ABSTRACT

In an era marked by rapid technological advancement and increasing reliance on secure digital ecosystems, cryptographic hash algorithms are central to ensuring the integrity, confidentiality, and performance of blockchain-based systems. This study presents a comparative analysis of two prominent cryptographic hash functions—SHA-512 and BLAKE3—within the context of smart contract optimization in decentralized applications (DApps) on the Ethereum blockchain. The research investigates the performance, efficiency, and security implications of both algorithms through experimental implementation using Solidity-based smart contracts integrated with Ethereum development tools such as Truffle, Ganache, and MetaMask.

Key performance indicators include encryption/decryption speed, CPU and memory usage, gas consumption, and algorithmic resistance to cryptographic attacks such as collision and pre-image. The study further explores the integration of both algorithms into a hybrid cryptographic model to evaluate its potential for enhancing execution time efficiency, lowering operational costs, and ensuring compliance with international data protection standards such as the GDPR and Indonesia's Government Regulation No. 71 of 2019.

Findings indicate that while SHA-512 offers robust security guarantees, BLAKE3 demonstrates superior resource efficiency and speed on modern hardware. The proposed hybrid model combining both algorithms is shown to improve the scalability and security of blockchain-based financial DApps, making it a promising solution for secure and efficient decentralized systems. This research provides practical insights and recommendations for developers and policymakers regarding the selection and implementation of cryptographic standards in blockchain infrastructures.

Keywords: Blockchain, SHA-512, BLAKE3, Smart Contract, Cryptographic Algorithm, Network Security, Gas Efficiency, Ethereum, DApps.