CSEE W4840 Final Project Proposal
Group: Gold Miner
Project Topic: Bitcoin Miner

Mingyang Song (ms6525)
Zhe Mo (zm2404)
Tianyu Qin (tq2155)
Xueji Zhao (xz3159)

Introduction

Bitcoin mining is the process of adding new transaction records to the public ledger of the Bitcoin network, which requires solving a complex cryptographic puzzle. The most common algorithm used for this task is SHA256, which requires performing large numbers of hash operations per second. By doing this, a miner will be rewarded with a certain amount of bitcoin.

Objectives

The goal of this project is to build a FPGA-based bitcoin miner which can communicate with the bitcoin pool through ethernet and efficiently perform SHA256 hash operations.

Input

Keyboard to control the whole system.

Output

VGA monitor to display status, results, hash rate etc.

Core algorithm

This project will consist of both software and hardware. The Bitcoin mining software will be implemented to communicate with the FPGA and the bitcoin pool. The software will feed the FPGA with a Bitcoin block header, which will be processed by the SHA256 hashing algorithm on the FPGA board. Once the FPGA completes a mining job, the software will receive the result and submit it to the Bitcoin pool for validation and inclusion in the blockchain. Throughout the process, the software will interface with the Bitcoin pool in order to determine whether the assigned task has been successfully solved by other miners.

Milestone

1. Build up the FPGA board implemented with SHA-256;
2. Build up a serial interface to send and receive date;
3. Integrate the serial interface with FPGA board;
4. Create connection with Bitcoin mining pools to request work and submit Proof-of-Work.