

Blockchain-Based Certificate Verification

Academic credential fraud is a persistent, high-value problem: forged degree certificates circulate widely while employer verification still depends on slow manual processes. This project implements a blockchain-based certificate verification system that replaces trust-in-paper with trust-in-cryptography. Universities issue certificates through an admin portal; each certificate's data is hashed (SHA-256) and the hash is anchored on a private Ethereum-style blockchain via a Solidity smart contract, with a unique QR code generated per certificate encoding its on-chain record identifier.

Verification is public and instant: an employer scans the QR code on the verification portal, the system re-hashes the presented certificate data and compares it against the immutable on-chain record, returning a verified/invalid verdict in seconds. The smart contract additionally supports revocation (for fraudulent or superseded certificates) and maintains an audit log of issuance and verification events. Bulk issuance via CSV upload models a real graduating batch. The architecture follows the industry-standard pattern of off-chain documents with on-chain hash anchoring, keeping the chain lightweight while making forgery computationally infeasible. Built-to-order with smart contracts, full-stack source code, deployment guide, project report, presentation PPT, and viva Q&A; support, this project covers blockchain fundamentals, smart-contract development, applied cryptography, and full-stack integration — a career-relevant final-year submission in the second-largest blockchain student search niche.