First Meeting - 11.13

MSc Project
Runchao Han

November 15, 2017

1 Overview of the Project

The project aims at the widely used mining algorithms for cryptocurrencies. PoW based cryptocurrencies rely on mining powers to get coins, which contributes to the decentralised characteristic of digital currencies like Bitcoin. However, currently ASIC and FPGA technologies are utilised for mining, making the computing power centralised. This project is to improve state-of-the-art mining algorithms to make them obtain better performance on CPU/GPUs, while keeping them memory-consuming and non-parallelisable.

The basic requirements of the imrpoved algorithms are listed below:

1. Memory-hard. The process of minting a block requires lots of memory space.
2. Non-parallelisable. It is impossible to minimise the cost by parallelising this algorithm.
3. Dynamic difficulty. The difficulty of minting a block can vary.

2 Methodology and Process of the Project

To make this project practical, we divide it into clearly defined steps with achievable tasks.

1. Survey about state-of-the-art mining algorithms:
   - Find/collect current popular mining algorithms
   - Choose the mostly accepted one(s)
   - Acknowledge the chosen one(s)
2. Collect data about the performance, electric power cost on different hardwares:
   - Choose hardwares for implementations of algorithms on different platforms: CPU,GPU,FPGA and Memory.(No need to run ASIC version by ourselves)
   - Collect data
   - Make comparisons, including tabulating and plotting them
3. Decompose the algorithms to stages with clearly defined functions and make analysis:
   - Observe the code, including some runs/tests

    - Decompose the algorithm to logical stages with specific functions
    - Analyse them to find out possibilities of optimisations

4. Implement the optimised version and make comparisons

3 Miscellaneous

- Frequent and effective reports/outputs
    - Help the supervisor learn about it
    - Help the student learn about it and keep the right direction
- Document every meeting/feedback and arrange them
- Every report should be produced by Latex

4 Next Week's Plan

- Survey about state-of-the-art mining algorithms
- Read their source code if possible

5 Related Papers

- The scrypt password-based key derivation function. No. RFC 7914.
  http://www.rfc-editor.org/rfc/rfc7914.txt
- Scrypt is maximally memory-hard.
  https://eprint.iacr.org/2016/989.pdf
- Dash whitepaper.
  https://github.com/dashpay/dash/wiki/Whitepaper
- Hashcash-a denial of service counter-measure.
  ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf
- STRICT MEMORY HARD HASHING FUNCTIONS.
  https://bitslog.files.wordpress.com/2013/12/memohash-v0-3.pdf
- Cuckoo Cycle.
  https://github.com/tromp/cuckoo
- Dagger: A Memory-Hard to Compute, Memory-Easy to Verify Scrypt Alternative.
  http://www.hashcash.org/papers/dagger.html
- MOMENTUM - A MEMORY-HARD PROOF-OF-WORK VIA FINDING BIRTHDAY COLLISIONS.
  http://www.hashcash.org/papers/momentum.pdf