[ENGR3410] Final Project Proposal:
Implementing Bitcoin Miner

Changjun Lim

1 Project Description

Bitcoin is a representative peer-to-peer cryptocurrency. Without a central control system, the Bitcoin network can assure the reliability of transactions. Every record of transactions is stored in blocks and each block is validated with proof of work. It is called Bitcoin mining to ensure the validity of a block by doing a time-consuming process(which needs many calculations). Bitcoin mining is like solving cryptographical problems(calculate to reverse the hash function SHA-256) within the appointed amount of time. So FPGA is usually better than multi-purpose processors like CPU because it can optimize calculation.

The purpose of this project is to understand the working mechanism of Bitcoin and implement Bitcoin miner using FPGA. I will implement the Bitcoin mining algorithm using Verilog or VHDL and test its performance on FPGA. When the time allows, I will find the way to optimize the miner and run the miner on a real Bitcoin network. As Demo, I will present this project and share this project by uploading source code and the report on Github. I will use the following references.

- Philip Dotemoto, FPGA Based Bitcoin Mining
  (http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1285&context=eesp)
- Open-Source FPGA Bitcoin Miner
  (https://github.com/progranism/Open-Source-FPGA-Bitcoin-Miner)

2 Project Objective

- Understand the Bitcoin network and the Bitcoin mining algorithm
- Implement the Bitcoin mining algorithm
- Run Bitcoin miner on FPGA
- (Advanced) Optimize the miner
- (Advanced) Run the miner on the real Bitcoin network and extend the miner into other cryptocurrency systems

3 Work Plan

- [12/1] Design the Bitcoin miner on a block diagram (3 hrs)
- [12/3] Implement the Bitcoin mining algorithm using Verilog or VHDL (4 hrs)
- [12/3] Make Test bench for the miner (3 hrs)
- [12/5] Test the program and revise it (5 hrs)
- [12/7] Run the miner on FPGA (1 hr)
- [12/10] Write a report (3 hr)
- [12/11] Share the project on Github(source code and page) (1 hr)
- [12/10] (Advanced) Optimize the miner (4 hrs)
- [12/10] (Advanced) Implement the connection module to Bitcoin network (4 hrs)
- [12/11] (Advanced) Run the miner on the real network (3 hrs)