CredChain

Web3 Employment & Academic Credentials Verification Platform

Project Proposal for AlgoBharat Hack Series 2025

Track: Bring Your Own Project

by
PAPPU KUMAR
HARSH PARIHAR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, MADRAS

March 21, 2025

1 Comprehensive Project & Module Description

CredChain is a next-generation Web3 platform that revolutionizes the verification of academic and professional credentials using blockchain technology. Built on Algorand, it creates a transparent, immutable, and secure ecosystem where users can store, manage, and share their verified credentials with potential employers, educational institutions, and professional networks.

By integrating with India's robust digital infrastructure (Aadhaar and DigiLocker), CredChain establishes a trustless verification mechanism that eliminates fraudulent credentials while preserving user privacy through Zero-Knowledge Proofs(ZKPs). The platform significantly reduces the time and resources spent on background verifications and streamlines the hiring process with smart contract automation.

In this project, we will develop a fully functional proof-of-concept that focuses on the end-to-end credential verification workflow, from document submission to employer verification, demonstrating the core value proposition of our larger vision.

2 Problem Statement

The current credential verification system relies on a few trusted data providers and organizations to verify the information and report it to the relevant parties. This process is time-consuming, often taking weeks, leading to significant delays in hiring and other critical areas. In addition to time and resources, the current credential verification ecosystem faces several critical challenges.

1. **Credential Fraud:** According to the report published by Hirepro.in [6], 85% of employers have caught applicants lying on their resumes, costing organizations billions annually in mishiring.

2. **Inefficient Verification Processes:** Background checks typically take 3-10 [7]business days and cost $50-$200 per candidate, creating significant delays in hiring processes.

3. **Data Silos and Privacy Concerns:** Traditional verification requires multiple touchpoints with separate institutions, each with their own verification processes and data privacy concerns.

4. **Credential Portability Issues:** Professionals face challenges transferring verified credentials across borders, institutions, and platforms.

5. **Lack of Standardization:** No universal format exists for credentials, making interoperability between systems difficult.

6. **Centralized Storage Vulnerabilities:** Credentials stored in centralized databases are vulnerable to hacks, data breaches, and unauthorized access.

3 Proposed Solution

To address the mentioned challenges, we are proposing ***CredChain***, a next-generation Web3 platform that will revolutionize the verification of academic and professional credentials with the help of blockchain technology (i.e. Algorand).

3.1 Core Components

1. **Decentralized Identity Management**
    - Aadhaar-based identity validation creates the foundation of trust.
    - The principles of self-sovereign identity give users control of their data.
    - Persistent cryptographic links between credentials and verified identities.
2. **Credential Issuance & Verification Protocol**
    - Integration with DigiLocker [9] for existing credential extraction.
    - Direct issuance of blockchain-verified credentials by educational institutions and employers.
    - Cryptographic proof mechanisms ensuring credential authenticity.
3. **Privacy-Preserving Verification**
    - Zero-Knowledge Proofs [5] allow selective disclosure of credential information.
    - Consent-based access control through time-bound smart contracts.
    - Granular permission settings for different verification needs.
4. **Smart Contract Hiring Workflows**
    - Automated verification processes reducing manual intervention.
    - Programmable hiring criteria and credential matching.
    - Audit trails for all verification activities.
5. **Interoperable Credential Format**
    - W3C [8] Verifiable Credentials standard implementation.
    - Cross-platform compatibility with existing HR systems.
    - Extensible schema for diverse credential typess.

3.2 Key Features

- **One-Click Verification:** Employers can instantly verify credentials with cryptographic certainty.
- **Tamper-Proof Records:** All credentials are immutably stored on Algorand blockchain.
- **Time-Bound Access:** Smart contracts automatically revoke access after verification period ends.
- **Selective Disclosure:** Candidates control exactly what information is shared with each verifier.
- **Real-Time Verification:** No waiting periods for institutional responses.
- **Audit Trail:** Complete history of credential issuance and verification.

