Miners and the Blockchain: An Agent Based Model Approach To Understand Behavior In Mining Pools

Chris Fennell
Michigan State University
East Lansing, MI, USA
cfennell@msu.edu

Presented at the *CHI'18* Workshop on HCI for Blockchain, April 21-26, 2018, Montreal, Canada.

Abstract
Cryptocurrencies today represent a shift in trust from centralized banks to a decentralized network otherwise known as a blockchain. One of the most important components of blockchains are the individuals who maintain it: the miners. While Bitcoin remains the most well known currency, other alt-currencies have emerged and many miners have created/purchased specialized machines to maintain the blockchain for the block reward offered by owners of these currencies. Through agent based modeling, I simulated miners behavior in which individuals choose between staying or leaving an alt-currency. Results show that miners are sensitive to the total hashrate of a cryptocurrency they are mining. Significant dips can cause the other miners to leave the blockchain for another blockchain with a higher expected payoff.

Author Keywords
Cryptography; Cryptocurrency; Blockchain; Mining

ACM Classification Keywords
H.1.2 [User/Machine Systems]: Human factors; H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction

Individuals can choose from a plethora of cryptocurrencies today and while some are well known such as Bitcoin, Litecoin, or Ethereum, there are in fact many more to choose from. As a result, Cryptocurrency markets have emerged and have been described as very volatile [8]. As an example, the current price at the time of the writing of the book by Brito and Castillo titled "Bitcoin, a Primer for policy makers" in April 2013 was $260 [1] but the current price as of January 2018 was $11,445. The price even peaked as high as $19,500 [4]. Yet while we are interested in studying the impact of the cryptocurrency market there is a distinction that needs to be understood first: miners.

Fundamentally, the blockchain is a decentralized ledger and can be thought of a collection of all the transactions for a given cryptocurrency. There are many types of protocols that manage the distribution of rewards but the one that is used predominantly in blockchain is *Proof of Work* (PoW). As an example, Bitcoin was built on a *Proof of Work* in which miners are the fundamental component of the decentralized network. Miners would use highly customized computer rigs to validate each block in the blockchain. With this protocol, there must be incentives offered that would help maintain the ledger. In the case of PoW cryptocurrencies distributing a small reward is an elegant system that gives miners compensation in the form of currency [7].

Mining Pools

In the blockchain, each new block that is generated needs to be verified. As a result of verifying the block, a reward is given in the form of cryptocurrency. Since the blocks are solved in order, the miners compete against each other for the reward. The miners can estimate how quickly they can solve a block based on the rate that they can "hash" a block. This rate is known as a hashrate and is typically displayed in hashes per second (Hs) though other variations do exist. Each subsequent block increases in difficulty slightly and as a result the hashing power is not as effective as before.

One way around the conundrum of competing is for miners to pool their collective computational powers and work together to obtain the reward. The upside of the pool approach is that the miners now are receiving more rewards because they are verifying the blocks together. The hashing rate is an interesting metric because not all miners are equal. Like many types of markets or investments, not all miners have the same capital. Some are hobbyists miners possessing a relative small hashing power while others have nearly unlimited resources and can obtain orders of magnitude greater hashing power. If placed on a continuum, the hash rate per second can go from (almost) 0 hashes per second to Tera hashes (or even higher) and the greater the hash rate the higher the payout. Many pools have fees (usually $\approx$1%) yet despite that miners choose to operate within a pool because pooling resources reduces the variance in the payouts. Lewenberg et al [5] examined bitcoin pools and examined how miners could switch between pools. They concluded that miners are motivated to switch between pools to increase their expected payout. In recent years, the rise of other PoW cryptocurrencies have emerged and miners have the choice of choosing between different cryptocurrencies with the hope of increasing their expected payout.

Agent Based Model

Cryptocurrencies are difficult to understand because they represent a complex system that ties a currency to a decentralized network. One way researchers have explored the behaviors and effects of individuals is through simulation of Agent Based Models (ABM). William Luther's [6] model looked at the network effects and switching costs of agents and Cocco et al [2] model explored traders and chartists by trading bitcoins. While both use bitcoin as a currency, neither view the perspective of miners who are choosing to partake in mining.

Work in Progress

The early work I've conducted examines miners as a key stakeholder in maintaining the blockchain. This work has focused on understanding the miners use of mining pools through the NETLOGO software[10]. For this model, I set up a simulated world that places two types of agents into our world: Miners and cryptocurrency blockchains. The model is designed to simulate a world with between 1 and 5 cryptocurrency blockchains. Each cryptocurrency in this model calculates an expected payout which is dependent on the total number of miners supporting each blockchain.

Variable	Value
Miners	50
Blockchains	5
Money distribution	Exp. Dist.
Evaluation Freq.	100
Exchange rate	up to 1.0
Max Ticks (hours)	8760

Table 1: ABM Experiment Parameters

The agent of interest in this context would be the miners. These individuals have built/purchased specific equipment in order to mine for a specific cryptocurrency. While it is possible that miners can spread their risk by mining different currencies, for this model it is assumed that miners would focus on one currency at a time. This would be in keeping with the DIY type mining market in which users build small machines as a form of hobby and would have a small mining setup. So, the miners in this sense could not afford to spread their work to multiple currencies because it would a) be inefficient by reducing hashing power for a currency b) decrease risk by increasing the probability for an efficient rate of return. Another important assumption is that the model does is that it does not simulate the mining for blocks but rather it simply models miners mining in pool. Miners were assigned a random hashrate which ranges from 0 to the default hashrate value. Additionally, the miners were also assigned an initial monetary value which was distributed based on an exponential distribution.

