# ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh

Ahsan Farabi
*Dept. of CSE*
*United International University*
Dhaka, Bangladesh
afarabi221266@bscse.uiu.ac.bd

Israt Khandaker
*Dept. of CSE*
*United International University*
Dhaka, Bangladesh
ikhandaker221263@bscse.uiu.ac.bd

Jayed Ahsan
*Dept. of CSE*
*United International University*
Dhaka, Bangladesh
jahsan221125@bscse.uiu.ac.bd

Ibrahim Khalil Shanto
*Dept. of CSE*
*United International University*
Dhaka, Bangladesh
ishanto213193@bscse.uiu.ac.bd

Nusrat Jahan
*Dept. of CSE*
*United International University*
Dhaka, Bangladesh
njahan221323@bscse.uiu.ac.bd

Md. Jarif Khan
*Dept. of CSE*
*BRAC University*
Dhaka, Bangladesh
md.jarif.khan@g.bracu.ac.bd

*Abstract*—Academic credential fraud threatens educational integrity, especially in developing countries like Bangladesh, where verification methods are primarily manual and inefficient. To address this challenge, we present ShikkhaChain—a blockchain-powered certificate management platform designed to securely issue, verify, and revoke academic credentials in a decentralized and tamper-proof manner. Built on Ethereum smart contracts and utilizing IPFS for off-chain storage, the platform offers a transparent, scalable solution accessible through a React-based DApp with MetaMask integration. ShikkhaChain enables role-based access for governments, regulators, institutions, and public verifiers, allowing QR-based validation and on-chain revocation tracking. Our prototype demonstrates enhanced trust, reduced verification time, and improved international credibility for Bangladeshi degrees, promoting a more reliable academic and employment ecosystem.

*Index Terms*—Blockchain, Smart Contracts, Educational Certificates, IPFS, Verification System, Decentralized Applications

## I. INTRODUCTION

Verifying academic credentials is a cornerstone of trust in education and employment systems. In Bangladesh, however, verification remains dominated by manual and paper-based processes that are slow, inefficient, and vulnerable to forgery. The absence of robust digital infrastructure has led to credential fraud, delays in recruitment, and reduced international credibility of Bangladeshi degrees. A scalable, tamper-resistant mechanism for issuing and validating certificates is therefore essential to strengthen both domestic and global trust in the education system.

Recent studies have explored blockchain-based approaches to credential management, demonstrating benefits such as immutability, decentralization, and transparency [1]–[3]. Yet significant gaps persist: existing systems often lack role-aware governance (e.g., distinguishing governments, regulators, institutions, and public verifiers), overlook integration with decentralized storage like IPFS for scalability, and rarely align with localized regulatory and infrastructural needs. These

limitations reduce their applicability in national contexts such as Bangladesh.

To address these challenges, we present **ShikkhaChain**, a blockchain-powered credential verification system tailored for Bangladesh. ShikkhaChain leverages Ethereum smart contracts to issue, verify, and revoke certificates, while IPFS provides decentralized off-chain storage linked by on-chain content identifiers (CIDs). A React-based decentralized application (DApp) with MetaMask integration offers secure, role-based access for government authorities, regulators, institutions, graduates, and employers. The system ensures transparent, tamper-proof, and efficient verification, promoting greater trust in both academic and employment ecosystems.

The main contributions of this paper are as follows:

- Design of a role-aware, layered architecture that integrates government, regulator, institutional, and public roles for transparent credential governance.
- Development of Ethereum smart contracts that support certificate issuance, verification, and revocation with event-driven off-chain indexing.
- Integration of IPFS for scalable and tamper-resistant off-chain storage linked to on-chain records.
- Implementation of a functional prototype featuring a React-based DApp with QR code and hash-based verification.
- Comparative analysis with prior blockchain-based systems, highlighting improvements in role-awareness, revocation, and transparency.

The remainder of this paper is structured as follows: Section II reviews related work on blockchain credential systems. Section III presents the system architecture and design. Section IV details the prototype results and comparative analysis. Section V discusses security and trust features. Section VI outlines limitations and future directions. Section VII concludes the paper.