4 Technical Architecture Overview

4.1 System Architecture Layers

The CredChain platform utilizes a layered architecture to ensure modularity, scalability, and security:

4.1.1 User Layer

- **Components:** Mobile application (React Native), Web application (React.js)
- **Technical Implementation:**
  - Both interfaces share a common design system using Tailwind CSS.
  - State management through Redux for consistent user experience.
  - WebAuthn integration for passwordless authentication.
  - Progressive Web App capabilities for offline credential access.
- **Cross-Platform Consistency:** GraphQL client for data fetching ensures consistent data models across platforms

4.1.2 Application Layer

- **API Gateway:**
  - Built on Express.js with GraphQL for flexible queries.
  - Implements rate limiting, request validation, and JWT authentication.
  - Provides unified interface to all microservices.
- **Authentication Service:**
  - OAuth 2.0 and OpenID Connect implementation.
  - Multi-factor authentication using TOTP and biometrics.
  - Session management with secure cookie implementation.
  - Integration with Aadhaar Authentication API using XML digital signatures.
- **Credential Management Service:**
  - Implements W3C Verifiable Credentials data model.
  - Handles credential lifecycle (issuance, storage, sharing, revocation).
  - Manages cryptographic operations for credential signing.
  - Indexing and search functionality for credential discovery.
- **Consent Manager:**
  - Fine-grained permission system based on OAuth 2.0 scopes.
  - Time-bound access control with automatic expiration.
  - Audit logging of all consent grants and revocations.
  - Integration with blockchain for immutable consent records.
- **ZKP Generator:**
  - Implementation of zkSNARK [5] protocols for credential proof generation.
  - Circuit compilation for common credential verification scenarios.
  - Integration with Web Crypto API for client-side cryptographic operations.

4.1.3 Integration Layer

- **DigiLocker Integration:**
  - OAuth 2.0-based authentication with DigiLocker [9].
  - API client for document retrieval and metadata extraction.
  - Document parsing and standardization to W3C Verifiable Credential format [8].
  - Digital signature verification for DigiLocker-issued documents.
- **Aadhaar Integration:**
  - Implementation of Aadhaar Authentication API (v2.5) [10].
  - Secure handling of demographic and biometric data.
  - Compliance with UIDAI security and privacy requirements.
  - UID token generation for internal identity mapping.
- **Organization API:**
  - RESTful API endpoint for educational institutions and employers.
  - Batch processing capabilities for issuing multiple credentials.
  - Webhook notifications for credential verification events.
  - API key management and throttling for partner access.

4.1.4 Blockchain Layer

- **Algorand Standard Assets (ASA) [2]:**
  - Custom ASA schema for different credential types.
  - Metadata structure following JSON-LD standards.
  - Implementation of revocation mechanisms through asset freeze.
  - Transaction optimization for cost-efficiency. .
- **Smart Contracts:**
  - Written in PyTeal with comprehensive testing frameworks.
  - Stateful contracts for credential management workflows.
  - Stateless contracts for verification logic.
  - Time-lock contracts for controlled access periods.
  - Escrow accounts for secure verification processes.
- **IPFS Document Storage:**
  - Content-addressable storage for credential documents.
  - Encryption layer using AES-256 [1] for sensitive documents.
  - Pinning service integration for document persistence.
  - Deduplication of common document types.

4.2 Technical Communication Flows

4.2.1 Credential Issuance Flow

1. User authenticates through Aadhaar verification via the Authentication Service.
2. User grants DigiLocker [9] access permissions through Consent Manager.
3. Integration Layer retrieves documents from DigiLocker [9].
4. Credential Management Service validates documents against issuing institutions.
5. Validated documents are encrypted and stored on IPFS [3], returning a content hash.
6. Credential metadata and IPFS [3] hash are packaged as an Algorand Standard Asset.
7. PyTeal smart contract issues the ASA to the user's Algorand wallet.
8. Credential details are indexed in the application database for efficient querying.

4.2.2 Credential Verification Flow

1. User selects credentials to share and defines access parameters (duration, information visibility).
2. Consent Manager creates a consent record and generates a smart contract.
3. For privacy-sensitive data, ZKP [5] Generator creates zero-knowledge proofs.
4. Smart contract deploys to Algorand blockchain with time-bound access controls.
5. Verifier receives access link with temporary credentials.
6. Verifier authenticates and accesses the verification portal.
7. Smart contract validates verifier identity and access permissions.
8. IPFS [3] retrieves and decrypts relevant documents.
9. Verification results are displayed with cryptographic proof of authenticity.
10. All verification activities are logged to the blockchain for auditing.
11. Upon expiration, smart contract automatically revokes access.

