

CERTIFICATE VALIDATION USING BLOCKCHAIN TECHNOLOGY

PROJECT MENTOR :

Sri. K. N. V. Suresh Varma

Presented by:

JYOTHI - 21B91A0462
AJAY - 21B91A0403
HEMANTH - 21B91A0459
VENKAT SAI - 21B91A0435



Introduction

Overview of Blockchain Technology:

Definition: Blockchain is a decentralized, distributed ledger technology that records transactions across multiple computers in a secure and tamper-resistant manner.

Key Features :

- Decentralization
- Transparency
- Immutability
- Security
- Emerging tool for secure document authentication.
- Addresses document fraud and misuse.



Project Objective

Aim of the project :

- Enhance the document verification process using blockchain.
- Identify security themes necessary for document verification.
- Analyze existing blockchain-based educational certificate verification solutions.



Problem Statement

Current Challenges :

- Digitization of academic certificates increases security breaches.
- Institutions face difficulties in validating digital certificates.
- Compromised user privacy regarding academic credentials.



Existing System

Current Process:

- Generates an electronic file for paper certificates.
- Uses Hyperledger for authenticity verification.

Disadvantages:

- Manual verification is time-consuming.
- Hyperledger's limitations:
 - Not suitable for public blockchain due to privacy issues.
 - Low scalability for widespread use.
 - Primarily a B2B platform.



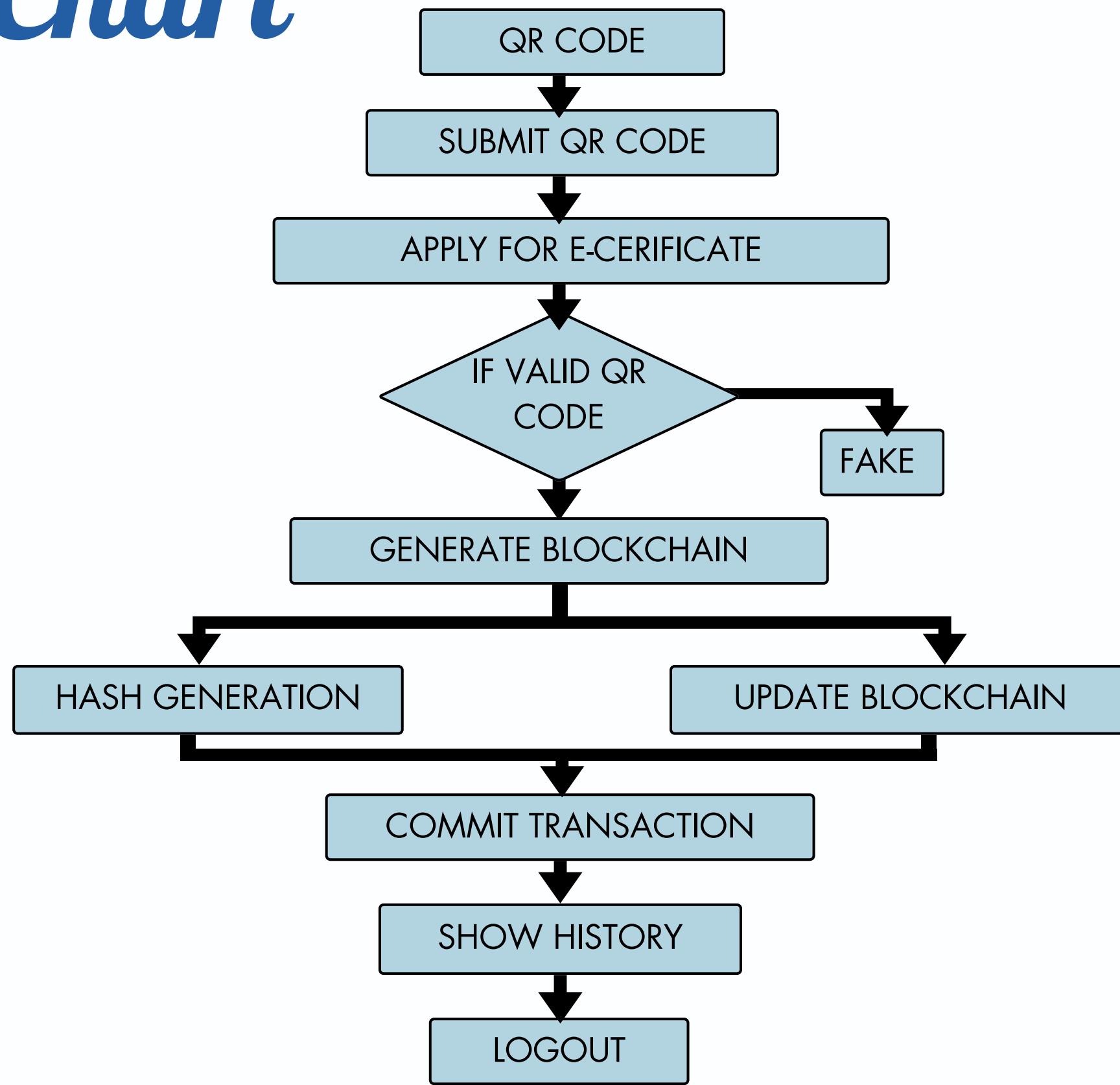
Proposed System

**Introducing Blockchain and QR
code-based verification system for
certificates**

A system that combines blockchain's security features with the simplicity of QR codes to verify the authenticity of digital or physical certificates.



