BAB I
PENDAHULUAN

1.1 Latar Belakang

Istilah *cryptocurrency* akhir-akhir ini (setelah kemunculan bitcoin pada tahun 2009) secara terus menerus menjadi lebih banyak dibicarakan oleh banyak kalangan. Dimulai dari kalangan jurnalis dan juga mulai masuk ke bidang *socio-ekonomi*[1] karena sifatnya yang tidak dikelola secara utuh oleh 1 bank sentral. Karena sifatnya tersebut, keamanan dari seluruh aktivitas diawasi oleh seluruh *miner* dari *cryptocurrency* yang digunakan. Selain itu sebuah *cryptocurrency* harus memiliki jumlah uang yang terbatas dan tidak bisa dibuat begitu saja agar uang tidak hanya dapat dimiliki secara instan oleh orang-orang tertentu.

Penggunaan *cryptocurrency* mengharuskan pemilik uang memiliki sebuah *wallet* yaitu sebuah dompet digital yang merupakan tempat penyimpanan uang tersebut. *Wallet* tersebut kemudian dapat disimpan dalam tempat penyimpanan elektronik seperti *harddisk* dan sejenisnya. Kemudian setiap 1 nominal dari uang pada *cryptocurrency* memiliki sebuah kode unik yang diakui dan datanya selalu diperbaharui pada setiap *wallet*. Selain itu setiap 1 nominal dari uang tersebut mempunyai nilai tertentu terhadap uang dari sebuah negara. Sayangnya nilai tersebut sangat fluktuatif. Hal ini dikarenakan kelemahan terbesar *cryptocurrency* yaitu sejumlah uang yang terdapat pada *wallet* dapat hilang begitu saja karena kesalahan pemilik, kerusakan tempat penyimpanan elektronik ataupun dicuri oleh *hacker*.

Secara umum *cryptocurrency* dibagi menjadi 2 yaitu *crytocurrency* dengan scrypt dan *cryptocurrency* tanpa scrypt. Salah satu *cryptocurrency* yang banyak digunakan saat ini adalah litecoin. Litecoin merupakan sebuah proyek *open source* yang dirilis dibawah lisensi MIT/X11. Litecoin disebut-sebut sebagai saingan terbesar dari bitcoin (*cryptocurrncy* pertama dan juga merupakan yang terbanyak penggunaannya) sebagaimana yang dilansir oleh Wall Street Journal dan The New York Times. Pada tahun 2013, sebuah majalah mingguan berbahasa Inggris The Economist menyebutkan bahwa litecoin merupakan alternatif dari bitcoin. Menurut Charles Lee (pencipta litecoin), perbedaan antara bitcoin dengan litecoin terletak pada proses pembuatan bitcoin yang membutuhkan komputer

dengan spesifikasi yang cukup tinggi sedangkan litecoin bisa dibuat di komputer biasa.

Dalam *cryptocurrency*, sebuah algoritma *hash* merujuk pada *key derivation function* dalam ilmu kriptografi. Kegunaan fungsi ini adalah untuk mengubah sebuah masukan (biasanya merupakan sebuah kunci) menjadi masukan standar dari sebuah sistem kriptografi. Scrypt adalah salah satu algoritma yang kemudian digunakan oleh litecoin. Scrypt merupakan sebuah fungsi *memory-hard sequential* yang berarti membutuhkan lebih banyak memori dari fungsi non-*memory-hard*. Akibatnya, sebuah *cryptocurrency* yang menggunakan algoritma scrypt sulit untuk diimplementasikan pada banyak prosesor yang pararel. Hal ini dikarenakan memori internal dari masing-masing prosesor pararel yang kecil, sementara algoritma scrypt membutuhkan memori yang cukup besar. Selain litecoin, scrypt juga digunakan oleh beberapa *cryptocurrency* yang ada. Pada implementasinya, sebuah konsep pipeline akan digunakan untuk mengorganisir kerja dari algoritma scrypt sehingga eksekusi scrypt membutuhkan waktu yang lebih singkat.

Sampai saat ini sudah banyak jenis perangkat keras digunakan untuk implementasi *cryptocurrency*. Hal ini dikarenakan implementasi langsung pada perangkat keras memiliki kecepatan proses yang tinggi. Selain itu pemilihan perangkat keras yang tidak tepat akan sangat berpengaruh pada hasil, kecepatan dan efektifitas proses. Salah satu pilihan perangkat keras yang digunakan adalah *Central Processing Unit* (CPU). CPU hanya memiliki 1 prosesor inti sehingga proses algoritma hanya dilakukan oleh prosesor tesebut. Kemudian pada perkembangannya penggunaan *Graphic Processing Unit* (GPU) membuat proses tersebut dilakukan oleh beberapa prosesor kecil secara pararel. Pada *cryptocurrency* dengan scrypt penggunaan GPU tidak cukup baik. Selain itu GPU membutuhkan daya yang cukup besar sehingga memungkinkan hasil dari proses *mining* lebih kecil dari pada biaya untuk mengoprasikan GPU tersebut.

Selanjutnya *Field Programmable Gate Array* (FPGA) digunakan karena kemampuannya yang dapat dengan mudah di program kembali. Untuk memperoleh hasil kerja yang cukup baik, FPGA tidak menggunakan banyak daya sehingga FPGA merupakan salah satu komponen aplikatif yang hemat energi. Pada akhirnya *Application Specific Integrated Circuit* (ASIC) diproduksi untuk lebih menghematkan proses tersebut karena penggunaannya yang sangat tertentu.

Namun kekurangan utama pada ASIC adalah produksinya yang harus merupakan produksi massal dan sistem harus sudah sangat matang.

