The Islamic University of Gaza

Faculty of Information Technology

CertiVerify: Blockchain-Based Certificate Verification System

Prepared by: Adam Eyad Saleh
Student ID: 120204353
Supervised by: Dr. Raed Rashed
Semester: Second Semester 2025/2026

Abstract

CertiVerify is a blockchain-based web application developed as part of the Special Topics 2 course. It allows academic institutions to issue and verify certificates securely using Ethereum smart contracts. The system ensures data integrity and transparency by recording certificate details on the blockchain, preventing any modification or forgery.

Introduction

The project aims to explore how blockchain technology can be applied in real-world academic systems. Traditional certificate verification methods depend on centralized databases that may be unreliable or subject to human error. CertiVerify provides a decentralized alternative, offering secure issuance and verification of certificates using blockchain technology and smart contracts on the Ethereum Sepolia test network.

Objectives

The objectives of this project are to:

- Understand and apply blockchain technology within a web application context.
- Design a decentralized certificate verification platform.
- Use smart contracts to manage certificate data securely.
- Integrate MetaMask for blockchain interaction.

System Design and Architecture

The system architecture consists of:

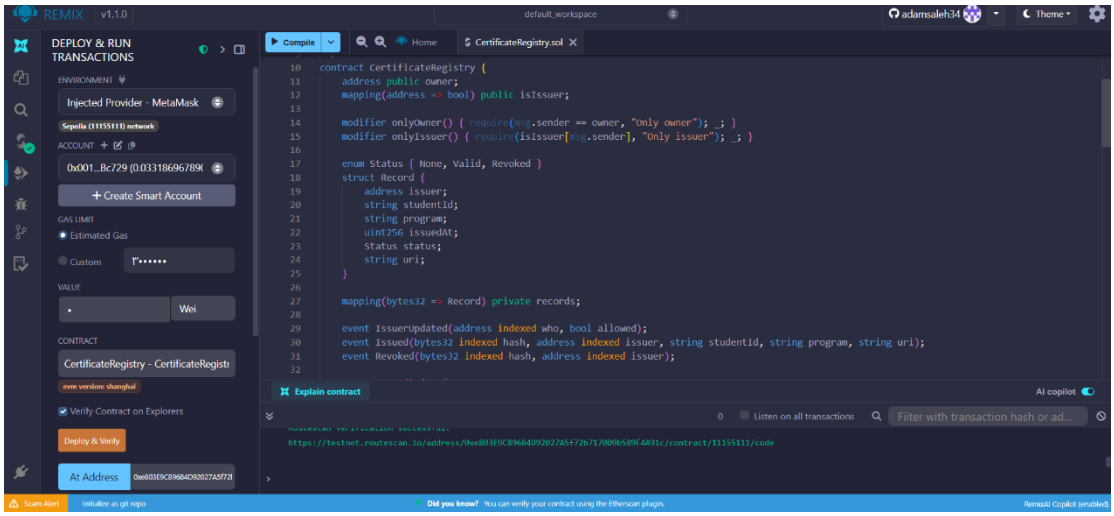
1. **Frontend:** Developed using HTML, CSS, and JavaScript for user interface and interaction.
2. **Backend/Smart Contract:** Written in Solidity and deployed through Remix IDE on the Ethereum Sepolia network.
3. **Blockchain Layer:** Used to store issued certificate hashes, ensuring immutability and transparency.

Implementation

1. Smart Contract Deployment (Remix IDE)

The smart contract was written in Solidity (v0.8.20) and deployed using Remix IDE. It defines the `issue()` and `verify()` functions to manage certificates on the blockchain.

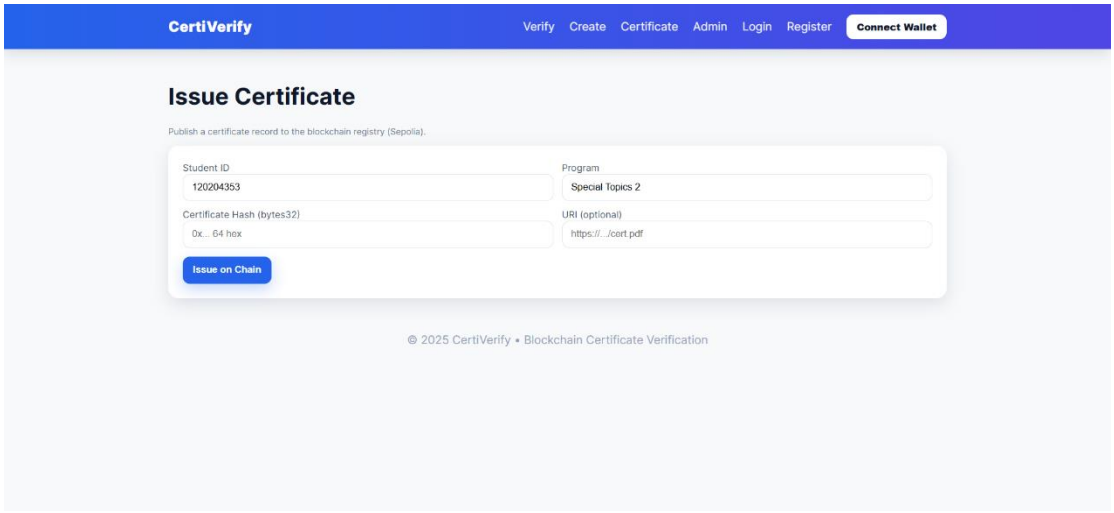
Figure 1: Deploying the Smart Contract using Remix IDE



Certificate Issuance (Create Page)

Authorized users enter certificate details (Student ID, Program, URI) and issue them via MetaMask confirmation. Once issued, the certificate hash is permanently stored on the blockchain.

