Blockchain-Based Student Accreditation and Credential Verification System

Mr.S.S.Jadhav
Assistant Professor, Computer Engineering
All India Shri Shivaji Memorial Society's
College of Engineering
Savitribai Phule Pune University
Pune, India

Parth Lanke
Computer Engineering
All India Shri Shivaji Memorial Society's
College of Engineering
Savitribai Phule Pune University
Pune, India

Kushagra Pachouly
Computer Engineering
All India Shri Shivaji Memorial Society's
College of Engineering
Savitribai Phule Pune University
Pune, India

Tanmay Kale
Computer Engineering
All India Shri Shivaji Memorial Society's
College of Engineering
Savitribai Phule Pune University
Pune, India

Dhruav Mandare
Computer Engineering
All India Shri Shivaji Memorial Society's
College of Engineering
Savitribai Phule Pune University
Pune, India

***Abstract*—The verification of academic credentials remains one of the most critical challenges in higher education and employment ecosystems. With the rapid digitalization of records, the circulation of forged certificates and manipulated transcripts has increased significantly, damaging institutional reputation and eroding public trust.**

Existing frameworks such as India's Digital Locker, Cerberus, and EduCTX represent significant advances but exhibit key limitations. The Digital Locker Framework, though government-backed, is still centrally controlled, making it susceptible to single-point failure and limited interoperability. Cerberus, a blockchain-based approach, ensures immutability through Merkle trees but suffers from high on-chain complexity and limited user accessibility. EduCTX, on the other hand, focuses primarily on credit transfer and lacks mechanisms for credential authenticity and issuer validation.

This project proposes a Blockchain-Based Student Accreditation and Credential Verification System, which integrates the advantages of distributed ledger technology with QR code-enabled instant verification and digital signature-based authentication. In this system, every credential issued by an accredited institution is hashed, digitally signed, and registered on a permissioned blockchain network. Each certificate contains an embedded QR code that links to its blockchain record, allowing employers, universities, and organizations to validate authenticity in real time.

The blockchain ledger ensures immutability, transparency, and auditability, while smart contracts provide a revocation mechanism for invalid or withdrawn credentials. Sensitive data such as student details remain stored off-chain in encrypted form, thereby maintaining compliance with privacy laws like the General Data Protection Regulation (GDPR) and India's Information Technology Act.

The proposed framework creates a secure, tamper-proof, and decentralized academic ecosystem, bridging the gap between universities, students, and verifiers. It reduces verification time from days to seconds, mitigates fraud, and promotes trust through cryptographic verification and institutional accountability.

***Index Terms*—Blockchain, Cryptography, QR code, Fraud prevention, Merkle tree**

I. INTRODUCTION

A. Overview

Academic credential fraud undermines educational integrity and erodes employer confidence. Manual verification processes are slow, fragmented, and vulnerable to manipulation.

Existing frameworks like the Digital Locker Technology Framework (MeitY) and blockchain systems such as Cerberus and EduCTX address this partially but suffer from scalability and interoperability issues.

The proposed system leverages permissioned blockchain, digital signatures, and QR-based validation to streamline student accreditation and verification processes. Each issued certificate is recorded on-chain, allowing verifiers to validate authenticity by scanning the QR code printed on it.

B. Motivation

The need for a secure, transparent, and interoperable system for academic verification arises from the growing number of fake certificates in circulation, Time-consuming manual verification processes.

The project aims to address these issues through blockchain-enabled transparency, ensuring institutions and employers can verify certificates instantly and confidently.

C. Problem Definition

To design and implement a Blockchain-Based Student Accreditation and Credential Verification System that:

- Enables universities to issue digitally verifiable certificates.
- Allows students to hold QR-embedded credentials.

- Provides verifiers with instant authenticity and issuer validation.

II. BACKGROUND AND FUNDAMENTAL CONCEPTS

A. Blockchain Technology

Blockchain is a decentralized, distributed, append-only ledger maintained by a group of peers on a common network, where all the transactions taking place on the network are transparent and permanent. This technology consists of blocks connected to each other with the help of previous block's information and cryptographic hashing. This chain of reference makes blockchain tamper-proof. The network, being decentralized, has no central authority to govern or overlook the entire transactions or operations. Every node on the network has a copy of the transactions, making verification of false claims easier.

