ABSTRAK

Kemunculan *cryptocurrency* yang diawali Bitcoin pada tahun 2009 telah membawa perubahan yang cukup besar pada proses transaksi dunia maya. Perubahan tersebut juga menarik minat para ahli kriptografi, socio-ekonomi dan para peneliti dibidang desain sistem perangkat keras dan perangkat lunak. Hal ini diakibatkan sifat *cryptocurrency* yang tidak memiliki bank sentral dan mengandung proses kriptografi dalam setiap proses transaksinya. Sampai saat ini implementasi perangkat lunak maupun perangkat keras sudah banyak dilakukan, namun implementasi dengan efisiensi yang paling baik terus dikembangkan.

Pada penelitian kali ini dirancang sebuah implementasi dari prosesor scrypt untuk litecoin yang juga merupakan salah satu *cryptocurency*. Implementasi dilakukan dengan perangkat keras menggunakan FPGA. Hal ini dikarenakan FPGA memiliki kemampuan untuk diprogram secara mudah dengan kecepatan proses yang cukup tinggi. FPGA juga memiliki konsumsi daya yang rendah sehingga biaya *mining* tidak akan melibihi hasil yang didapatkan dari proses *mining*.

Sistem *mining* yang dirancang menggunakan algoritma scrypt yang mengakibatkan jumlah memori yang digunakan sebesar 1Kbit untuk setiap *core*. Sehingga implementasi pada *board* FPGA ATLYS hanya dapat dilakukan dengan 1 *core*. Pengimplementasian sistem *mining* dengan arsitektur pipeline mengurangi jumlah clock yang digunakan sebesar 7,92%. *Hash rate* pada implementasi FPGA sebesar 610H/s dengan frekuensi maksimum yang dapat digunakan adalah 26,968 MHz.

Kata kunci : Kriptografi, *Cryptocurrency*, Scrypt, Litecoin, HDL, FPGA