4.3 Cryptographic Infrastructure

4.3.1 Key Management

- Hierarchical Deterministic (HD) wallet architecture for user key management.
- Multi-signature requirements for credential operations.
- Threshold signatures for organizational credential issuance.
- Key rotation policies and secure backup mechanisms.

4.3.2 Zero-Knowledge Proof Implementation [4]

- Circuit design for common credential verification scenarios:
  - Age verification without revealing birth date.
  - Salary range verification without revealing exact amount.
  - Employment duration verification without revealing specific dates.
  - Degree verification without revealing grades.
- zk-SNARK protocol implementation using the Groth16 proving system [4].
- Trusted setup ceremony for parameter generation.
- Optimization for mobile device performance.

4.3.3 Privacy-Preserving Features

- Data minimization through selective disclosure.
- Unlinkability between different presentations of the same credential.
- Forward secrecy for all communications.
- Secure multi-party computation for cross-organizational verification.

4.4 Scalability and Performance Considerations

4.4.1 Database Architecture

- Polyglot persistence approach:
  - MongoDB for flexible credential schema storage.
  - Redis for session management and caching.
  - PostgreSQL for relationship data and complex queries.
- Database sharding strategy for horizontal scaling.
- Read replicas for query-intensive operations.

4.4.2 Microservices Deployment

- Containerization using Docker and Kubernetes.
- Auto-scaling policies based on transaction volume.
- Geographic distribution for low-latency global access.
- Circuit breaker patterns for resilient service communication.

4.4.3 Blockchain Optimization

- Transaction batching for cost reduction.
- Layer-2 solutions for high-frequency operations.
- State pruning techniques for efficient node operation.
- Selective on-chain storage with off-chain computation.

5 Implementation Plan and Timeline

This section presents our implementation plan, detailing key phases, core activities, and a structured timeline. The project is divided into five phases with two major milestones or submissions. Each phase is carefully planned for smooth execution. Refer to Figure [1] for a comprehensive breakdown of our approach and timeline.

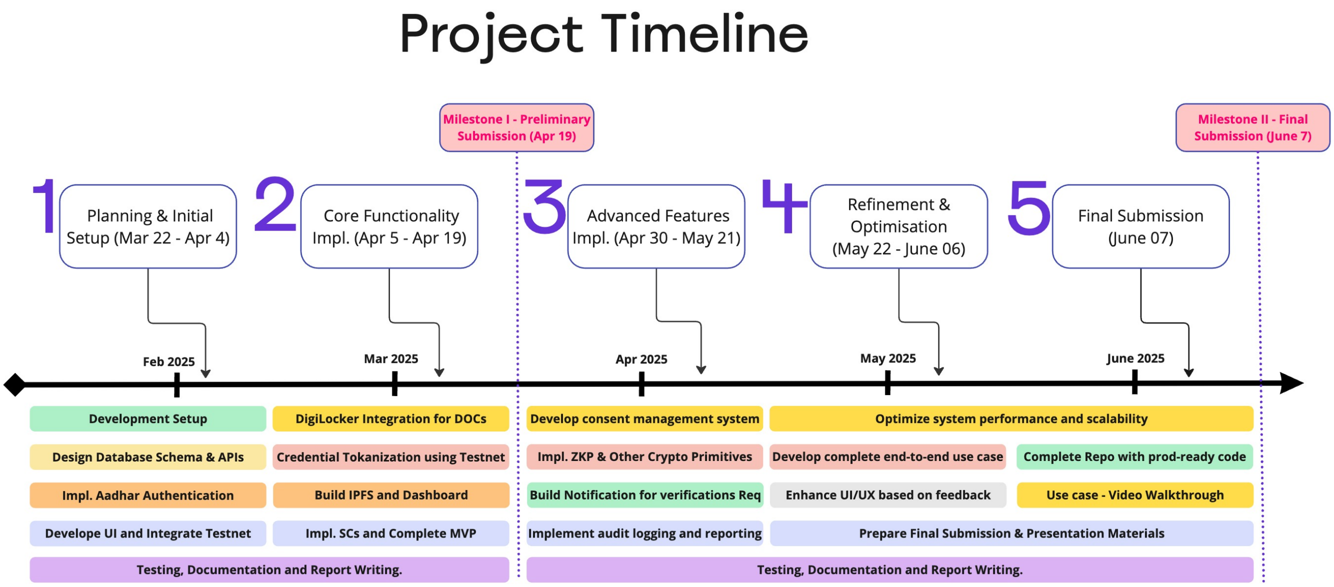
Project Timeline
Milestone I - Preliminary Submission (Apr 19)
Milestone II - Final Submission (June 7)
1
Planning & Initial Setup (Mar 22 - Apr 4)
2
Core Functionality Impl. (Apr 5 - Apr 19)
3
Advanced Features Impl. (Apr 30 - May 21)
4
Refinement & Optimisation (May 22 - June 06)
5
Final Submission (June 07)
Feb 2025
Mar 2025
Apr 2025
May 2025
June 2025
Development Setup
Design Database Schema & APIs
Impl. Aadhar Authentication
Develope UI and Integrate Testnet
DigiLocker Integration for DOCs
Credential Tokanization using Testnet
Build IPFS and Dashboard
Impl. SCs and Complete MVP
Testing, Documentation and Report Writing.
Develop consent management system
Impl. ZKP & Other Crypto Primitives
Build Notification for verifications Req
Implement audit logging and reporting
Optimize system performance and scalability
Develop complete end-to-end use case
Enhance UI/UX based on feedback
Complete Repo with prod-ready code
Use case - Video Walkthrough
Prepare Final Submission & Presentation Materials
Testing, Documentation and Report Writing.