B. Document Frauds

Document fraud is the falsifying, altering or misinterpreting of education credentials with the hope of achieving a unfair advantage in educational progress. Some of the most commonly frauded documents are entirely fabricated diplomas or certificates, modifying dates, grades, content in legitimate documents, forged seals and so on. Over the years, this is an issue that is persistent, despite the various methods and policies implemented to eradicate this form of corruption.

C. Merkle Tree

Merkle tree, also known as a hash tree, is a data structure similar to a binary tree where each leaf of the tree is a cryptographic hash of a data block. Each internal node is the hash of its children. The root hash summarizes the entire data present in the tree. Merkle tree allows for easier tamper detection as any change made in any of the intermediate or leaf nodes affects the root hash of the tree. This is a simple property of hash function, where hash of a particular word/sentence is constant. The Merkle tree provides a secure and compact summary of all the data, due to which it sees a lot of its implementation in blockchain.

D. Smart Contracts

Smart Contracts are self-executing pieces of code that are in terms directly with the lines of code written in them. It automatically verifies and enforces the performance of the contract, without the need of intermediaries. Despite the complex appearance, smart contracts work on the simple principle of 'if/then' logic. Some of the popular languages to write smart contracts are Solidity, which is widely used in Ethereum and EVM-compatible blockchains, Rust, Vyper.

E. Consensus

Consensus is the process of mutual agreement on the state of the ledger among the nodes in a distributed blockchain network. Meaning they agree on a single process to decide which transactions are valid and in what order they occurred. This is necessary since there is no central authority to govern transactions or decide what is absolute. A good consensus algorithm ensures Agreement, Validity, Fault Tolerance, Finality, Liveness. Some of the major consensus mechanisms are Proof of Work, Proof of Stake, Proof of Authority.

III. LITERATURE REVIEW

A. Review of Existing Systems

The digitalization of academic records has prompted the development of various document management and verification frameworks. Each existing system addresses parts of the verification process but fails to provide a comprehensive, interoperable, and scalable solution.

1) Digital Locker Framework (MeitY, 2017): India's Digital Locker provides a secure online repository for storing and sharing electronic documents verified by issuing authorities. Although it supports digital signatures and government validation, it remains centralized, dependent on Aadhaar-based authentication, and lacks real-time revocation and cross-institutional interoperability.

2) Cerberus (NUST, 2019): Cerberus employs blockchain technology and Merkle trees to store degree information on-chain, ensuring immutability and verifiability through QR codes. However, its on-chain implementation is complex, not easily scalable, and requires technical knowledge for operation and maintenance, which limits adoption by universities.

3) EduCTX (University of Maribor, 2017): EduCTX introduced a decentralized academic credit system using a Delegated Proof of Stake (DPoS) blockchain model, representing student credits as ECTX tokens. While effective for academic credit transfer, it does not verify degree authenticity or issuer legitimacy, making it unsuitable for global credential verification.

4) Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) – W3C Standards (2021): DIDs and VCs promote self-sovereign identity (SSI) by enabling credential interoperability and privacy-preserving verification. However, widespread adoption is hindered by high technical complexity, need for key management, and limited institutional readiness for decentralized identity integration.

B. Comparative Analysis of Existing Systems

- Digital Locker: Centralized, Government portal, No blockchain; single-point control
- Cerberus: Public Blockchain, QR + Merkle Tree, Complex implementation; scalability issues
- EduCTX: DPoS Blockchain, Token-based Credit Transfer, Not for credential verification
- DIDs & VCs: Decentralized Identity, Cryptographic Proof, Technically complex; user key management

C. Gaps Identified in Existing Work

- Centralized Control: Most systems rely on central authorities or servers, creating single points of failure.
- Limited Interoperability: No unified schema or protocol connects universities, verifiers, and accreditation bodies.

- Lack of Revocation Mechanism Implementation: Revocation mechanism is only mentioned in theory and not practice.
- Poor Usability: Blockchain-based systems demand wallet setup or cryptographic expertise.
- Verification Delays: Manual processes and dependency on institutional approvals slow down verification.
- Lack of Transparency: Verifiers cannot independently validate issuer authenticity.
- Blockchain Awareness: Lack of awareness about blockchain technology in day-to-day systems.

D. Motivation for Proposed System

The gaps identified across Digital Locker, Cerberus, and EduCTX directly inspired the design of the Blockchain-Based Student Accreditation and Credential Verification System.

