Blockchain-Based Certificate Verification System with Batch Issuance and Revocation

Final Year Project Proposal

Session Fall 2025

4th Year Students

BSc. (Hons.) BS in Software Engineering

Department of Software Engineering

FAST School of Computing

FAST National University, Karachi Campus

21 September 2025

Project Registration

Project ID (for office use): _____

Type of project: [ ] Traditional   [ ] Industrial   [ ] Continuing

Nature of project: [ ] Development   [ ] Research & Development   [ ] Research

Sustainable Development Goals (SDGs): [ ] Quality Education   [ ] Industry, Innovation, and Infrastructure

Area of Specialization: [ ] Blockchain

Project Group Members

Sr.#	Reg.#	Student Name	CGPA	Email ID	Phone #	Signatu
1	21K-3861	Syed Muhammad Huzaifa	2.03	k213861@nu.edu.pk	03212949737	
2	22K-4437	Tulaib Tausif	2.65	k224437@nu.edu.pk	03313674433	
3	22K-4800	Reeshaiel Shah	2.4	k224800@nu.edu.pk	03313674433	

Declaration

FYP group members have cleared all prerequisite courses for FYP-I as per their degree requirements.

1   Project Abstract

This project aims to design and implement a blockchain-based certificate verification system that addresses the critical issues of certificate fraud, duplication, and manual verification delays. Traditional verification methods rely heavily on centralized databases or physical records, making them vulnerable to tampering and time-consuming to verify. Leveraging the Polygon blockchain, the proposed system will enable universities to issue tamper-proof certificates whose hashes are stored on-chain, ensuring security and authenticity. Employers and third parties will be able to verify certificates instantly using a QR code, without exposing any sensitive student data.

Key features include batch issuance of certificates in a single blockchain transaction to optimize cost and time, a revocation mechanism to invalidate certificates in case of errors or fraud, and privacy protection by storing only cryptographic hashes of certificate data. A web-based frontend will provide portals for students and employers, while a Node.js backend will handle blockchain interactions. By deploying on the cost-effective Polygon network, the system ensures scalability and near-zero transaction fees, making it practical for real-world adoption.

2   Introduction

Academic and professional certificates are often subject to fraud, duplication, and manual verification delays. Traditional verification systems depend on centralized databases or paper-based records, which can be manipulated or require significant time and effort to validate. Blockchain technology provides a decentralized and tamper-proof solution for secure certificate issuance and verification.

The objective of this project is to design and implement a blockchain-based certificate verification system with practical features including batch issuance and certificate revocation. Sub-tasks include developing a smart contract on the Polygon blockchain to handle issuance, revocation, and verification; creating a backend API to interact with the blockchain; and building a user-friendly frontend for universities, students, and employers. Success will be measured by the ability to securely issue, verify, and revoke certificates on a live testnet.

3   Success Criterion

The project will be considered successful if it delivers a fully functional prototype that allows authorized university administrators to issue a certificate, store its hash on the Polygon blockchain, and enable third parties to verify or detect revocation of the certificate using a web interface. Batch issuance of multiple certificates in a single transaction must

also be demonstrated on the Polygon Mumbai testnet. The system should achieve near-zero transaction costs and maintain privacy by storing only cryptographic hashes.

4   Related Work

Existing blockchain-based certificate verification solutions, such as Blockcerts and OpenCerts, demonstrate the feasibility of using distributed ledgers to secure educational credentials. However, many of these systems focus only on single certificate issuance and lack practical features like batch issuance, revocation, and cost optimization. Academic prototypes often remain at a demo level and fail to address real-world scalability and user experience challenges.

5   Project Rationale

The increasing prevalence of fake degrees and forged professional credentials necessitates a robust and cost-effective solution for certificate verification. By leveraging blockchain's immutability and decentralization, this project offers a secure, privacy-preserving method for universities and employers to validate academic achievements. The project provides valuable experience in blockchain development and real-world application of decentralized systems.

5.1   Aims and Objectives

- Enable universities to issue tamper-proof certificates on the blockchain.

- Implement batch issuance to optimize cost and time.

- Develop a revocation mechanism for invalid certificates.