Hash rate merupakan acuan tingkat efektifitas dari sebuah implementasi algoritma *hasing*. *Hash rate* didapatkan dari banyaknya hasil algoritma *hasing* persatuan waktu biasanya dalam satuan M*hash*/s (*millions hashes per second*). Selain itu, *hash rate* juga dapat diukur dari banyaknya hasil algoritma *hasing* persatuan energi, biasanya dalam satuan M*hash*/J (*millions hashes per joule*). Konsumsi daya total diukur dalam satuan *watt*.

Pada perancangan kali ini, penulis menggunakan FPGA sebagai implementasi perangkat keras. FPGA merupakan salah satu alat untuk implementasi perangkat keras yang cukup baik. Hal ini disebabkan kerena FPGA memiliki harga yang tidak terlalu mahal, implementasi yang mudah, memiliki kemampuan untuk diprogram kembali serta memiliki kecepatan yang cukup tinggi. Proses implementasi sistem ke FPGA menggunakan bahasa verilog.

Dengan munculnya *cryptocurrency*, saat ini banyak berkembang peluang bisnis dalam berbagai hal. Produksi massal ASIC untuk proses *mining* dalam *cryptocurrency* merupakan salah satunya. Selain itu pengadaan *money changer* ataupun *Automated Teller Machine* (ATM) untuk *cryptocurrency* juga merupakan peluang yang cukup baik.

1.2 Rumusan Masalah

Masalah yang menjadi dasar pembuatan Tugas Akhir ini adalah bagaimana menjadikan FPGA sebagai sarana implementasi perangkat keras dari proses *mining* litecoin. Masalah yang diselesaikan pada Tugas akhir ini :

1. Merancang algoritma scrypt menggunakan bahasa dekripsi verilog.
2. Mengimplementasikan arsitektur pipeline pada algoritma scrypt.
3. Merancang sistem *mining cryptocurrency* yang menggunakan algoritma scrypt menggunakan bahasa verilog.
4. Simulasi sistem *mining cryptocurrency*.
5. Implementasi sistem *mining cryptocurrency* di FPGA.

1.3 Tujuan Penulisan

Tujuan tugas akhir ini dapat dirumuskan sebagai berikut :

1. Menganalisis hasil perancangan dan simulasi sistem *mining cryptocurrency* berbasis algoritma scrypt dengan arsitektur pipeline.

2. Menganalisa performansi dan *resource* dari sistem *mining cryptocurrency* berbasis algoritma scrypt dengan arsitektur pipeline pada implementasinya di FPGA.

1.4 Batasan Masalah

Pada tugas akhir ini masalah dibatasi pada:

1. Perancangan hanya pada sistem *mining* dari *cryptocurrency*
2. Sistem yang digunakan adalah *cryptocurrency* berbasis algoritma scrypt khususnya meggunakan *cryptocurrency* litecoin
3. *Hardware Description Language* yang digunakan adalah verilog
4. Simulasi menggunakan perangkat lunak ModelSim-Altera dan ISim dan sintesis perangkat keras menggunakan perangkat lunak Xilinx ISE 14.5.
5. Board FPGA yang digunakan adalah Digilent ATLYS Spartan 6 XC6SLX45 CSG324C.
6. Performansi hanya diukur dari waktu pemrosesan satu buah blok data pada algoritma scrypt, frekuensi maksimum yang dapat digunakan serta jumlah *resources* yang dibutuhkan untuk implementasi perangkat keras.

1.5 Metodologi Penelitian

Penulisan buku Tugas Akhir ini menggunakan metode penelitian sebagai berikut:

1. **Studi Literatur**

   Metode ini digunakan untuk mendapatkan teori-teori yang berhubungan dengan perancangan dan implementasi algoritma scrypt dengan atau tanpa menggunakan arsitektur pipeline pada FPGA dengan menggunakan bahasa verilog.

2. **Perancangan**

   Melakukan pemodelan, desain dan perancangan sistem menggunakan bahasa verilog.

3. **Eksperimen**

   Perancangan dan pengujian sistem algoritma scrypt dengan atau tanpa menggunakan arsitektur pipeline secara implementasi pada FPGA.

4. **Optimalisasi**

Melihat performansi hasil simulasi dan implementasi dari sistem *mining cryptocurrency* berbasis algoritma scrypt dengan arsitektur pipeline dan kemudian di optimalisasi.

1.6 Sistematika Penulisan

Secara umum keseluruhan Tugas Akhir ini dibagi menjadi lima bab bahasan, ditambah dengan lampiran dan daftar istilah yang diperlukan.Penjelasan masing-masing bab adalah sebagai berikut:

BAB 1 : PENDAHULUAN

Bab ini akan membahas latar belakang pemilihan topik tugas akhir, tujuan penelitian, perumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan tugas akhir**.**

BAB 2 : DASAR TEORI

Bab ini memberikan pemaparan tentang teori-teori yang mendukung dan mendasari penelitian tugas akhir ini.

BAB 3 :PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab ini membahas mengenai model sistem yang digunakan dan kemudian mensimulasikannya. Parameter kerja dan asumsi simulasi yang digunakan akan dijelaskan di sini.

BAB 4 : HASIL DAN ANALISIS

Bab ini menjelaskan tentang pengujian sistem serta analisis terhadap keluaran yang dihasilkan.

BAB 5 : KESIMPULAN DAN SARAN

Bab ini merupakan bab terakhir dari laporan tugas akhir yaitu berupa kesimpulan untuk sistem yang penulis kerjakan, serta saran untuk penelitian berikutnya.