## II. RELATED WORK

The application of blockchain in higher education has gained momentum due to its potential for data integrity, decentralized trust, and streamlined credential verification. We group prior work into: (i) credential verification systems, (ii) decentralized frameworks and IPFS integration, (iii) governance and access control, and (iv) smart-contract implementations.

### A. Credential Verification and Academic Trust

Blockchain has been widely adopted to establish trust and prevent tampering in educational credentials. Centeno and Palaoag [4] designed a prototype for blockchain-based degree verification. Xu [5] proposed a decentralized credential authentication framework to reduce fraud. Shivarkar [6] proposed a decentralized digital certification system replacing paper-based certificates. Nguyen and Lin [7] developed EduLedger for decentralized transcripts. These solutions demonstrate security benefits but often overlook stakeholder role differentiation and modular policy integration.

### B. Systematic Reviews and Global Implementations

Silaghi and Popescu [8] reviewed blockchain initiatives in higher education, highlighting scalability and regulatory adoption gaps. De Alwis et al. [9] emphasized governance for accreditation. Country-specific case studies include a UAE national platform [10] and BlockMEDC for Moroccan institutions [11], which show feasibility yet limited generalizability and standardized role-based governance.

### C. Decentralization, IPFS, and Data Provenance

Decentralized storage like IPFS mitigates centralized failures. Rahman et al. [1] combined Ethereum and IPFS for tamper-resistant records; Ahmad and Lee [12] proposed TrustChainEdu (IPFS–blockchain hybrid). Nasir and Bukhari [13] linked IPFS with on-chain proof for provenance. These works evolve secure architectures but do not address policy-level differentiation between ministries, universities, and employers—addressed in our design.

### D. Smart Contracts, Revocation, and Role-Based Access

Smart contracts enable automated issuance and revocation. Park and Zhang [2] introduced BlockCerts+ with revocation; Mohapatra and Sen [14] designed SmartCertEdu embedding issuance, storage, and verification with IPFS; Habib et al. [3] proposed CredSec for stakeholder-friendly access; Flanery et al. [15] framed learner-centered Web3 credential control. Gaps remain in integrating role-aware contracts, regulator-controlled institution lists, and publicly verifiable yet privacy-preserving records—gaps addressed by ShikkhaChain.

## III. SYSTEM ARCHITECTURE AND DESIGN

ShikkhaChain is designed to issue, verify, and revoke academic certificates using blockchain and Web3 technologies. The architecture is modular, layered, and role-based, ensuring scalability, policy enforcement, and decentralized trust (Fig. 1). In addition, the workflow for issuance and verification is illustrated in Fig. 2.

### A. Stakeholder Roles

The system defines distinct roles to establish governance, accountability, and role-based access:

- **Government:** Acts as the root authority, responsible for onboarding regulators, setting national policies, and overseeing compliance across the ecosystem.
- **Regulators:** Serve as intermediaries, maintaining an up-to-date registry of authorized institutions, enforcing issuance policies, and auditing institutional activities.
- **Institutions:** Universities and colleges authorized by regulators can issue new certificates or revoke fraudulent/invalid ones. They interact directly with the smart contracts.
- **Public (Graduates/Employers):** Graduates present verifiable digital certificates to employers, while employers or any verifier can check authenticity through the DApp using a QR code or hash.

This stakeholder model ensures hierarchical trust delegation, where control flows from the government down to the end-users without a central database.

### B. System Layers

The layered architecture separates responsibilities to achieve modularity and extensibility:

1) **User Layer:** Provides browser-based interaction through a React.js interface, with MetaMask wallet integration for authentication and transaction signing.
2) **Application Layer:** Implements dashboards for different roles (government, regulator, institution, public). It manages certificate requests, verification results, and revocation operations, ensuring a user-friendly interface.
3) **Access Layer:** Handles blockchain connectivity using Web3.js and ethers.js. This layer supports communication with Ethereum nodes via providers such as Infura or Alchemy and ensures secure MetaMask wallet connectivity.
4) **Blockchain Layer:** Contains the Ethereum smart contracts that encode core logic for certificate issuance, verification, and revocation. State changes (e.g., a revoked certificate) are immutable and transparent.
5) **Off-chain Storage Layer:** Stores certificate metadata (e.g., graduate name, institution, degree type) on IPFS. The content identifier (CID) is stored on-chain, providing both scalability and tamper-resistance.