Figure 1: Comprehensive Project Timeline Highlighting Key Phases and Core Activities.

Phase 1: Planning and Initial Setup

Phase 1	Activities
Timeline (March 22 - April 4)	• Set up development environment and version control. • Design database schema and API specifications. • Implement core authentication service with Aadhaar integration. • Develop basic UI wireframes and prototype. • Set up Algorand testnet environment.

Phase 2: Core Functionality Implementations

Phase 2	**Activities**
Timeline (April 5 - April 19)	• Implement DigiLocker integration for document retrieval • Develop credential tokenization as Algorand Standard Assets • Build IPFS integration for document storage • Create smart contracts for basic verification workflows • Develop simple dashboard for credential management • Complete MVP for preliminary submission

Milestone I - Preliminary Submission

Phase	**Activities**
Milestone I (April 19)	• GitHub repository with documented code • Video walkthrough of MVP functionality • Technical documentation

Phase 3: Advanced Features Implementation

Phase 3	**Activities**
Timeline (April 30 - May 21)	• Implement Zero-Knowledge Proof protocol for privacy-preserving verification. • Develop consent management system with time-bound access. • Create employer verification portal. • Build notification system for verification requests. • Implement audit logging and reporting features.

Phase 4: Refinement & Optimisation

Phase 4	**Activities**
Timeline (May 22 - June 7)	• Optimize system performance and scalability. • Enhance UI/UX based on feedback. • Comprehensive security testing and fixes. • Develop complete end-to-end use case scenario. • Prepare final documentation and presentation materials.

Milestone II - Final Submission with Use Case

Phase	**Activities**
Final Milestone (June 7)	• Complete GitHub repository with production-ready code. • Comprehensive documentation. • Use case walkthrough video. • Presentation for IRL event.

6 Expected Impact and Outcomes

6.1 Immediate Benefits

6.1.1 For Job Seekers

- 90% reduction in verification time for job applications.
- Complete control over personal data sharing.
- Portable credentials usable across multiple platforms.
- Elimination of repetitive document submissions.

6.1.2 For Employers

- 70% cost reduction in background verification processes.
- Near-instant verification of candidate credentials.
- Higher quality candidates through trusted verification.
- Reduction in fraudulent applications and mis-hires.

6.1.3 For Educational Institutions

- Streamlined credential issuance process.
- Reduced administrative burden for verification requests.
- Enhanced reputation through tamper-proof credentials.
- New revenue streams through verification services.