The motivation lies in creating a decentralized yet user-friendly verification network that ensures:

- Immutability: Through cryptographic hashing and blockchain storage of credentials.
- Transparency: Every certificate and issuing authority is verifiable on a shared ledger.
- Usability: Students and verifiers can perform checks using a simple QR code scan, without requiring knowledge of blockchain.
- Privacy & Compliance: Only hashed or anonymized data is stored on-chain, maintaining confidentiality and legal compliance.
- Institutional Accountability: Revocation and audit trails ensure institutional responsibility for every issued credential.

Thus, the proposed model integrates blockchain's immutability, digital signature security, and QR-based accessibility to deliver a scalable, interoperable, and tamper-proof academic verification ecosystem, addressing all major deficiencies found in prior frameworks.

IV. SYSTEM ARCHITECTURE

The proposed blockchain-based credential verification system follows a modular, multi-layered architecture that integrates on-chain smart contracts, off-chain storage, and web-based interfaces. The architecture ensures immutability, security, and efficiency by dividing responsibility across four primary layers: the User Interface Layer, Application Layer, Blockchain Layer, and Off-Chain Storage Layer.

A. Overview of Architecture

The overall system architecture comprises:

- User Interface Layer
- Application / Middleware Layer
- Blockchain Layer
- Off-Chain Storage Layer (IPFS)

Each layer performs a distinct function, ensuring secure certificate issuance, transparent verification, and reliable revocation mechanisms.

B. User Interface Layer

This layer contains all user-facing modules built using React.js, HTML, CSS, and JavaScript. It provides simple and intuitive workflows for different stakeholders.

1) Issuer Portal: Used by universities and institutions to upload, sign, and issue certificates. It maintains issuance history and student credential logs.

2) Student Dashboard: Allows students to view, download, and share their digital certificates. QR-based sharing is supported for quick verification.

3) Verifier Interface: Enables employers and academic institutions to verify certificates through QR scanning. Verification results include Valid, Invalid, or Revoked.

4) Accreditation Authority Panel: Used to approve and register new issuers. Ensures only trusted institutions can participate in certificate issuance.

C. Application / Middleware Layer

This layer implements server-side logic, handles smart contract calls, and secures system operations. It is built using Node.js, Express.js, and Web3.js.

1) API Gateway: Processes certificate issuance, verification, and revocation requests from the frontend.

2) Smart Contract Interaction Module: Handles low-level blockchain communication and executes contract functions for storing and verifying credentials.

3) Role-Based Access Control: Ensures only authorized roles (Issuer, Verifier, Student, Accreditation Authority) access specific functionalities.

4) Hashing and Encryption Engine: Computes SHA-256 hashes of certificate files before blockchain storage. Ensures any modification is immediately detectable.

5) Audit and Logging Service: Maintains transaction logs for compliance, tracking changes, and supporting verifiability.

D. Blockchain Layer (On-Chain Components)

A permissioned blockchain network forms the trust backbone of the system, providing tamper-proof storage and decentralized verification.

1) Credential Smart Contract: Stores certificate hashes and metadata. Supports issueCredential(), verifyCredential(), and revokeCredential() functions.

2) Issuer Registry Smart Contract: Maintains a list of verified issuers and public keys. Prevents unauthorized certificate creation.

3) Revocation Contract: Allows authorized nodes to revoke certificates. Updated revocation status reflects instantly during verification.

4) Consensus Mechanism: Uses PBFT or PoA for fast, deterministic finality suited for institutional networks.

5) QR-Based Verification: Each issued certificate includes a QR code containing the blockchain transaction hash or credential ID. Scanning retrieves on-chain data for authenticity checks.

E. Off-Chain Storage Layer (IPFS)

Certificate files are stored in the InterPlanetary File System (IPFS) to avoid blockchain overhead.

1) IPFS Storage Node: Stores original certificate documents in a decentralized manner. Provides permanent access via a content identifier (CID).

2) CID Mapping: Only the CID and necessary metadata are stored on-chain. Enhances privacy and reduces transaction cost.

3) Integrity Verification: During verification, the uploaded certificate is hashed again and checked against the stored CID. Any mismatch indicates tampering.

F. End-to-End Data Flow

1) Certificate Issuance: Issuer uploads file → SHA-256 hash generated → Certificate stored on IPFS → CID recorded on blockchain → QR code generated and attached to certificate.

2) Certificate Verification: Verifier scans QR → Hash retrieved from blockchain → Local hash computed → If both match, certificate is valid.

