

ABSTRAK

SYARIFUL MUJADDIQ, Sistem Verifikasi Sertifikat Berbasis *Blockchain* dengan Implementasi Algoritma SHA-256 dan *Smart Contract* (Di bawah bimbingan Muhyiddin A M Hayat, S.Kom., M.T. dan Lukman, S.Kom., M.T.)

Penelitian ini merancang dan mengimplementasikan sistem verifikasi sertifikat berbasis *blockchain* dengan penerapan *Secure Hash Algorithm 256* (SHA-256) untuk menjaga integritas data, serta *smart contract* sebagai mekanisme validasi otomatis pada jaringan Ethereum. Sistem ini dikembangkan untuk Fakultas Teknik Universitas Muhammadiyah Makassar guna mengatasi pemalsuan sertifikat digital dan inefisiensi metode verifikasi konvensional. Setiap sertifikat diproses untuk menghasilkan *hash* SHA-256, diunggah ke *InterPlanetary File System* (IPFS) melalui Pinata, kemudian *hash* dan *Content Identifier* (CID) dicatat *on-chain*. Dua metode verifikasi disediakan, yaitu unggah file PDF untuk verifikasi internal dan pemindaian *Quick Response* (QR) Code untuk verifikasi publik. Arsitektur sistem memanfaatkan Node.js, Express, React, dan *smart contract* berbasis Solidity dengan manajemen melalui Hardhat. Hasil *unit testing*, integrasi, dan *end-to-end testing* menunjukkan tingkat keberhasilan 100% dalam penyimpanan dan verifikasi *hash*, keberhasilan penuh unggah IPFS, serta waktu respons verifikasi rata-rata di bawah lima detik. Sistem ini memberikan verifikasi sertifikat yang aman, transparan, dan terdesentralisasi, sehingga meningkatkan kepercayaan dan efisiensi dalam autentikasi dokumen digital.

Kata Kunci: Verifikasi Sertifikat, Blockchain, SHA-256, *Smart Contract*, IPFS.