Flow Chart



How It Works :

- Each certificate is hashed and stored on the blockchain, generating a unique identifier.
- A corresponding QR code is embedded on the digital or physical certificate.
- When the QR code is scanned, it retrieves the certificate data from the blockchain, enabling easy, real-time verification.

Why It's Effective:

- Ease of Use
- Security
- Efficiency



Implementation Steps

1. Create Digital Certificate :

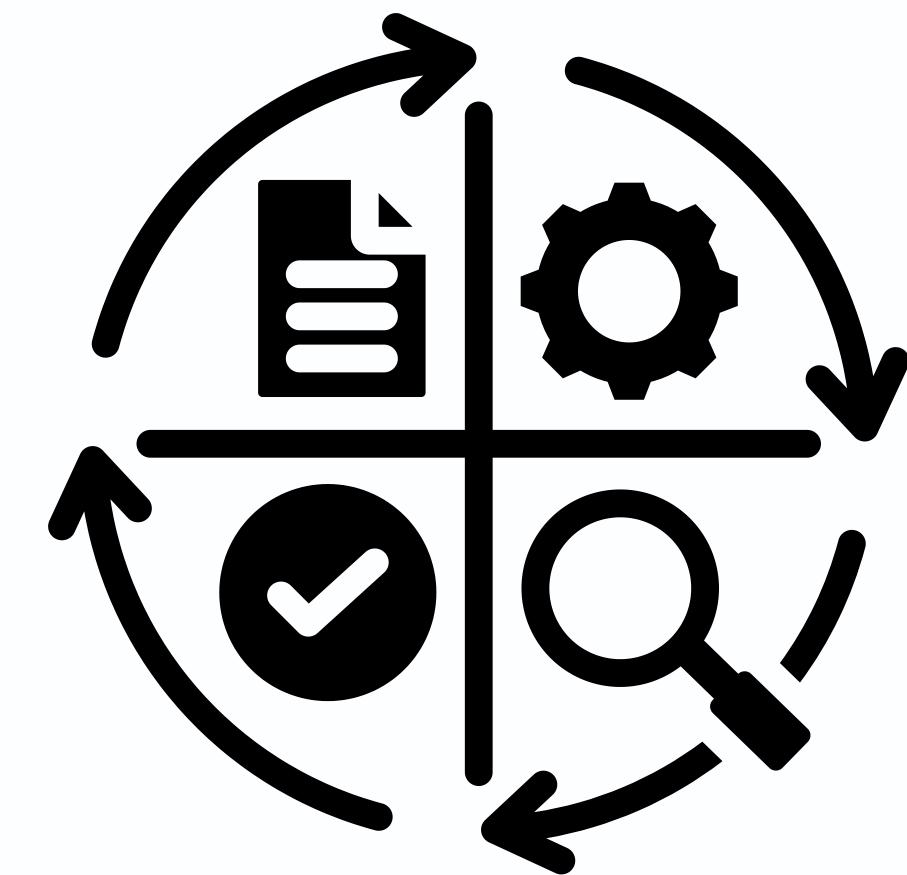
- Include recipient's name, issuing authority, date of issuance, and achievement details.

2. Generate Unique Identifier :

- Use cryptographic hashing (e.g., SHA-512) to create a certificate hash.

3. Choose Blockchain Platform :

- Options: Ethereum, Hyperledger, or custom solution with smart contract support.



Smart Contract Development

4. Create Smart Contract:

- Store certificate details and unique identifier on the blockchain.
- Include functions for certificate verification.



