University).

Abstract - This composition describes a blockchain technology algorithm for validating digital instruments. As the number of university and advanced education scholars and graduates continues to grow each time, there's a need to fluently validate scale instruments. In this paper, we project two fiscal models in which the price of services is balanced between graduates and employers as the main actors of services. scholars demand cheap and fluently empirical instruments, and employers demand presto and dependable evidence of their degrees. The issue of fake credentials is a big bone. Getting a fake education instrument in India isn't that delicate.

Key Words: **(Blockchain, Document Verification, QR Code, Privacy Protection, Hash Value, connect to the blockchain network, Digital Certificate, distributed, Pre-processing)**

1. INTRODUCTION

During the training scholars will get numerous instruments. scholars produce these instruments when applying for public or private sector jobs. All of these instruments must be manually vindicated. occasionally scholars present fake instruments and are delicate to identify. The issue of fake academic credentials has long been a problem in academia. This is because similar instruments are cheap to produce and bear homemade confirmation, which greatly complicates the confirmation process. This problem can be answered by storing digital instruments on the blockchain.

1.1 Problem Definition

Student certificate verification using blockchain technology is a process that utilizes the decentralized and immutable nature of blockchain to verify the authenticity and integrity of student certificates. It involves recording certificate details, such as academic qualifications and achievements, on a blockchain network. This information is cryptographically secured and stored across multiple nodes in the network, making it resistant to tampering and fraud.

1.2 Model Architecture

For blockchain- grounded inflexible instruments, universities must first enroll. Each university has a portmanteau address for transferring deals. Universities can only be added by smart contract possessors. Once added, the university can pierce the system to produce instruments containing data fields. Each instrument created is stored in the Interplanetary train System (IPFS) and returned with a unique hash generated using the SHA-256 algorithm. This serves as a unique ID for each document. All this data, along with this generated hash and instrument details, is stored on the blockchain and the performing sale ID is transferred to the pupil.

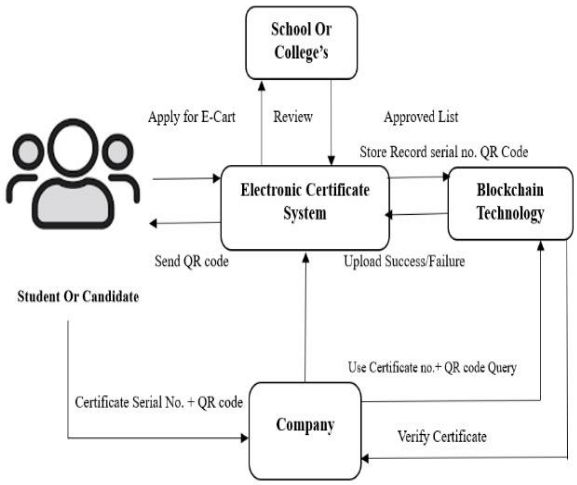

Fig -1: Model Architecture

1.3 Algorithm consensus algorithm

A consensus algorithm is a mechanism used in distributed systems to achieve agreement among multiple participants or nodes on a single shared value or state. Consensus algorithms are crucial for ensuring the integrity, consistency, and fault tolerance of distributed systems, especially in scenarios where there is a possibility of node failures or malicious behavior.

Contrast-Limited Adaptive Histogram Equalization (CLAHE): CLAHE further refines AHE by introducing a constraint on the amount of contrast enhancement

applied. It limits the amplification of the histogram equalization process to prevent over-amplification of noise and maintain a more natural appearance.

smart contrast algorithms

These are just a few examples of smart contrast algorithms, and there are many variations and combinations of these techniques. Each algorithm has its strengths and weaknesses, and the choice of algorithm depends on the specific requirements of the application and the desired visual outcome cases. Some notable consensus algorithms include:

Raft: Raft is a consensus algorithm designed for simplicity and ease of understanding. It divides the participants into three roles: leader, follower, and candidate. The leader is responsible for coordinating the consensus process, and followers replicate the leader's actions. Raft focuses on strong leader election and log replication to achieve consensus.

2. Implementation

Implementing certification verification using QR codes and blockchain technology can provide a secure and tamper-proof method for verifying the authenticity and integrity of certificates.

1. Certificate Creation: The certification authority generates the certificates and assigns a unique identifier to each certificate. The certificate details, including the issuer, recipient, and certification data, are stored in a digital format.

2. QR Code Generation: A QR code is generated for each certificate, containing the unique identifier or a reference to the certificate data. The QR code can be printed on the physical certificate or made available electronically.

3. Blockchain Integration: The certificate data and its unique identifier are hashed and stored on a blockchain. The blockchain provides an immutable and decentralized ledger to securely store and verify the certificate information. The certificate hash serves as a digital fingerprint or proof of the certificate's existence.

4. QR Code Linking: The QR code is linked to the corresponding certificate entry on the blockchain. This linkage can be achieved by storing the unique identifier or the blockchain transaction ID within the QR code itself or associating it in a centralized database.

5. Verification Process: When a certificate needs to be verified, the recipient or anyone with access to the certificate can scan the QR code using a QR code reader application on their smartphone or device.

6. QR Code Decoding: The QR code reader decodes the information embedded in the QR code, which typically includes the unique identifier or reference to the certificate data.

7. Blockchain Lookup: The decoded unique identifier or reference is used to retrieve the corresponding certificate entry from the blockchain. The certificate data, including the hash value, is fetched from the blockchain.
8. Hash Comparison: The fetched certificate data is hashed again, and the resulting hash is compared with the stored hash value retrieved from the blockchain. If the hashes match, it indicates that the certificate has not been tampered with.

9. Additional Verification: Depending on the requirements, additional verification steps can be performed, such as checking the issuer's digital signature, expiration date, or cross-referencing the certificate details with a trusted database.

3.Objectives

The system saves paper, reduces administrative costs, prevents document counterfeiting, and provides accurate and reliable digital certificate information. This system ensures the accuracy, security and immutability of information. Implement a validation algorithm that can validate each peer for each access request.

Scope of Study

The purpose of system is to enhance the security, transparency, and trustworthiness of certificates or credentials issued by a system or organization. By integrating QR codes into the certificates, individuals or entities can easily scan the code with a smartphone or other devices to retrieve and verify the certificate's information. This process helps in preventing tampering or forgery of the certificate. The use of blockchain technology adds an additional layer of security and immutability to the verification process.