3) Revocation: Issuer or Accreditation Authority invokes smart contract → Certificate marked as Revoked → Updated status shown in verification portal.

G. Architectural Advantages

- Immutability: Certificates stored on blockchain cannot be altered.
- Real-Time Verification: QR scanning provides instant authenticity checks.
- Privacy Preservation: Only hashes stored on-chain; personal data remains off-chain.
- Decentralized Trust: Removes reliance on a central verification authority.
- Scalability: IPFS combined with permissioned blockchain supports large-scale deployment.

V. PROPOSED CREDENTIAL VERIFICATION MODEL

The system component architecture illustrates the interaction between four primary layers: the User Interface Layer, the Application Layer, the Blockchain Layer, and the Off-Chain Storage Layer. At the top of the architecture, user entities such as the Issuer, Student, Verifier, and Accreditation Authority interact through dedicated web portals. These interfaces transmit requests to the Application Layer, which consists of the API Gateway, Smart Contract Interaction Module, Hashing Engine, and Role-Based Access Control. This layer processes certificate issuance, revocation, and verification requests before directing them to the blockchain.

The Blockchain Layer contains smart contracts that store certificate metadata, issuer identities, and revocation information. It operates on a permissioned blockchain using PBFT or PoA consensus to ensure tamper-proof and transparent credential storage. Each issued certificate is assigned a blockchain transaction hash and linked to a QR code for real-time verification. Only the certificate hash and metadata are stored on-chain.

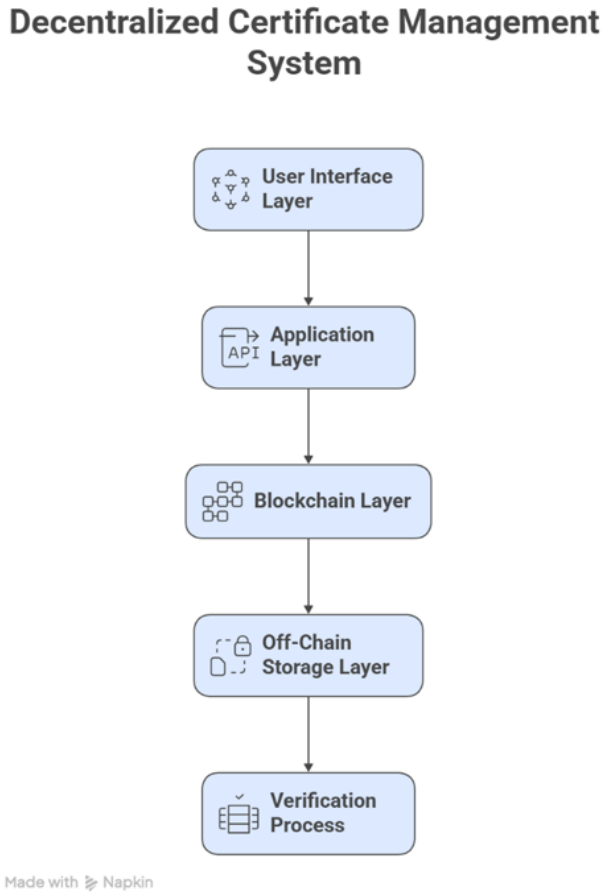

Fig. 1. System Component Architecture of the Proposed Credential Verification Model

The Off-Chain Storage Layer, implemented using IPFS, stores the original certificate documents in decentralized storage. IPFS generates a unique Content Identifier (CID) for each file, which is recorded on the blockchain for integrity verification. During verification, the certificate uploaded by the verifier is hashed and compared against the CID stored in the blockchain. A match confirms authenticity; a mismatch indicates tampering or forgery.

The architecture demonstrates a secure end-to-end workflow where certificate issuance, storage, and verification are handled in a decentralized, tamper-resistant, and privacy-preserving manner. It ensures seamless communication between users and the underlying blockchain through the middleware layer, providing efficient and transparent academic credential validation.

VI. ARCHITECTURAL OVERVIEW

The proposed blockchain-based credential verification system is designed as a modular, multi-layered architecture that integrates smart contracts, off-chain storage, and web-based

interfaces to provide secure, verifiable, and tamper-proof academic credentials. The architecture is divided into four main layers: the User Interface Layer, the Application Layer, the Blockchain Layer, and the Off-Chain Storage Layer. Each layer is responsible for specific system operations and communicates seamlessly through secure APIs and smart contract calls.

