WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Blockchain-Based Verification System for Academic Certificates and E-Signing

Prof.N.M.Dimble, Sakshi S. Rasal, Viraj A. Dhas, Ajinkya M. Damodar, Avinash B. Chavan

Department of Computer Engineering, Navsahyadri Education Society's Group of Institute Faculty of Engineering, Pune, Maharashtra, India

Abstract

In today's digital era, educational certificates such as SSLC, HSC, and degree certificates are being digitized for ease of access and management. However, maintaining and validating these certificates remains a cumbersome task for both students and organizations. This project proposes a blockchain-based system for securely storing, verifying, and e-signing academic certificates. The approach involves converting physical certificates into digital formats, generating hash values using a chaotic algorithm, and storing them on the blockchain. Verification is facilitated via a mobile application, ensuring a secure and efficient process.

Key Words: Blockchain, Academic Credentials, Certificate Verification, Digital Signing, Cryptographic Hashing.

1. INTRODUCTION

Academic credentials are essential indicators of qualifications, yet their reliability is increasingly undermined by fraud and unauthorized alterations. The need for a secure, scalable, and globally accessible verification method is more urgent than ever. Blockchain technology, with its inherent immutability and decentralization, offers a compelling solution. This study proposes an integrated platform that uses blockchain to store digital certificates and validate them in real time. The platform includes an Android-based mobile application for administrators to upload credentials and for verifiers to authenticate them using a unique hash.

2. LITERATURE SURVEY

2.1 Cheng et al. (2018) – Blockchain and Smart Contracts for Digital Certificates

Jiin-Chiou Cheng and colleagues proposed a blockchain-based system for issuing tamper-proof graduation certificates using Ethereum. The solution incorporated smart contracts and QR codes for validating the authenticity of documents. While it offered decentralization and transparency, a major drawback was its dependency on internet access and external QR code scanning applications, which made it less efficient in offline or constrained environments.

2.2 Wang et al. (2019) – Certificate and Revocation Transparency

Ze Wang et al. introduced a framework based on blockchain that not only validated certificate authenticity but also enabled transparency in certificate revocation. The system integrated with Firefox and used certificate transparency (CT) logs. Although the system strengthened accountability for Certificate Authorities (CAs), it suffered from performance issues, including delayed validations and limited user scalability.

2.3 Zhang and Ma (2018) – Consortium Blockchain and Secret Sharing

Aisong Zhang and Xinxin Ma developed a decentralized certificate revocation system using a consortium blockchain. Their approach utilized a secret-sharing scheme to protect user privacy while supporting certificate authentication and revocation. The primary innovation was its secure handling of user data; however, the consortium model limited participation and relied on partial centralization, making it less robust for open environments.

2.4 Madala et al. – Hyperledger Fabric Implementation

Madala and his team adopted the Hyperledger Fabric blockchain platform to create a secure academic credential system. Their architecture included certificate transparency techniques to ensure only authorized issuers could register certificates. Despite its secure design, this model encountered challenges with scalability, high latency in transaction processing, and an inability to handle large datasets efficiently in a decentralized environment.

2.5 Marco Baldi et al. – Public Ledger-Based Certificate Validation

Marco Baldi and collaborators introduced a model where certificate validation was performed through public ledgers and private blockchain infrastructure. Their use of Certificate Revocation Lists (CRLs) enhanced certificate management, with CAs distributing CRLs over a secure blockchain. However, the need for private blockchain hosting raised questions about system openness, cost, and ease of adoption for smaller educational institutions.

3. OBJECTIVES OF PROPOSED SYSTEM

3.1. Ensure Certificate Authenticity and Integrity

To guarantee that academic certificates cannot be forged or altered, the system will use cryptographic hashing and blockchain immutability. Each certificate will be uniquely identified by a hash that acts as its digital fingerprint, ensuring data integrity throughout its lifecycle.

3.2. Eliminate Centralized Dependence

Conventional systems rely heavily on centralized databases which pose single points of failure. The proposed system will adopt a decentralized approach using blockchain to store and verify academic records, eliminating risks associated with central authority compromise.

3.3. Enable Real-Time and Remote Verification

Employers, institutions, and other stakeholders often face delays in certificate verification. This system will enable real-time validation through a mobile or web-based application, allowing verifiers to instantly confirm the legitimacy of academic credentials from any location.

3.4. Integrate a Secure E-Signing Mechanism

To authenticate the issuing authority, the system will include a digital signing feature that allows authorized academic institutions to sign certificates electronically. This e-signature ensures that the document is institutionally verified and tamper-evident.

3.5. Automate Validation via Smart Contracts

The inclusion of smart contracts will streamline the validation process. These contracts will autonomously check certificate hashes against the blockchain ledger, reducing human error and administrative burden.

3.6. Provide a User-Friendly Interface

The system aims to be accessible for all stakeholders, including administrators, students, and verifiers. A simplified and intuitive user interface will facilitate easy navigation, certificate upload, and validation processes.

