Mine with it or sell it: the superhashing power dilemma

Francesco Bruschi
Department of Electronics, Information and Bioengineering (DEIB)
Politecnico di Milano
Italy, Milan
francesco.bruschi@polimi.it

Vincenzo Rana
Department of Electronics, Information and Bioengineering (DEIB)
Politecnico di Milano
Italy, Milan
vincenzo.rana@polimi.it

Lorenzo Gentile
Department of Electronics, Information and Bioengineering (DEIB)
Politecnico di Milano
Italy, Milan
lorenzo.gentile@polimi.it

Donatella Sciuto
Department of Electronics, Information and Bioengineering (DEIB)
Politecnico di Milano
Italy, Milan
donatella.sciuto@polimi.it

ABSTRACT

In proof of work blockchain systems, there are strong incentives towards designing hardware that can mine faster and/or with less power consumption. There are two ways of taking advantage of such devices: one can use them to mine more coins with less power, or he can sell it to other miners. The two strategies are not independent, of course: if everybody has the boosting technology, the difficulty will rise, and it won't be an advantage anymore. On the other hand, if the boost is above a certain threshold, being used only by a small subset of miners might mean centralizing the system, with potentially dangerous consequences on the platform credibility. In this paper we analyse the impact of different strategies to exploit a significant increase in mining hardware efficiency. To do so, we developed a multi-agent based simulator, that mimics the relevant mechanics of the mining ecosystem, as well as some features of the miners as economic actors. We then characterized different significant sell-it-or-mine-with-it strategies, and observed the simulated outcome.

Categories and Subject Descriptors

G.3 [**Distributed Systems**]: Blockchain—*Mechanism Design*

Keywords

mining, bitcoin, ethereum, blockchain, hash, hardware, simulation

1. INTRODUCTION

Proof-of-work is a set of techniques, first described in [Dwork and Naor 1993], that allows to limit the access to a virtual resource, requiring some computational intensive task to be done. Access to the resource can be granted if the request is associated with the demonstration of having carried out a task that requires effort. The first application proposed for these techniques was to prevent mail spamming: if every email was required to demonstrate a computational effort associated to its writing, such that it was negligible for "normal" mail use but infeasible for spamming (millions of mails day), this would disincentive massive spamming. The very same idea came in hand in the definition of the so called Nakamoto consensus, at the heart of the Bitcoin system. In Bitcoin, the proof of work is used to have access to the history validation task: who wants to add the next block in the chain invests computational power to find a nonce with some properties. The more computational power invested, the higher is the probability of adding the next block. Each validated block is worth a reward. This system, in the context of some other rules, guarantees that the system will eventually converge to a common representation of the history or, in other words, that forks in the history are unstable.

The proof of work requires to find a nonce that, concatenated to the block to be validated, causes its SHA256 hash to be below a certain value, called difficulty. The difficulty is regulated by a negative feedback mechanism, that aims at keeping the time required to validate a block constant on average. If more effort is spent globally on the proof of work, then the blocks will be mined more frequently/quickly, and the system rules will increase the difficulty. The net worth of a miner obviously depends, among other things, on the number of blocks that he mines, on the value of the cryptoasset and on how much he pays for hashing power. Two ways of increasing net worth are then: to lower electricity cost and to increase hardware efficiency i.e., to have more hashing power with the same electricity. In this work we analyse the question: what would be the best strategy to exploit a new technology that allows boost in hashing power? Is it best to keep it secret, and use it to mine more blocks exploiting the competitive advantage in hashing power with respect to the others, or is it better to sell it to a fraction of other miners? Or to all other miners? We analyse and discuss some strategies that an actor with a boosting technology could

Symposium on Cryptocurrency Analysis (SOCCA) 2018. Dec. 6, 2018, Toulouse, France
Copyright is held by author/owner(s).

implement. In addition, we validate our discussion with the help of a multi agent simulator we developed, as an open source project, for this purpose.