A. Layer 1: User Interface Layer

This layer provides the entry point for all system users. It delivers browser-based interfaces for certificate issuance, verification, and access.

1) Issuer Portal: Used by verified educational institutions to create, digitally sign, and upload student certificates. It ensures controlled issuance and maintains institutional transaction history.

2) Student Dashboard: Allows students to view, download, and share their issued certificates. It also provides QR-based sharing for easy verification.

3) Verifier Interface: Enables employers and academic institutions to authenticate certificates by scanning the QR code or uploading the certificate file for validation.

4) Accreditation Authority Panel: Used by the governing authority to register and approve institutions, manage issuer permissions, and maintain overall trust across the network.

B. Layer 2: Application / Middleware Layer

This layer handles the business logic, security controls, and blockchain interactions. It is implemented using Node.js, Express.js, and Web3.js libraries.

1) API Gateway: Processes certificate issuance, verification, and revocation requests submitted from the user interfaces.

2) Smart Contract Handler: Executes blockchain transactions, interacts with deployed smart contracts, and retrieves on-chain data for verification.

3) Role-Based Access Control (RBAC): Ensures that only authorized users (issuer, verifier, accreditation authority) can perform restricted operations.

4) Hashing Engine: Computes SHA-256 hashes of certificate files and metadata before submitting them to the blockchain.

5) Logging and Audit Module: Stores logs of all issuance and verification events to ensure traceability and compliance.

C. Layer 3: Blockchain Layer

This is the core trust layer of the system. A permissioned blockchain network ensures tamper-proof and transparent credential storage.

1) Credential Smart Contract: Stores certificate hashes and metadata. Provides functions for issuing, revoking, and verifying credentials.

2) Issuer Registry Contract: Maintains a list of trusted institutions. Only registered issuers are allowed to upload or revoke certificates.

3) Revocation Contract: Allows authorized entities to revoke issued certificates, ensuring that invalid credentials are instantly flagged during verification.

4) Consensus Layer: Uses PBFT or PoA consensus mechanisms to achieve fast, deterministic transaction finality suitable for multi-institution environments.

5) QR-Based Verification: Each certificate includes a QR code that contains its blockchain transaction ID or credential identifier. Verification retrieves this on-chain record and compares it with the uploaded file.

D. Layer 4: Off-Chain Storage Layer (IPFS)

Due to blockchain's limited storage capacity, actual certificate files are stored in IPFS.

1) IPFS Node: Stores full certificate documents and generates a unique Content Identifier (CID) using SHA-256.

2) CID Mapping: Only the CID and certificate metadata are stored on the blockchain, ensuring privacy, scalability, and low transaction costs.

3) Integrity Verification: During verification, the uploaded certificate is re-hashed and compared against the stored CID. Any mismatch indicates modification or forgery.

E. Layer 5: End-to-End Workflow

- Issuer uploads certificate → File hashed → Stored in IPFS → CID registered on blockchain → QR code generated.
- Verifier scans QR → System retrieves blockchain record → Compares stored hash with computed hash → Returns validity status.
- Issuer or authority can revoke a certificate → Smart contract updates revocation status → Reflected instantly in the verification portal.

VII. USE CASE DIAGRAM AND FUNCTIONAL ANALYSIS

The use case diagram illustrates the major interactions between system actors and the CredHub platform. It captures how universities, accreditation bodies, and employers/verifiers interact with the credential issuance, verification, and revocation components of the system. The diagram highlights the core functionalities required to ensure secure issuance, transparent verification, and controlled revocation of academic credentials.

A. Use Case Diagram Description

The CredHub system consists of three external actors—University, Accreditation Body, and Employer/Verifier. Each actor performs specific operations as shown in the use case diagram.

1) University: The university is responsible for issuing academic credentials and initiating revocation requests when needed. Its use cases include:

- Issue Batch: Uploading a new batch of student credentials.

