Project Proposal

Optimising the Performances of Proof-of-Work Algorithms on CPU and GPU
to Democratise the Cryptocurrency Mining Process

Student: Runchao Han (ID: 10140466)
Supervisor: Christos Kotselidis

November 15, 2017

1 Background

Cryptocurrencies like Bitcoin[4] implemented through the blockchain technology are at the highest international interest because of their decentralisation and anonymity nature. Proof-of-Work (PoW)[2] based cryptocurrencies rely on computing specific hash values called "mining" to get coins, the process of which obtains the consensus on the whole blockchain network[4]. However, currently ASIC and FPGA technologies are utilised for mining, making the computing power centralised.

2 Description

This project is to optimise state-of-the-art mining algorithms for better performances on CPU/GPUs to minimise the performance gap between CPU/GPU and FGPA/ASIC. Attempts[5][1][3][6] exist at present, but are proved to be not as successful as expected. This project will take a step further to contribute to the democratisation of cryptocurrencies and better efficiencies of CPU/GPU mining.

3 Deliverables

1. A thorough review and benchmarking on state-of-the-art mining algorithms.
2. Implementations of optimised mining algorithms and their benchmarking.
3. A brand-new mining algorithm with better performances on CPU/GPU.

References

[1] Daniel Larimer. Momentum - a memory-hard proof-of-work via finding birthday collisions. Technical report, 2013.

[2] Ben Laurie and Richard Clayton. Proof-of-work proves not to work. 2004.

[3] Sergio Demian Lerner. Strict memory hard hashing functions. Technical report, 2014.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[5] Colin Percival and Simon Josefsson. The scrypt password-based key derivation function. Technical report, 2016.

[6] Ronald L Rivest, Adi Shamir, and David A Wagner. Time-lock puzzles and timed-release crypto. 1996.