This separation of concerns improves maintainability and supports future upgrades such as Layer-2 migration.

### C. Smart Contract Design

ShikkhaChain's smart contracts implement fine-grained access control and certificate lifecycle management:

- `issueCertificate()`: Called by an authorized institution to issue a certificate. The metadata CID is recorded on-chain, and an event is emitted for off-chain indexing.
- `verifyCertificate()`: Publicly accessible function to validate whether a certificate hash corresponds to a registered CID and has not been revoked.
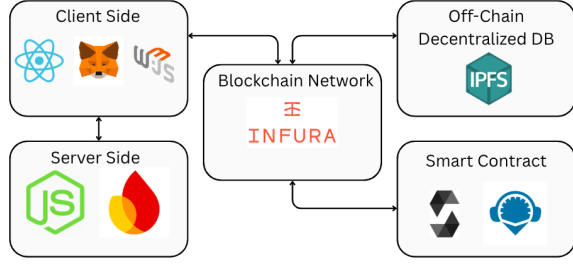
Fig. 1. Layered system architecture of ShikkhaChain, illustrating stakeholder roles, blockchain/IPFS integration, and modular access layers.
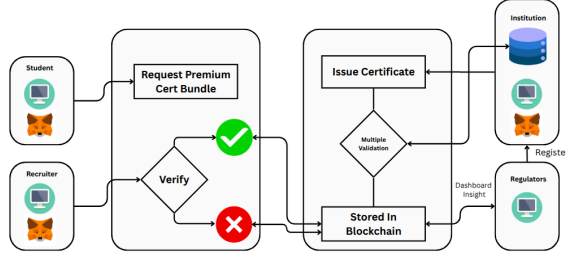


Fig. 2. Workflow of certificate issuance and verification in ShikkhaChain. Institutions issue credentials, which are stored on IPFS and linked on-chain, while verifiers confirm authenticity through the DApp.

- `revokeCertificate()`: Invoked by authorized institutions to mark a certificate as invalid. The status change is recorded immutably on-chain.

Contracts enforce role checks at runtime, ensuring only permitted entities can perform sensitive actions. Additionally, emitted events (e.g., `CertificateIssued`, `CertificateRevoked`) enable external services to build audit trails and analytics.

### D. Verification Process

The verification workflow is designed to be lightweight and user-friendly:

1) The verifier scans the certificate QR code or inputs the certificate hash into the DApp.
2) The DApp retrieves the associated metadata CID from the blockchain.
3) Using the CID, the DApp fetches the certificate metadata stored on IPFS.
4) The smart contract is queried to check certificate status (valid, revoked, or not found).
5) The system displays verification results, including certificate details, issuer, and current status.
6) Optionally, the verified result can be exported as a digitally signed PDF using jsPDF, suitable for archiving or submission to external parties.

This process eliminates manual verification delays and ensures real-time authenticity checks without dependence on centralized authorities.

## TABLE I
## COMPARISON OF BLOCKCHAIN-BASED CREDENTIAL SYSTEMS

| System | Storage | Role Access |
|---|---|---|
| **ShikkhaChain** | IPFS + on-chain CID | 4 Major Roles |
| Verifi-Chain [1] | IPFS | No roles |
| BlockCerts+ [2] | On-chain hash + local file | Issuer-only |
| CredSec [3] | IPFS | Admin, Issuer, Verifier |
| BlockMEDC [11] | IPFS | No roles |

## IV. RESULTS AND COMPARATIVE ANALYSIS

We implemented a prototype of **ShikkhaChain** using React.js for the decentralized application (DApp), Solidity smart contracts on the Ethereum Goerli test network, and IPFS for off-chain storage. MetaMask was used for secure wallet-based authentication and transaction signing.