4. PROPOSED SYSTEM

4.1 Methodology

The system involves a multi-layered approach where academic certificates are digitized and secured using blockchain. Institutions generate hash values using a cryptographic algorithm and record them on the blockchain. The corresponding verification application allows secure access to verify the originality of these documents through hash matching.

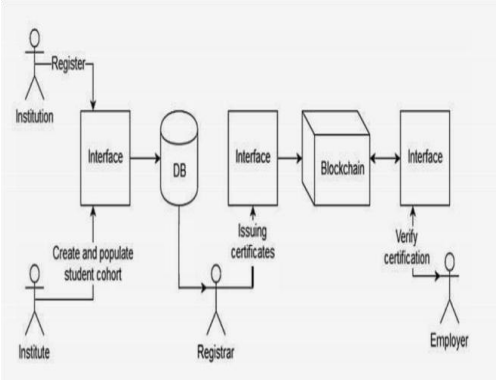


Fig -1: Architecture of the proposed system

4.2 Digital Certificate Creation

Certificates are converted from physical to digital format through image processing techniques like sampling and quantization. Each certificate is linked to a student profile stored securely in the system database.

4.3 Hashing Mechanism

A secure chaotic hashing algorithm is applied to create a fixed-size unique identifier for each certificate. This hash is collision-resistant, ensuring no two different certificates generate the same value.

4.4 Validation Process

Verifiers access the system via a mobile app. They input the student ID and certificate type. The app retrieves the stored hash and compares it to a newly generated one from the presented certificate. A match confirms authenticity.

4.5 Application Interface

The application features an admin login to upload and manage student records. Verifiers have access to a verification module. Success or failure messages are shown based on the validation result.

5. MATHMATICAL MODEL

Blockchain technology can be used to verify the authenticity and integrity of documents by utilizing concepts like cryptographic hash functions, digital signatures, and consensus protocols. Here's an outline of the mathematical model and concepts involved in document verification using blockchain:

5.1 Document Hashing

Every document to be verified is first hashed using a cryptographic hash function, which transforms the document into a fixed-size string of characters (hash). This hash acts as a unique fingerprint of the document.

5.2 Digital Signature

To validate authenticity, the hash is digitally signed with the creator's private key.
Formula:
If SK() is the signing function and K is the private key:

SK(h(D)) = Signature
This confirms the document originates from the rightful source.

Mathematical Representation:

Let D be a digital certificate and H() a cryptographic hash function.
Hashing: h = H(D)
Digital Signing: S = Sign(h, PrivateKey)
Blockchain Entry: Block = {PreviousHash, h, S, Timestamp, CertificateID}

For verification:
1. Hash D′ as h′ = H(D′)
2. Check if h′ == h
3. Verify S using the institution's public key
Consensus: PoW/PoS ensures block validity and immutability

5.3 Storing of Blockchain

Once a digital signature has been applied to the hash of a document, it is stored on a blockchain along with supplementary metadata such as the timestamp and a unique identifier. Each record (or block) also includes a reference to the hash of the preceding block, creating a linked sequence of entries that form an immutable ledger.

Mathematical Representation:
Let T□ denote a transaction block within the blockchain. It contains the following components:
T□ = {Previous_Block_Hash, Document_Hash, Timestamp, Signature, Document_ID}

Where:
Previous_Block_Hash: Represents the cryptographic hash of the immediately preceding block in the chain. This ensures each block is securely connected to its predecessor.
Document_Hash = h(D): This is the result of applying a hash function to the original document D, serving as a digital fingerprint.
Timestamp: Indicates the exact time when the block containing the document was added to the blockchain.
Signature = SK(h(D)): A digital signature derived by encrypting the document hash with the private key of the issuer, confirming document authenticity.
Document_ID: A unique identification code assigned to the specific document or credential being recorded.

5.4 Verification Process Storing of Blockchain

5.4.1. Integrity Validation

The integrity of a document is confirmed by comparing the cryptographic hash of the currently submitted document with the hash originally recorded in the blockchain.
Let D′ be the document presented for verification. Its hash is computed as:
h(D′) = H(D′)
To ensure the document hasn't been modified:
If h(D′) = h(D),
then the document remains unchanged since storage.
Here:

1. H() is the cryptographic hash function (e.g., SHA-256),
2. h(D) is the hash originally stored on the blockchain,
3. h(D′) is the hash of the document at the time of verification.

5.4.2. Authenticity Confirmation

To verify that the document was signed by the original issuer, the system checks whether the digital signature matches the stored hash using the public key of the signer.
Let K□ub represent the public key, and SK(h(D)) be the digital signature (created using the issuer's private key). The verifier applies the verification function:
VK□ub(SK(h(D))) = h(D)
Where:

1. VK□ub(·) is the verification function that uses the issuer’s public key to validate the signature.
2. If the output equals h(D), it proves that the document was indeed signed by the correct source and has not been altered.

