Building A Litecoin Miner on Udoo

Project Proposal for CS290G Cryptographic Engineering

Ruoyu Wang and Jake Corina

Background

A cryptographic currency is a medium of exchange which is designed around certain cryptographic algorithms. Compared to fiat money which usually has governmental backing and regulation, a cryptographic currency is special in the way that theoretically no one is able to accelerate, stunt or abuse the production of money. The total amount of cryptographic currency is usually made public with its design, and the total amount of money produced within a certain timespan is bounded by fixed parameters. While fiat money could be overprinted by a government, there is no single organization that could affect the total amount of money of a cryptographic currency. This feature combined with other factors like safety, anonymity, etc. has made cryptographic currency a very popular topic of discussion.

Mining refers to the process of producing money through computation via certain algorithms (mostly based on collisions of a hash function) in a cryptographic currency system. As a cryptographic currency system is always distributed, people can produce their own money, and those people are referred to as miners. Just like mining in real life, mining in cryptographic currency also means a lot of work. Although mining could be done on generalized devices like a personal computer, more and more people have started mining on video-cards, FPGA or ASIC to obtain a better results, and thus, more profit.

There are some cryptographic currencies that are specifically designed to reduce, though not completely remove, the advantages of using video-cards, FPGA or ASIC for mining. Litecoin, for example, is based on a cryptographic algorithm (scrypt) that demands a very large amount of memory. In general, on the specially designed hardware, large amounts of memory is both cost and power inefficient. For this reason we are interested in implementing a CPU miner on a mini-computer like Udoo. These mini-computers are usually cheaper than a full sized PC, and provide comparably sufficient memory and computation power. Hopefully they could, in some sense, be a replacement for the expensive alternative of the specially-designed mining devices.

Goals

In this project, we would like to implement a CPU miner for Litecoin on a Udoo-Dual Lite device. Although there are several existing mining programs available on the Internet like cpuminer, none of them are specially optimized for ARM. So apart from basic porting and implementation, we would like to optimize our mining program for ARM architecture and make comparison with the naive implementation.

Given the fact that we don’t have much time to spend on this class project, we will start on a basic implementation of miner, try to port it to ARM Linux, and then profile and optimize it.
Eventually we shall have a working mining program on Udoo, as well as a report of how different optimizations would affect the computational efficiency.

Timeframe
All the work shall be done by the end of this quarter.