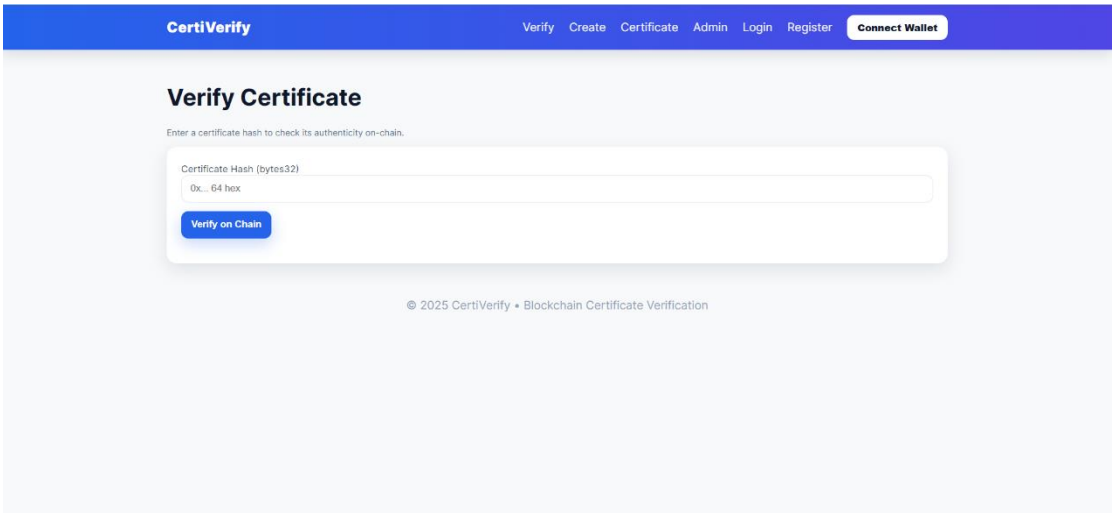
Figure 2: Certificate Creation Interface (Create Page)



Certificate Verification (Verify Page)

The verification interface allows users to check certificates by entering their hash. The system interacts with the smart contract to validate authenticity and status.

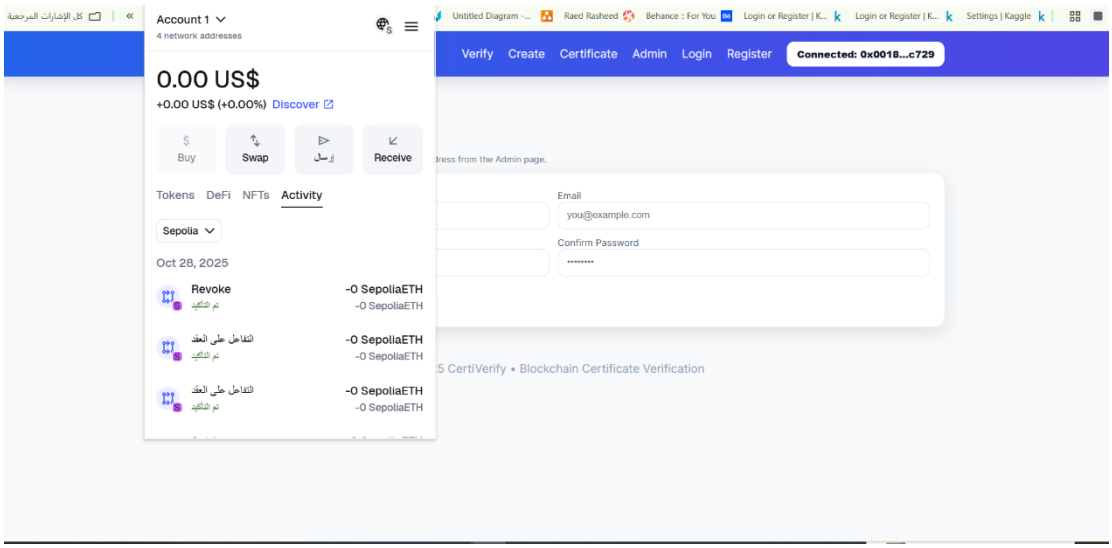
Figure 3: Certificate Verification Interface (Verify Page)



Blockchain Transaction (MetaMask Integration)

MetaMask manages user authentication and blockchain transactions. When issuing or verifying certificates, the user confirms transactions through MetaMask.

Figure 4: MetaMask Transaction Confirmation



Results and Discussion

CertiVerify successfully demonstrates the use of blockchain in academic certificate verification. The integration between MetaMask, Remix, and the frontend worked seamlessly on the Sepolia test network, ensuring secure and transparent operations.

Conclusion

The project achieved its objectives by providing a simple and secure method for certificate verification through blockchain. It reflects the practical understanding of decentralized applications and smart contracts gained during the Special Topics 2 course.