Together, these steps ensure:

1. The document’s contents remain intact (integrity),
2. The source of the document is legitimate (authenticity).
3. To verify the document, the verifier checks two things:

5.5 Blockchain Consensus

To finalize entries, blockchain consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) are used.
PoW(Tn) ⇒ Valid Block
PoS(Tn) ⇒ Valid Block
These ensure all nodes agree on the legitimacy of new entries.

5.6 Security Analysis

Security is maintained through:

1. Hash function pre-image resistance
2. Digital signature unforgeability
3. Blockchain immutability via consensus

Summary of Mathematical Model:

By applying these cryptographic and blockchain principles, document verification becomes a secure, transparent, and tamperproof process.

1. Hash Generation:

Each document (D) is converted into a fixed-length cryptographic hash using a secure function:h(D) = H(D)
his hash serves as a digital fingerprint unique to that document.

2. Digital Signing:

The generated hash is then signed with the private key of the document issuer to create a digital signature:SK(h(D)) = Signature
This step ensures that the source of the document can be validated later.

3. Blockchain Entry:

The signed hash, along with metadata like timestamp and a unique document ID, is recorded as a block in the blockchain:T□ = {Previous_Hash, h(D), SK(h(D)), Timestamp, Document_ID}

Each block links to the previous one, forming a secure and immutable ledger.

4. Verification Process:

During validation:

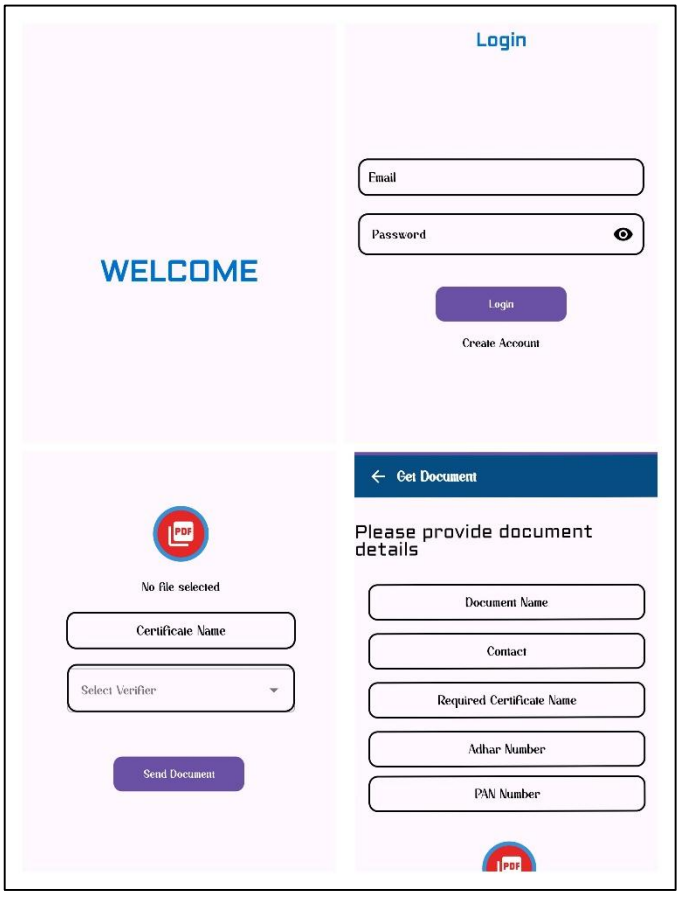
1. A new hash (h(D′)) is computed from the presented document.
2. It is compared with the stored hash (h(D)) to ensure the document hasn't been altered.
3. The digital signature is also verified using the issuer's public key to confirm authenticity :VK□ᵤb(SK(h(D))) = h(D)

4. Consensus Assurance:

Blockchain consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS) are used to validate and agree on new entries:

PoW(T□) ⇒ Valid Block or PoS(T□) ⇒ Valid Block

6. INTERFACE OF DEVELOPED SYSTEM



7. CONCLUSION

This research presents a blockchain-enabled framework to tackle academic document forgery. Securing data is critical, and blockchain's immutability ensures stronger data protection. The proposed application enables users to both view and verify credentials. It offers high assurance of data correctness and helps individuals manage their electronic documents effortlessly

REFRENCES

[1]. Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; YiHua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[2]. Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[3]. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

[4]. Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[5]. Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[6]. Nitin Kumavat, Swapnil Mengade,Dishant Desai ,Jesal Varolia,"Certificate Verification System using Blockchain"Computer Engineering Department, Mumbai University.

[7]. S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.

[8]. Omars Saleh, osman ghazali, muhammad ehsan rana, "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, University Utara Malaysia, Kedah, Malaysia.

[9]. Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/ 10.1109/ATC.2018.8587428.

[10]. Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).