2. STATE OF THE ART

In [Sivanesan et al. 2018] authors propose an open source simulator of block-less network to implement distributed ledgers, that the authors claim being more suitable for cyber physcal systems. The systems being modeled by simulator are fee-less, so it is not possible to observe or analyse economical phenomena. In [Taylor 2017], authors examine how the advent of proof of work cryptoasset ledgers has shaped the digital design efforts into the implementation of ad hoc hardware to optimize resolution of proof of work puzzles. In [Fairley 2017], the author depicts the concerns of a scenario of evergrowing power demand for mining, under conditions that he describes as a "perfect storm": "Those efficiency gains are slowing while bitcoin value is rising fast-and its potential transaction growth is immense". An interesting phenomenon is the formations of "pools" in which miners put their computational power in common, and share the rewards they get. This way, the expected income value doesn't change, but the rewards are more predictable in time (variance in time diminishes). In [Qin et al. 2018], authors study the problem, from the perspective of a miner, of how to select a pool, based on the reward mechanisms that the pools offer. They then go on at using simulation to validate the pool selection strategies outlined.

3. MINE WITH IT OR SELL IT: POSSIBLE STRATEGIES

As you know, with great power comes great responsibility. Indeed, being able to develop a substantial technological advancement in the field of cryptocurrencies mining, mainly in terms of mining efficiency, does not directly imply a positive outcome neither for the blockchain community nor for the personal business of a super-miner i.e., a miner who has access to the boosting technology. In order to avoid the collapse of the blockchain ecosystem, it is necessary to carefully evaluate the different super-mining strategies that can be applied:

1. Underuse the superhashing technology, in order to either:
   - 1.1. Reduce the cost of mining, maintaining constant the hashing power, or
   - 1.2. Increase the hashing power, maintaining constant the mining cost.

   The impact of this strategy on both the personal business of the single miner and the blockchain ecosystem is almost negligible, unless the increase in the efficiency reaches astonishing levels (e.g., several order of magnitude);

2. Exploit the superhashing technology by increasing (in a controlled way) the number of mining devices (or RIG) employed, thus increasing both hashing power and mining cost, but with a much better/lower coefficient in terms of cost/hash. This can be done by pursuing one of the two following paths:
   - 2.1. Personally exploiting the produced mining devices in order to take advantage of the mining rewards, but with the drawback of increasing the centralization of the blockchain control with the growth of the total hashing power generated;
   - 2.2. Selling the technologically advanced devices to different network actors, thus earning money by selling to other players the possibility of obtaining higher mining rewards thanks to the new hardware (with a small risk of someone being able to replicate the same technological advancement).

3. Abuse the superhashing technology, introducing in the network enough highly efficient mining hardware to reach the extreme consequence that it is not profitable anymore to mine with other hardware devices with lower efficiency levels. The social outcome of this scenario strongly depends on the number of miners involved. In particular:
   - 3.1. If all the newly introduced hashing power belongs to the same miner, the blockchain collapse in a completely centralized platform, thus losing all its appeal and, probably, most of its value;
   - 3.2. On the other hand, if multiple miners are involved, the network will simply adapt with a new difficulty, thus resulting in a final situation characterized by a different distribution of the hashing power, but with a possibly similar level of decentralization. In this case, the introduction of the new highly efficient hardware simply results in a sort of non-recurring tax that has to be paid in order to remain involved in the mining activity.

The main metrics to be considered in the last two scenarios are both the number of new mining devices introduced in the network (m) and their increase in efficiency with respect to the existing hardware (k). Evaluating how these two factors influence the stability of the network and the behaviour of the other miners makes possible to better understand the implications of superhashing utilization, and helps in defining the better exploitation strategy in terms of economic rewards.

4. SIMULATIONS

In this section, we present a multi agent model we designed in order to validate our hypothesis regarding different responses that the network may show for some possible strategies. An open source Python implementation of the model, based on the framework MESA [Kazil and Vērzemnieks 2018], is available on GitHub [Gentile et al. 2018].

4.1 Model

The main entities of the model are the network and a set of mining pools. In our simulations we tuned parameters taking into consideration Ethereum on September 2018. The network is mainly characterized by:

- Total hash rate;
- Reward, in term of cryptoasset, given for mining a block;

- Block time, that is the average time the network spends to mine a block;
- Number of mining pools;
- Average number of machines per mining pool;
- Energy consumption per machine;
- Maximum hash rate per machine without using the boosting technology;
- Cryptoasset value with respect to fiat currency. At the moment we assumed that this value is constant;
- A decentralization index, based on the Gini index of the mining pools' hash rates.