- Provide QR-code based verification for employers.

- Ensure privacy by storing only certificate hashes on-chain.

5.2   Scope of the Project

The project covers smart contract development, backend API creation, and frontend web interfaces. It will be deployed on Polygon testnet in FYP-I and potentially mainnet in FYP-II. It excludes integration with university ERP systems and mobile app development in the initial phase.

6   Proposed Methodology and Architecture

The system will be built using an iterative development methodology. The smart contract, written in Solidity, will manage certificate issuance, revocation, and verification on the Polygon blockchain. The backend, built with Node.js and Express, will provide RESTful APIs for interaction between the frontend and blockchain. The frontend will be developed using React/Next.js and will feature student and employer portals. Certificate data will be hashed using SHA-256 before being stored on-chain to ensure privacy.

7   Individual Tasks

Team Member	Activity	Tentative Date
Syed Muhammad Huzaifa	Requirement analysis, proposal writing	Sep 22 – Sep 28
Syed Muhammad Huzaifa	Frontend UI/UX design and development, integration	Sep 29 – Oct 10
Syed Muhammad Huzaifa	Frontend functional testing and deployment	Oct 11 – Oct 17
Tulaib Tausif	Blockchain research, Solidity contract development, Hardhat testing	Sep 22 – Oct 6
Tulaib Tausif	Provide ABIs/addresses, blockchain integration and deployment	Oct 7 – Oct 17
Reeshaiel Shah	Backend API development and integration	Sep 22 – Oct 10

8   Gantt Chart

FYP-1 Gantt Chart with Human-Readable Dates
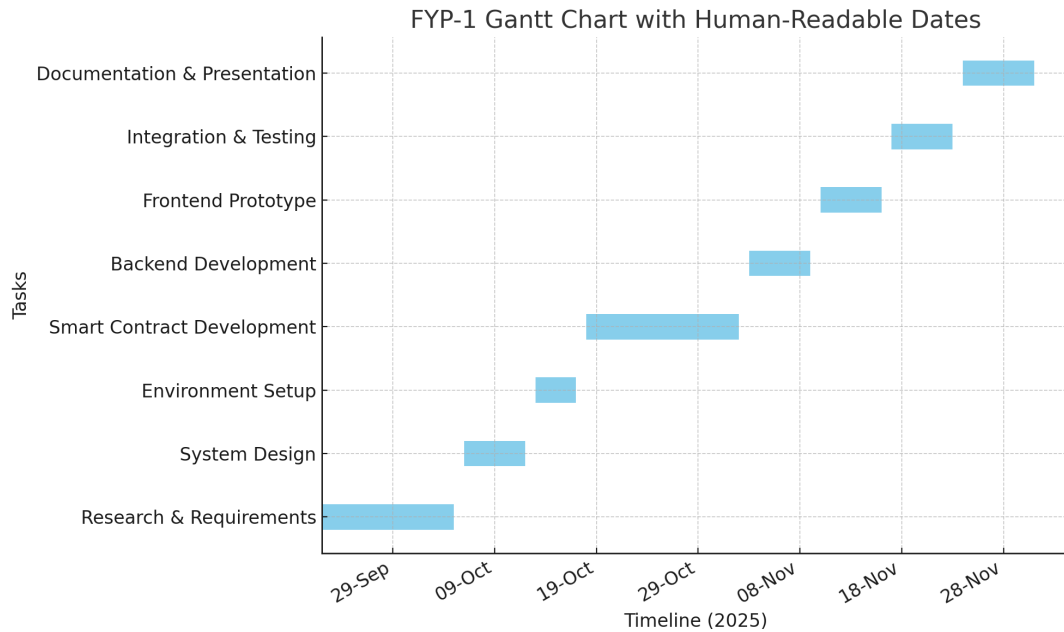
9   Tools and Technologies

- Blockchain: Polygon (Mumbai Testnet)

- Smart Contracts: Solidity, Hardhat

- Backend: Node.js, Express, ethers.js

- Frontend: React/Next.js

- Database (optional): MongoDB

- Other: MetaMask wallet, QR code libraries

10   References

1. Existing blockchain certificate systems such as Blockcerts (2016).