Perbandingan Kinerja Algoritma Hash Spongent dan Photon pada Sistem Blockchain berbasis Ethereum = Performance Comparison of Spongent and Photon Hashing Algorithm in Ethereum-based Blockchain System

Mega Apriani, author

Abstrak

Teknologi blockhchain menyediakan komunikasi yang aman, privasi data, ketahanan dan transparansi. Dari ketiga generasi blockchain, generasi blokchain 2.0 lebih dikenal dengan platform Ethereum dan Hyperledger lebih banyak digunakan. Komponen utama pada blokchain adalah kriptografi. Algoritma kriptografi yang diimplementasikan untuk tanda tangan digital pada platform blockchain adalah algorima Elliptic Curve Digital Signature Algorithm (ECDSA). Sedangkan untuk algoritma fungsi hash pada Ethereum adalah KECCAK-256. Celah kerawanan pada blockchain terkait dengan fungsi hash adalah hacking hash function. KECCAK-256 dianggap cukup kuat dengan komputasi yang sekarang. Namun dengan adanya komputer kuantum, maka akan meningkatkan resiko peretasan pada fungsi hash. Lightweight cryptography adalah cabang baru kriptografi yang dirancang untuk mengatasi kompleksitas matematik, daya pemprosesan yang tinggi dan ruang memori yang besar terkait kriptografi primitive. Lightweight cryptography khusus fungsi hash telah disahkan berdasarkan standar internasional ISO/IEC 29192-5. Iso/IEC 29192-5 menetapkan tiga algoritma fungsi hash. Implementasi lightweight cryptography berbasis konstruksi sponge adalah PHOTON dan SPONGENT. Mengingat pentingnya fungsi hash dalam teknologi blockhain dan terdapat celah kerawanan dan daya komputasi yang mempengaruhi performa platform blockchain, maka pada penelitian ini akan direkomendasikan algoritma hash SPONGENT-256 dan PHOTON-256 untuk diimplementasikan pada sistem blockchain berbasis Ethereum. Implementasi algoritma hash SPONGENT-256 dan PHOTON-256 untuk diimplementasikan pada sistem blockchain berbasis Ethereum menghasilkan output berupa address, kunci publik dan wallet. Hasil test terhadap Algoritma SPONGENT-256 menghasilkan waktu yang singkat untuk dieksekusi rata-rata waktu real 0,0328 s, waktu user 0,0208 s dan waktu sys 0,0118 s. Hal ini akan memberikan hasil yang signifikan jika diimplementasikan pada sistem blockchain berbasis Ethereum dengan banyak node dan data yang akan dihasilkan. Namun algoritma SPONGENT-256 membutuhkan banyak memori untuk melakukan pemprosesan dengan rata-rata sebesar 75%. Sedangkan algoritma KECCAK-256 menggunakan memori lebih sedikit dibandingkan dengan algoritma PHOTON-256 dan algoritma SPONGENT-256 dengan rata-rata penggunaan memori sebesar 55%. Berdasarkan hasil implementasi algoritma hash SPONGENT-256 pada blokchain berbasis Ethereum dan analisis terhadap hasil maka dapat disimpulkan bahwa algoritma SPONGENT-256 dapat digunakan sebagai alternatif algoritma fungsi hash untuk sistem blokchain berbasis Ethereum.

.....Blockchain technology provides secure communication, data privacy, resilience and transparency. From the third generation of blockchain, blockchain generation 2.0 is better known as the Ethereum platform and Hyperledger is more widely used. The main component of the blockchain is cryptography. The cryptographic algorithm implemented for digital signatures on the blockchain platform is the Elliptic Curve Digital Signature Algorithm (ECDSA). As for the hash function algorithm on Ethereum is KECCAK-256. The vulnerability in blockchain related to hash functions is hash function hacking. KECCAK-256 is

considered quite powerful with current computing. However, the presence of a quantum computer increases the risk of hacking the hash function. Light cryptography is a new branch of cryptography designed to overcome the mathematical complexity, high processing power and large memory space associated with primitive cryptography. Hash function-specific lightweight cryptography has been certified according to the international standard ISO/IEC 29192-5. ISO/IEC 29192-5 defines three hash function algorithms. The implementation of lightweight cryptography based on sponge construction is PHOTON and SPONGENT. Given the importance of hash functions in blockchain technology and the vulnerability and computational power gaps that affect the performance of the blockchain platform, this research will recommend SPONGENT-256 and PHOTON-256 hash algorithms to be implemented on Ethereum-based blockchain systems. The implementation of the SPONGENT-256 and PHOTON-256 hash algorithms to be implemented on an Ethereum-based blockchain system produces output in the form of addresses, public keys and wallets. The test results of the SPONGENT-256 Algorithm produce a short time to execute with an average real time of 0.0328 seconds, user time 0.0208 seconds and system time 0.0118 seconds. This will give significant results if implemented on an Ethereum based blockchain system with many nodes and data to be generated. However, the SPONGENT-256 algorithm requires a lot of memory for processing with an average of 75%. While the KECCAK-256 algorithm uses less memory than the PHOTON-256 algorithm and the SPONGENT-256 algorithm with an average memory usage of 55%. Based on the implementation of the SPONGENT-256 hash algorithm on the Ethereum-based blockchain and analysis of the results, it can be said that the SPONGENT-256 algorithm can be used as an alternative hash function algorithm for Ethereum-based blockchain systems.