ABSTRAK

Sebagian besar sistem *identity-based cryptography* pada *blockchain* dapat mengatasi tantangan pengelolaan sertifikat yang rumit, perlindungan privasi, dan keamanan dalam sistem autentikasi tradisional. Sistem manajemen *private key* terdesentralisasi menghindari manajemen sertifikat yang rumit dan meningkatkan perlindungan privasi, peningkatan keamanan, privasi, dan efisiensi. Namun, biaya komputasi yang tinggi dari pasangan bilinear, biaya *overhead* sistem menjadi besar. Sehingga diperlukan efisiensi proses komputasi. Penelitian ini bertujuan untuk menerapkan *lightweight identity-based cryptography* yang ringan secara komputasi sehingga dapat diterapkan pada perangkat dengan daya komputasi terbatas.

Kata Kunci : ***Identity-based cryptography, light-weight identity based cryptograpy, blockchain,*** **komputasi ringan**