6.2 Broader Impact

6.2.1 Economic Efficiency

- Estimated $4.8 billion annual savings in Indian hiring market through reduced verification costs.
- Acceleration of hiring cycles by 40-60%, increasing workforce productivity.
- Reduction in credential fraud, estimated to cost businesses $600 million annually.

6.2.2 Digital Transformation

- Catalyst for blockchain adoption in HR and education sectors.
- Contribution to India's digital identity infrastructure.
- Model for credential portability across international borders.

6.2.3 Innovation Potential

- Extensible platform for additional verification services.
- Foundation for skills-based hiring transformation.
- Potential integration with emerging Web3 professional networks.

6.3 Key Metrics for Success

- Successfully verify 1,000+ credentials during pilot phase.
- Demonstrate 85%+ reduction in verification time.
- Achieve 95%+ accuracy in verification compared to traditional methods.
- Obtain positive user experience ratings from 80%+ of testers.
- Establish partnerships with at least 3 educational institutions for direct issuance.

7 Security and Compliance Framework

7.1 Security Measures

- **Penetration Testing Schedule:** Quarterly security assessments by third-party experts.
- **Bug Bounty Program:** Incentives for responsible disclosure of vulnerabilities.
- **Secure Development Lifecycle:** Automated security scanning in CI/CD pipeline.
- **Hardware Security Module (HSM) Integration:** For critical cryptographic operations.

7.2 Regulatory Compliance

- **GDPR Compliance:** Data minimization, right to erasure mechanisms, and consent management.
- **Personal Data Protection Bill Alignment:** Adapting to India's evolving data protection landscape.
- **ISO 27001 Framework:** Information security management system implementation.
- **SOC 2 Compliance Path:** Trust services criteria for security, availability, and confidentiality.

8 Conclusion

CredChain presents a transformative solution to the inefficiencies of traditional credential verification. By leveraging blockchain, Zero-Knowledge Proofs, and smart contracts, it ensures secure, tamper-proof, and instant verification while preserving user privacy. This proof-of-concept demonstrates its potential to streamline hiring, reduce fraud, and enable global credential portability, paving the way for a scalable, decentralized verification ecosystem.

References

[1] Ako Muhamad Abdullah et al. Advanced encryption standard (aes) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16(1):11, 2017.

[2] Algorand.Org. Algorand standard assets (asa) documentation, 2025. URL https://developer.algorand.org/docs/get-details/asa/. Accessed: 2025-03-20.

[3] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[4] Coinmonks Crypto Fairy. Under the hood of zksnark groth16 protocol. https://medium.com/coinmonks/under-the-hood-of-zksnark-groth16-protocol-2843b0d1558b, 2023. Accessed: 2025-03-20.

[5] Uriel Fiege, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 210–217, 1987.

[6] Hirepro.in. No resumes please - paving the way for talent-centric recruitment systems. Technical report, HirePro, 2023. URL https://hirepro.in/wp-content/uploads/2023/10/HirePro_Report_No_Resumes_Please_SHRM_IAC_Oct2023.pdf. Accessed: 2025-03-18.

[7] IDfy.com. The ultimate guide to improve your background verification process. https://www.idfy.com/the-ultimate-guide-to-background-verification-services/, 2024. Accessed: 2025-03-19.

[8] Romain Laborde, Arnaud Oglaza, Samer Wazan, François Barrere, Abdelmalek Benzekri, David W Chadwick, and Rémi Venant. A user-centric identity management framework based on the w3c verifiable credentials and the fido universal authentication framework. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–8. IEEE, 2020.

[9] MeitY National e Governance Division. Digilocker: Authorized partner api specification, version 1.11. https://img1.digitallocker.gov.in/assets/img/Digital%20Locker%20Authorized%20Partner%20API%20Specification%20v1.11.pdf, 2024. Accessed: 2025-03-20.

[10] Government of India (GoI) Unique Identification Authority of India (UIDAI). Aadhaar authentication api specification - version 2.5. https://uidai.gov.in//images/resource/Aadhaar_Authentication_API-2.5_Revision-1_of_January_2022.pdf, 2022. Accessed: 2025-03-20.