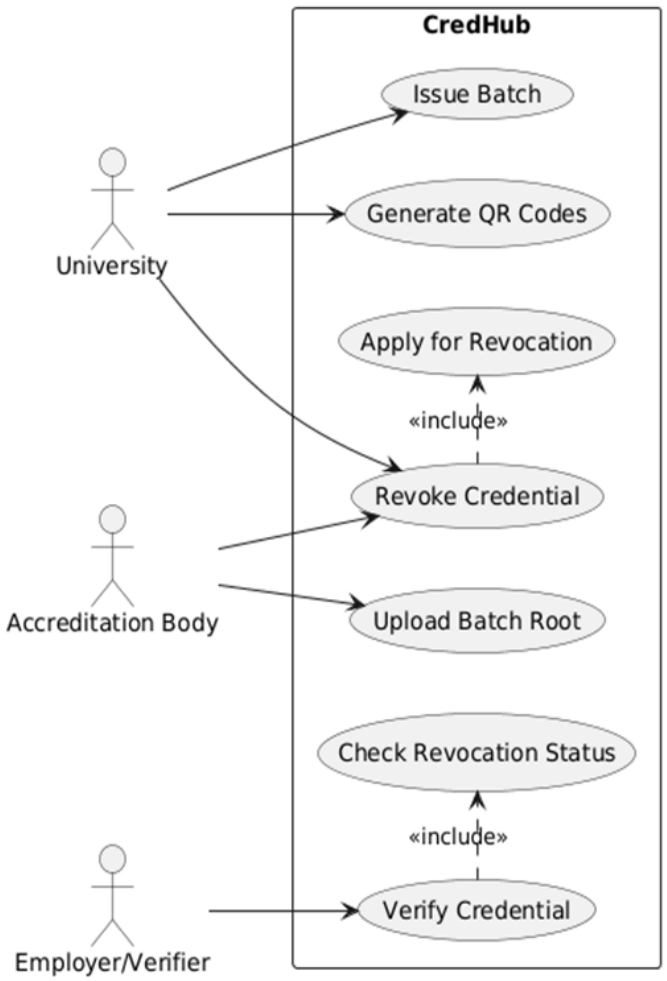

Fig. 2. Use Case Diagram

- Generate QR Codes: Generating QR codes linked to blockchain transaction IDs for verification.
- Apply for Revocation: Initiating a request to revoke a specific credential.
- Revoke Credential: Included in the revocation workflow, subject to approval.

2) Accreditation Body: The accreditation body validates university actions and manages trust within the ecosystem. Its use cases include:

- Upload Batch Root: Validating and registering the batch root hash on the blockchain.
- Revoke Credential: Approving and finalizing revocation requests from universities.

3) Employer / Verifier: The employer or third-party verifier checks the authenticity and current status of a credential. Its use cases include:

- Verify Credential: Verifying the certificate using the QR code or transaction ID.
- Check Revocation Status: Included within the verification process to ensure the credential is still valid.

The use case diagram also includes two `<<include>>` relationships:

- Apply for Revocation includes Revoke Credential.
- Verify Credential includes Check Revocation Status.

This ensures revocation is validated through accreditation authority approval and credential verification always checks the latest revocation status.

B. Functional Scenarios

The following scenarios describe how actors interact with CredHub in real-world workflows.

1) Scenario 1: Issuing a Batch of Credentials: The university compiles student records and uploads them as a batch. The system computes a Merkle root and forwards it to the accreditation body for validation. Once approved, the batch is committed to the blockchain, and QR codes are generated for each credential.

2) Scenario 2: Verifying a Credential: An employer scans the QR code on a student's certificate. The system retrieves the corresponding transaction metadata, verifies the stored hash, and checks the revocation status. If the hash matches and the credential is not revoked, the certificate is marked Valid.

3) Scenario 3: Applying for Credential Revocation: If a credential must be revoked (due to fraud, administrative error, or disciplinary action), the university submits a revocation request. The system routes the request to the accreditation body, which verifies the justification and executes the revocation on-chain using the Revoke Credential use case.

4) Scenario 4: Uploading Batch Root for Validation: For every batch of issued credentials, the university sends the batch root hash to the accreditation authority. The accreditation body verifies institutional legitimacy and records the batch root hash on-chain, enabling decentralized validation by verifiers.

5) Scenario 5: Checking Revocation Status: During verification, the system automatically checks if the credential has been revoked. Employers do not need separate queries, as the revocation check is included within the verification workflow.

VIII. CHALLENGES

1) **Revocation Mechanism Complexity**
   The system also proposes the implementation of a multi-party revocation mechanism. The implementation part if an advancement and improvement from the previous systems. However, since there is a requirement of multiple nodes to cooperate with each other, it may increase complexity and pose implementation challenges.
2) **Large Scale Integration and Adoption**
   Despite the efforts of making this system being able to integrate closely with existing credential verification systems, widespread adoption could be hindered with government collaboration being a major challenge.
3) **Scalability and Blockchain Overhead**
   Since the system uses a permissioned blockchain with merkle trees to improve scalability, with the increase

in transactions on the blockchain, the network's performance and storage overhead management remain a challenge.