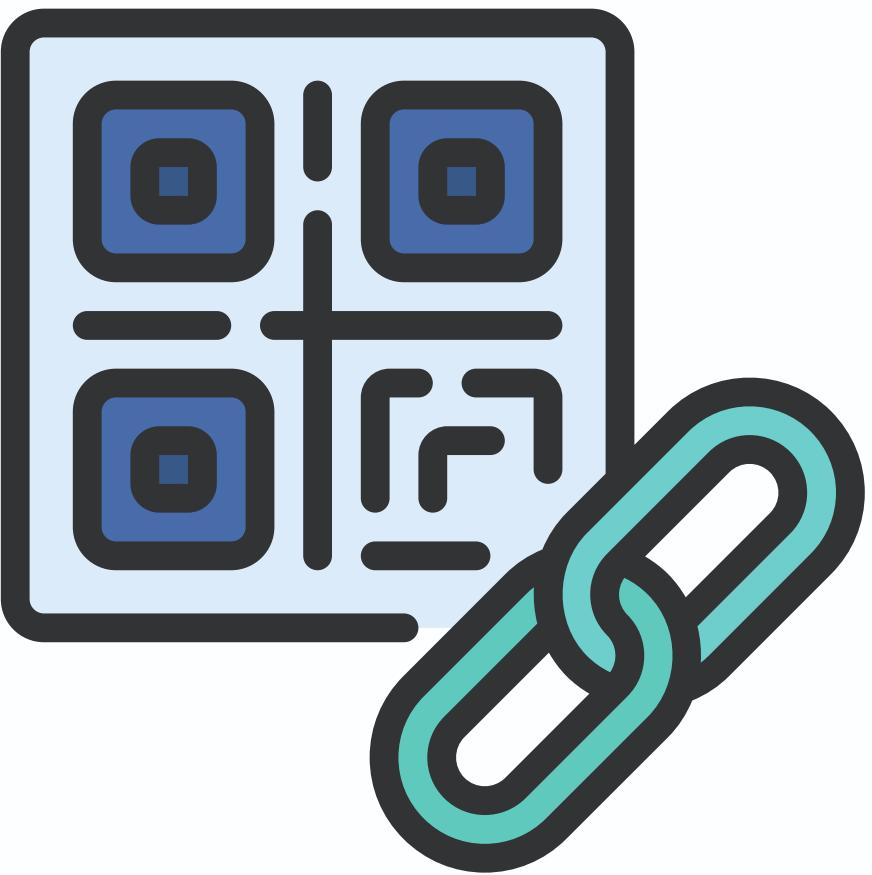
Linking Certificate to QR Code

5. Generate QR Code:

- Encode the unique identifier or smart contract link.

6. Embed QR Code:

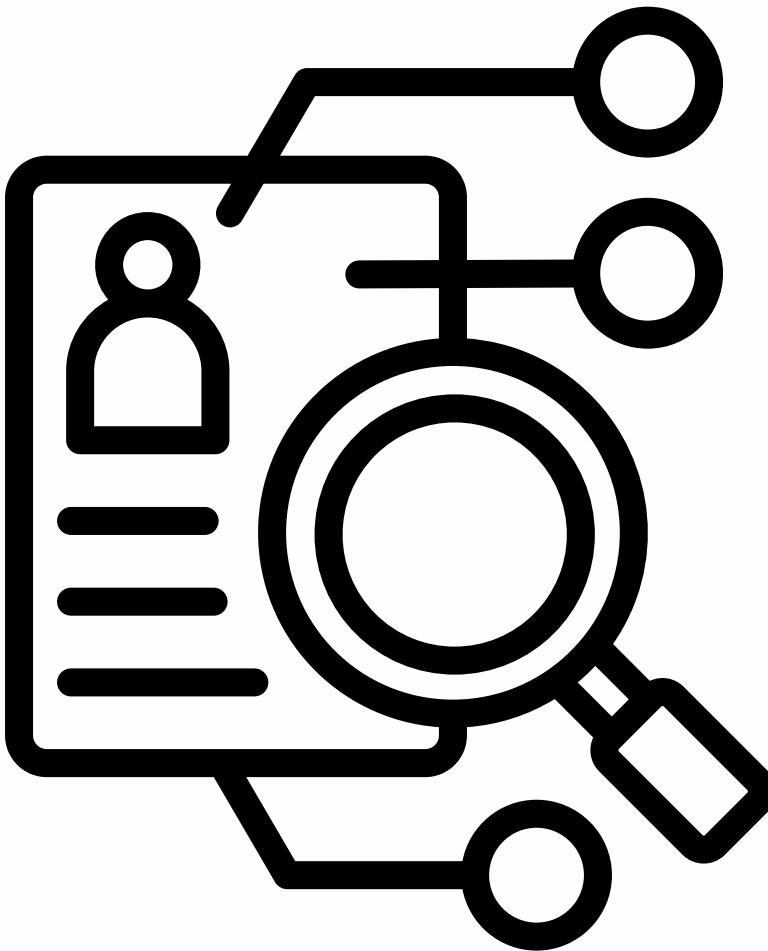
- Place on the digital or physical certificate for easy access.



Verification Process

How Verification Works:

- Scan the QR code using a mobile device.
- Retrieve the unique identifier or smart contract link.
- Query the blockchain for corresponding certificate information.
- Verify authenticity by matching the identifier with stored data.



Benefits of Proposed System

Advantages :

- Enhanced security and efficiency in document verification.
- Reduced manual efforts and time in validation.
- Improved privacy for users with tamper-proof certificates.



Conclusion

- Blockchain technology offers a transformative approach to document verification.
- The proposed QR code integration simplifies the verification process and enhances security.





Thank
you!