ABSTRAK

Keamanan dan integritas data merupakan aspek penting dalam era teknologi digital, terutama dalam manajemen sertifikat digital. Penelitian ini mengembangkan aplikasi sertifikat digital menggunakan teknologi *blockchain*, mengintegrasikan tanda tangan digital (*digital signature*) dan algoritma *hash Keccak256* untuk meningkatkan keamanan dan integritas. Metode pengembangannya menggunakan pendekatan *Rapid Application Development (RAD)* yang melalui tiga tahapan yaitu: Perencanaan Kebutuhan, Desain Workshop, dan Implementasi. Uji coba pada sertifikat digital memastikan ketahanan terhadap berbagai modifikasi seperti kompresi, perubahan data, penambahan gambar, dan rotasi, menunjukkan bahwa sistem dapat mendeteksi setiap perubahan sekecil apapun. Waktu rata-rata untuk menghasilkan tanda tangan berkurang dari 3,23 detik tanpa *blockchain* menjadi 2,11 detik dengan *blockchain*, dan validasi tanda tangan berkurang dari 2,11 detik tanpa *blockchain* menjadi 0,22 detik dengan *blockchain*. Hasil ini menunjukkan peningkatan kecepatan dan efisiensi yang signifikan. Aplikasi ini efektif dalam meningkatkan keamanan sertifikat digital, dengan memastikan bahwa setiap perubahan pada sertifikat digital mempengaruhi signature dan tetap menjaga integritasnya. Penelitian selanjutnya disarankan untuk mengevaluasi kinerja berbagai algoritma *hash* dalam konteks *blockchain*.

Kata kunci: *Blockchain, Digital Signature, Hash Keccak256,* Sertifikat Digital