4) **Dependence on Trusted Entities**
While the system decentralizes verification through blockchain, it still relies on trusted accreditation bodies and universities to enter authentic data. Insider threats or collusion at these levels could pose risks to system integrity.
5) **Offline Verification Limitations**
Verification relies on network access to the blockchain to confirm credential status and revocation. Offline verification or low-connectivity scenarios may be difficult to support seamlessly.

IX. FUTURE SCOPE AND IMPROVEMENTS

While the current model aims to deliver a secure and efficient verification framework, several enhancements can extend its functionality and adaptability in real-world environments.

1) Integration with National Digital Identity Frameworks:
The system can be connected to platforms such as Aadhaar or DigiLocker APIs for seamless authentication of issuers and users.
2) Adoption of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs):
Incorporating W3C-compliant DIDs and VCs can enable global interoperability and self-sovereign identity management.
3) Mobile Application for Instant Verification:
A mobile app can be developed for students and employers to issue, store, and verify credentials offline through secure QR scanning.
4) AI-Based Fraud Detection:
Machine learning models can be integrated to detect suspicious issuer behavior, duplicate credentials, or anomalous verification requests.
5) Cross-Border Credential Recognition:
Collaborations with international universities and accrediting bodies can establish a global academic credential exchange network.
6) Integration with Cloud and Edge Infrastructure:
Implementing cloud-based node hosting or edge verification servers can improve system availability and speed for large-scale deployment.

X. CONCLUSION

The proposed Blockchain-Based Student Accreditation and Credential Verification System successfully addresses the long-standing challenges of document authenticity, verification delays, and data integrity in academic ecosystems.

By integrating blockchain technology, digital signatures, and QR code-based verification, the system ensures that each credential issued by an institution is tamper-proof, transparent, and instantly verifiable. The adoption of a permissioned blockchain model maintains both scalability and institutional control, while the revocation mechanism powered by smart contracts guarantees that revoked or invalid credentials are detected immediately.

Unlike existing centralized solutions such as Digital Locker or partially decentralized systems like Cerberus and EduCTX, the proposed framework offers a balanced hybrid approach — combining blockchain immutability with user-friendly design and privacy-aware data management.

This system demonstrates the potential to transform traditional verification workflows by:

- Eliminating dependency on manual traditional systems.
- Providing verifiers with real-time authenticity checks.
- Enhancing institutional trust through transparent blockchain audit trails.
- Preserving user privacy by storing only credential hashes on-chain.

Overall, the system lays a strong foundation for secure digital credential management and represents a major step toward establishing trusted academic ecosystems aligned with future digital identity frameworks.

XI. REFERENCES

REFERENCES

[1] MeitY, *Digital Locker Technology Framework v1.1*, Ministry of Electronics and Information Technology, Government of India, 2017. (Reference for centralized document repository framework and government-grade credential storage.)

[2] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1503–1514, 2022. (Used as reference for blockchain credential verification using Merkle trees and smart contracts.)

[3] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018. (Source for tokenized academic credit models and distributed peer-to-peer education networks.)

[4] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model 1.0," *W3C Recommendation*, 2019. (Defines the global model for issuing and verifying digital credentials based on cryptographic proofs.)

[5] D. Reed et al., "Decentralized identifiers (DIDs) v1.0," Draft Community Group Report, 2020. (Provides standards for decentralized identity management and blockchain-linked verification systems.)

[6] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017. (Reference for blockchain privacy models and cryptographic data protection principles.)

[7] C. Mazzocca et al., "A survey on decentralized identifiers and verifiable credentials," *IEEE Communications Surveys & Tutorials*, 2025. (Survey reference for DIDs and VCs applications in identity and trust frameworks.)

[8] Government of India, *Information Technology Act, 2000 (Amended 2008)*, Ministry of Law and Justice, New Delhi. (For data protection, digital signature, and legal recognition of electronic records.)

[9] European Parliament, *General Data Protection Regulation (GDPR)*, 2018. (For compliance with data privacy and off-chain encryption standards.)

[10] Hyperledger Foundation, *Hyperledger Fabric Documentation*, Linux Foundation, 2024. (Technical reference for implementing permissioned blockchain and smart contract-based access control.)