ABSTRAK

Di era yang ditandai dengan kemajuan teknologi yang pesat dan meningkatnya ketergantungan pada ekosistem digital yang aman, algoritme hash kriptografi sangat penting untuk memastikan integritas, kerahasiaan, dan kinerja sistem berbasis blockchain. Studi ini menyajikan analisis komparatif dari dua fungsi hash kriptografi yang menonjol—SHA-512 dan BLAKE3—dalam konteks pengoptimalan kontrak pintar dalam aplikasi terdesentralisasi (DApps) pada blockchain Ethereum. Penelitian ini menyelidiki implikasi kinerja, efisiensi, dan keamanan dari kedua algoritme melalui implementasi eksperimental menggunakan kontrak pintar berbasis Solidity yang terintegrasi dengan alat pengembangan Ethereum seperti Truffle, Ganache, dan MetaMask.

Indikator kinerja utama termasuk kecepatan enkripsi/dekripsi, penggunaan CPU dan memori, konsumsi gas, dan ketahanan algoritmik terhadap serangan kriptografi seperti tabrakan dan pra-gambar. Studi ini lebih lanjut mengeksplorasi integrasi kedua algoritme ke dalam model kriptografi hibrida untuk mengevaluasi potensinya dalam meningkatkan efisiensi waktu eksekusi, menurunkan biaya operasional, dan memastikan kepatuhan terhadap standar perlindungan data internasional seperti GDPR dan Peraturan Pemerintah Indonesia No. 71 tahun 2019.

Temuan menunjukkan bahwa meskipun SHA-512 menawarkan jaminan keamanan yang kuat, BLAKE3 menunjukkan efisiensi dan kecepatan sumber daya yang unggul pada perangkat keras modern. Model hibrida yang diusulkan yang menggabungkan kedua algoritme terbukti meningkatkan skalabilitas dan keamanan DApps keuangan berbasis blockchain, menjadikannya solusi yang menjanjikan untuk sistem terdesentralisasi yang aman dan efisien. Penelitian ini memberikan wawasan dan rekomendasi praktis bagi pengembang dan pembuat kebijakan mengenai pemilihan dan penerapan standar kriptografi dalam infrastruktur blockchain.

Kata kunci: Blockchain, SHA-512, BLAKE3, Kontrak Cerdas, Algoritma Kriptografi, Keamanan Jaringan, Efisiensi Gas, Ethereum, DApps.