### A. Functional Outcomes

The prototype successfully demonstrated the complete lifecycle of academic certificates:

- **Issuance:** Authorized institutions upload certificate metadata to IPFS. The generated content identifier (CID) is immutably stored on-chain through a smart contract.
- **Verification:** Employers or public users validate certificates by entering a hash or scanning a QR code. The system fetches the CID from the blockchain, retrieves metadata from IPFS, and confirms the certificate's validity.
- **Revocation:** Institutions revoke compromised or invalid certificates through `revokeCertificate()`, and the updated status is recorded immutably on-chain.
- **Export:** Verified results can be exported as digitally signed PDFs for archiving or external submission.

### B. Comparative Feature Analysis

Table I highlights the differences between ShikkhaChain and representative blockchain-based credential systems. While prior systems provide decentralized storage and verification, they typically lack role differentiation and on-chain revocation tracking. ShikkhaChain uniquely integrates:

1) **Role-aware access control** across four distinct stakeholders (government, regulator, institution, public).
2) **IPFS-backed storage** with on-chain CIDs for scalability and tamper-resistance.
3) **On-chain revocation** that ensures transparent invalidation of compromised certificates.

### C. Performance Insights

Performance evaluation on the Goerli Ethereum test network showed the following:

- **Transaction Time:** 12–25 seconds per transaction, depending on network congestion.
- **Gas Cost:** Approximately $\sim 1,289,600$ gas units to issue a certificate. On Ethereum mainnet, this would incur significant cost, motivating adoption of Layer-2 solutions.
- **IPFS Latency:** 1–5 seconds for metadata retrieval, influenced by pinning and gateway reliability.

These results confirm the feasibility of ShikkhaChain, while also indicating that scaling to production environments would benefit from optimizations such as Layer-2 deployment, dedicated IPFS pinning, or a permissioned blockchain for national-level adoption.

## V. Security and Trust Features

- **Immutability:** Blockchain anchoring ensures tamper-resistance.
- **Content Integrity:** IPFS CIDs guarantee file integrity.
- **Transparency:** Public verification without intermediaries.
- **Decentralized Access:** Wallet-based authentication; no central DB of secrets.

## VI. Discussion and Limitations

Although the prototype demonstrates the feasibility of ShikkhaChain, several limitations remain that must be addressed for production-scale adoption:

- **On-chain cost and latency:** Transactions on the Ethereum mainnet incur high gas costs and confirmation delays. While acceptable for a prototype, large-scale deployment would require migration to Layer-2 solutions or permissioned blockchains.
- **IPFS availability:** Certificate metadata retrieval depends on IPFS pinning and gateway reliability, which may cause delays or temporary inaccessibility in practice.
- **Governance bootstrapping:** The hierarchical model requires effective onboarding of regulators and institutions. Without proper adoption and compliance enforcement, the trust model may weaken.
- **Privacy concerns:** Current design exposes certificate metadata publicly once the CID is known. Privacy-preserving verification (e.g., via zk-SNARKs) is needed to protect sensitive details while still proving authenticity.
- **Integration challenges:** ShikkhaChain currently functions as a standalone prototype. Standardized APIs and interoperability with national e-Governance systems would be necessary for real-world deployment.

## VII. Conclusion and Future Work

This paper presented **ShikkhaChain**, a blockchain-powered credential verification system for Bangladesh. By combining Ethereum smart contracts, IPFS storage, role-aware access, and QR-enabled verification, the system ensures secure issuance, transparent validation, and immutable revocation of academic certificates. Comparative analysis shows that ShikkhaChain advances prior solutions through multi-tiered stakeholder roles and on-chain revocation tracking.

Future work will focus on: (i) scalability via Layer-2 or permissioned networks, (ii) privacy with zero-knowledge proofs, (iii) mobile-first DApp with offline QR support, (iv) interoperability with national databases, (v) AI-driven anomaly detection to identify fraudulent patterns, and (vi) formal verification and third-party audits of smart contracts. These directions will help ShikkhaChain mature into a production-ready platform capable of securing academic integrity at national scale.