A mining pool is instead mainly characterized by:

- Boosting technology hash rate multiplier (k), that represents the technological competitive advantage a mining pool may have with respect to others. It allows to mine k-times faster than others, without increasing the energy consumption;
- Hash rate per machine, that is given by the product of the maximum hash rate per machine without using the boosting technology of the network and k;
- Number of machines (m) adopted by the mining pool;
- Hash cost, that is computed taking consideration the energy consumption per machine and m;
- Expected profit per block, that is the main factor a mining pool takes into consideration in order to start or stop mining.

A mining pool strategy is then defined as a couple (k, m). An increase of k may represent an investment of a mining pool in improving state of the art technology. An increase of m may represent an investment of a mining pool in buying new hardware. Therefore, it is possible to use the model to evaluate the impact of an investment. The model assumes time is discrete and one unit of time is represented by the block time. At each step of the model its internal time is implicitly increased by one unit and a mining pool is randomly selected as the winner of the PoW puzzle with a probability that is proportional to its hash rate percentage with respect to the total hash rate of the network. PoW is neither computed nor verified, because we assume mining pools do not cheat in our simulated environment. After PoW puzzle, each mining pool, in a sequential random order, computes its expected profit and eventually changes its strategy. At the moment we simulated scenarios in which just a single mining pool, called super mining pool, can change k and m. Other mining pool are allowed to just start or stop mining taking into consideration their expected profit.

4.2 Experimental results

Here we present some plots representing different responses of the network in case the super mining pool adopts the strategies defined in the chapter 3. Note that the super mining pool is identified by index 0.

We first show the case of strategy 1.1. If the super mining pool adopts k = 1 we observe that m = 100000 is required in order to be a competitive mining pool. If k = 10, of course both the number of machines required to obtain the same hash rate and the hash cost are reduced by factor 10. As expected, if m = 10000 and k = 10 we observe a physiological oscillatory behavior of the number of active mining pools (Figure 1).

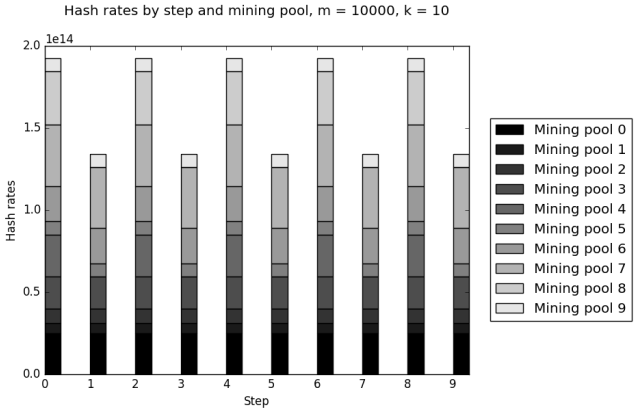

Figure 1: Hash rates by step and mining pool, m = 10000, k = 10

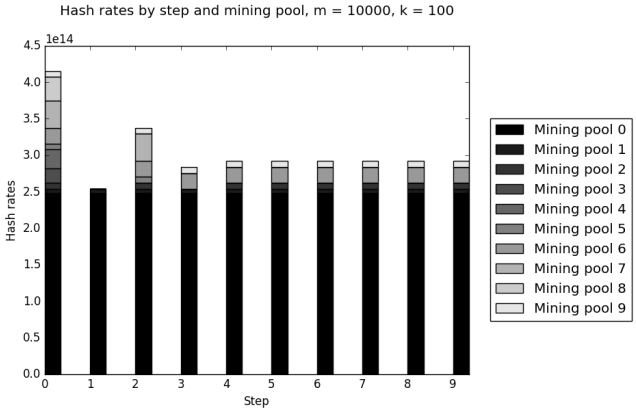

Figure 2: Hash rates by step and mining pool, m = 10000, k = 100

We consider now the case of strategy 2.1. The adoption of the boosting technology by the super mining pool, without abusing it, perturbes the number of active mining pools until a new equilibria is found and increases the network centralization (Figure 2).

Finally, we show the case of strategy 3.1. In this case all mining pools, except the super mining pool, go out of business (since mining is no profitable) immediately and the network is completely centralized (Figure 3).

We see also that if the super mining increases too much its number of machines, then he will go too out of business (Figure 4).

