CSEE W4840 Final Project Proposal
Bitcoin Miner

Ben Nappier (ben2113)
Peter Xu (px9117)
Patrick Taylor (pat2138)

Overview
We intend to implement a Bitcoin miner. The miner will be capable of mining Bitcoins solo or together with other miners in what is known as a Bitcoin mining pool. The goal will be to integrate peer-to-peer Bitcoin network communication software with fpga hardware attempting to solve the difficult Bitcoin mining problem. Additionally, we will measure the power consumption and results of our miner in order to gauge its efficiency.

Input
Keyboard to control parameters prior to running. The fpga may only have input from the p2p networking software.

Output
VGA Monitor to output status, results and efficiency metrics

Algorithm Description
Bitcoin mining requires running a proof of work algorithm and then communicating a correct solution with a peer-to-peer network. The fpga will be doing the proof of work algorithm, by guessing 256 SHA encryptions for the headers of Bitcoin blocks within a certain error tolerance. Bitcoin blocks are pending Bitcoin transactions and Bitcoin mining validates these transactions. When a miner solves the SHA of a block, the block is solved and the miner is rewarded with a fixed amount of Bitcoins. Our fpga will try to solve the SHA for a given time, check to see if another miner has solved it, then continue until our fpga solves it or another miner does in which case it should start trying to solve the newest block.

Hardware Software Integration
We plan to write our software in C to communicate with Bitcoin's peer-to-peer network. The software will also feed the fpga the Bitcoin block header, which it will use to guess the correct code for. The fpga, occasionally will communicate with the software, to inform either that the fpga has solved the block code or to see if the network has a new block to solve.

Milestones
- Create the peer to peer software
- Create the working algorithm

- Integrate the two systems
- Add efficiency metrics

- Creating support for Bitcoin Mining pools