### References

[1] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-chain: A credentials verifier using blockchain and ipfs," *arXiv preprint arXiv:2307.05797*, 2023. [Online]. Available: https://arxiv.org/abs/2307.05797

[2] M. Park and L. Zhang, "Blockcerts+: A secure blockchain-based certificate system with smart contract revocation," *IEEE Access*, vol. 11, pp. 134 756–134 770, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10172612

[3] M. A. Habib, M. M. Rahman, and N. H. Neom, "Credsec: A blockchain-based secure credential management system for university adoption," *arXiv preprint arXiv:2406.05151*, 2024. [Online]. Available: https://arxiv.org/abs/2406.05151

[4] K. Centeno Cuya and T. D. Palaoag, "Blockchain in higher education: Advancing security, verification, and trust in academic credentials," *Nanotechnology Perceptions*, 2024, published: May 2024. [Online]. Available: https://www.researchgate.net/publication/389949495_Blockchain_ensuring_academic_integrity_with_a_degree_verification_prototype

[5] Y. Xu, "Development of blockchain-based academic credential verification system," *Open Access Library Journal*, vol. 11, no. 09, pp. 1–20, 2024. [Online]. Available: https://www.researchgate.net/publication/384476272_Development_of_Blockchain-Based_Academic_Credential_Verification_System

[6] S. Shivarkar, "Academic certificate verification using decentralized digital certification," *International Journal of Scientific Research in Engineering and Management*, vol. 9, no. 2, pp. 1–9, 2025. [Online]. Available: https://www.researchgate.net/publication/389229234_Academic_Certificate_Verification_Using_Decentralized_Digital_Certification

[7] T. Nguyen and X. Lin, "Eduledger: Blockchain-based decentralized transcript management system," *Information Sciences*, vol. 644, pp. 119–138, 2023. [Online]. Available: https://doi.org/10.1016/j.ins.2023.04.018

[8] D. L. Silaghi and D. E. Popescu, "A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions," *Computers*, vol. 14, no. 4, p. 141, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/4/141

[9] A. de Alwis, A. Shrestha, and T. Sarker, "Exploring governance for accreditation in the education sector using blockchain technology: A systematic literature review," *Discover Education*, vol. 4, no. 57, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s44217-025-00449-y

[10] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: Uae case study and system performance," *Education and Information Technologies*, vol. 29, pp. 18 203–18 232, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10639-024-12493-6

[11] M. Fartitchou, I. Lamaakal, K. El Makkaoui, Z. El Allali, and Y. Maleh, "Blockmedc: Blockchain smart contracts for securing moroccan higher education digital certificates," *arXiv preprint arXiv:2410.07258*, 2024. [Online]. Available: https://arxiv.org/abs/2410.07258

[12] F. Ahmad and H. Lee, "Trustchainedu: Decentralized trust model for educational credential verification using blockchain and ipfs," *Computers and Education: Artificial Intelligence*, vol. 5, p. 100112, 2024. [Online]. Available: https://doi.org/10.1016/j.caeai.2024.100112

[13] A. Nasir and S. H. Bukhari, "Ipfs and blockchain integration for academic data provenance and verification," *Future Generation Computer Systems*, vol. 151, pp. 342–356, 2024. [Online]. Available: https://doi.org/10.1016/j.future.2024.03.007

[14] R. Mohapatra and A. Sen, "Smartcertedu: Smart contracts and ipfs for educational certificate management," in *Proceedings of the 2024 IEEE International Conference on Blockchain (Blockchain)*, 2024, pp. 231–238.

[15] S. A. Flanery, K. Mohanasundar, C. Chamon, S. D. Kotikela, and F. K. Quek, "Web 3.0 and a decentralized approach to education," *arXiv preprint arXiv:2312.12268*, 2023. [Online]. Available: https://arxiv.org/abs/2312.12268