We now show a summary plot comparing when only the super mining pool is active i.e., he totally controls the network and get all the rewards and when no mining pool is active i.e., for no mining pool the activity of mining is profitable)(Figure 5). We observe that for k lower than 2, the

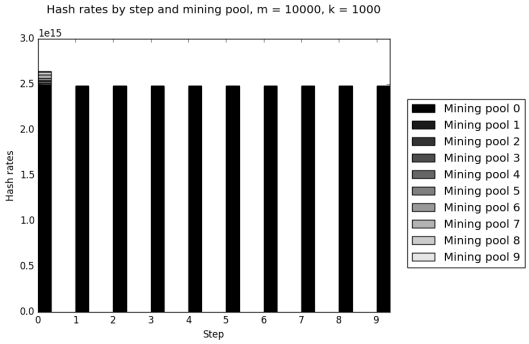

Figure 3: Hash rates by step and mining pool, m = 10000, k = 1000

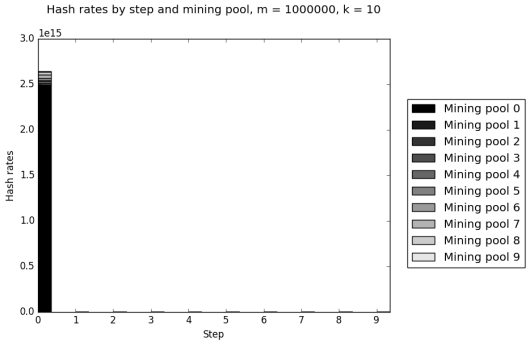

Figure 4: Hash rates by step and mining pool, m = 1000000, k = 10

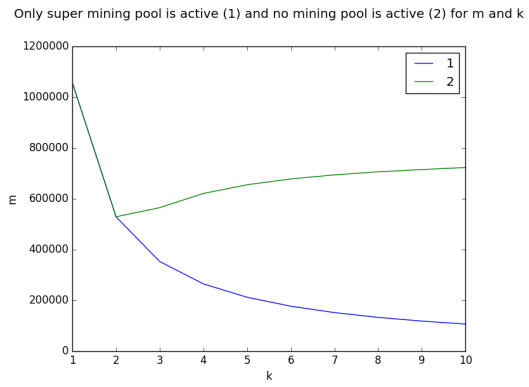

Figure 5: Only super mining pool is active (1) and no mining pool is active (2) for m and k

super mining pool can control the network but without any profit. If we consider k greater than 2, the more it grows the more significant is the profit of the super mining pool.

5. CONCLUSION AND FUTURE WORK

In this paper, we consider the incentives to design more powerful hardware in proof of work based cryptoassets systems. In particular, we considered how naive exploitation policies can have problematic side effects. We analysed different strategies, and evaluated them with a simulator, that we released open source. The experiments show an upper bound on the hashing power improvement that can be injected into the network before compromising its decentralization. Future work could consist in taking into consideration more complex mining strategies for any miner and generalize the model by decreasing the strictness of the underlying assumptions.

6. REFERENCES

Cynthia Dwork and Moni Naor. 1993. Pricing via Processing or Combatting Junk Mail. In *Advances in Cryptology — CRYPTO' 92*, Ernest F. Brickell (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 139–147.

P. Fairley. 2017. Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous. *IEEE Spectrum* 54, 10 (October 2017), 36–59. DOI: http://dx.doi.org/10.1109/MSPEC.2017.8048837

L. Gentile, V. Rana, and F. Bruschi. 2018. Incentive network simulator. (2018). https://github.com/lorenzogentile404/incentive-network-simulator

J. Kazil and N. Vērzemnieks. 2018. MESA. (2018). https://github.com/projectmesa/mesa

R. Qin, Y. Yuan, and F. Wang. 2018. Research on the Selection Strategies of Blockchain Mining Pools. *IEEE Transactions on Computational Social Systems* 5, 3 (Sept 2018), 748–757. DOI: http://dx.doi.org/10.1109/TCSS.2018.2861423

M. Sivanesan, A. Chattopadhyay, and R. Bajaj. 2018. Accelerating Hash Computations Through Efficient Instruction-Set Customisation. In *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*. 362–367. DOI: http://dx.doi.org/10.1109/VLSID.2018.91

M. Bedford Taylor. 2017. The Evolution of Bitcoin Hardware. *Computer* 50, 9 (2017), 58–66. DOI: http://dx.doi.org/10.1109/MC.2017.3571056