Condition	Action
Amount Mined >= Expected Payout	Continue Mining
Amount Mined < Expected Payout	Move to Cryptocurrency with highest expected payout

Table 2: Miner's Decision in the ABM

For the blockchains in the model, I wanted to get a general sense of how the model functions with a small number of miners and blockchains (See Table 1). I created an experiment in which the miners were assigned money according to an exponential distribution. This would allow most miners to have some money but a few miners would have significantly more than the others. The miners in the model have decided to "mine" but the key behavior that we are trying to model is which blockchain are they choosing to maintain.

For this ABM, the model advances through each tick which i have decided to labels as hours. So with each tick, an hour would have passed in a day. The miners make a decision to mine or not at an evaluation frequency which is set to 100 hours for this experiment. The decision logic is outlined in Table 2. If the amount they mined is greater than or equal to their expected payoff the miners continue to mine. Only when the amount mined by the miners is less than the expected payoff do the miners look for a blockchain with the highest payout. While in real world scenarios there may be other decisions that would affect the miners, the ABM model allows us to focus on the simplest behaviors in order to see how they interact with other variables. One important note is that if miners decide to leave it could be that the blockchain that they are currently mining is in fact the highest expected payout between all five blockchains. Finally, the experiment terminates after 8760 hours or a period of one year.

The results show (see Figure 1) amounts mined during each evaluation period during which the miners calculate their expected payoff. We can infer here that when the miners leave a market it causes one to market to go down and another to go up. Walking through the graph in terms of ticks shows us that Alt Currency 3 had the initial peak but then individuals shifted to Alt Currency 4 and to a lesser extent Alt currency 0. At around 4000 ticks the evaluations had shifted back to Alt Currency 3. We can also see that Alt Currency 1 and 2 never peaked like the others. From this we can infer that a few of the miners moved from one currency to another but later in the scenario, at around 6000 ticks, you can see that nearly all of the miners were moving between currencies. We cannot infer which currency they moved to/from in this graph but only that they did move. As expected, the expected payoff was important but what was interesting was how the model functioned in relation to the other variables. Hashrate in this model was endogenous to the expected payout by having it be a factor in the formula to calculate the payout. While this might seem obvious that the hashrate affected the expected payout, what became more clear through the modeling was the effect of the hashrate on the cryptocurrency itself.

Andrew Hayes [3] explored and analyzed over 66 cryptocurrencies in order to develop a model for cost of production of cryptocurrencies. He did so to come up with a way to give a value indicator to bitcoin. His conclusion was that as more miners enter the blockchain network it increases the overall hashing power of the currency and as a result influences the price. This model seems to support that finding by showing that when the miners expected payout is not met, they leave the market but by doing they decrease the

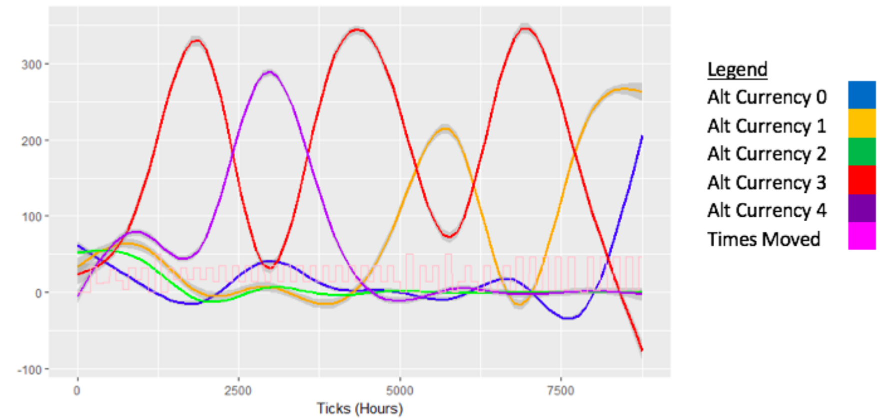

Figure 1: Insert a caption below each figure.

hashrate of that blockchain. When small scale miners leave a cryptocurrency the effect on price is predictably largely unchanged but if a miner with significant hashing power were to leave a cryptocurrency the effect would be more pronounced. It could lead to the collapse of a cryptocurrency.

An article by Quartz magazine [11] found that the bitcoin company Bitmain accounted for 29% of mining activity for that currency. Imagine for a moment if the Bitmain company decided to leave the bitcoin network. The impact on the network would be catastrophic because the slower the hashing ability the slower the blocks can be solved. Individuals who expected to use the blockchain to transfer currency would be at the mercy of the now sluggish decentralized network. At the same time however, Bitmain could redirect its effort to a different alt currency and that currency would then begin to rise.

Limitations and Future Work

Like many experimental methods, manipulating certain features limits its extensibility. This is often done so researchers might maintain experimental control and in the case of agent based models, it allows researchers to test what they would not otherwise be able to test. One limitation is that this model looks at mining the blockchain for a cryptocurrency and really pays no attention to other market features such as volume or trade of the cryptocurrency market. A more robust model could incorporate more complicated market features and could offer additional insight. However it is unclear what the benefit of creating a "perfect" cryptocurrency marketplace would be. New coins enter the market daily and others seemingly collapse never to be heard from again.

For PoW cryptocurrencies, Miners maintain the blockchain by validating the transactions on the network. These individuals may have decided that they want to be a part of the decentralized effort to have a truly unregulated currency that lacks government interference. Or it could be that their motivation is purely capitalisitic brought on by the profitable incentives for mining. With the price of cryptocurrencies continuing to fluctuate it would seem like a bit of a gamble to purchase or build customized computers to maintain the blockchain. However, Polygon magazine [9] reports that as of January, 2018 there is a global shortage of Graphic Processing Units (Video Cards) due to the demand brought on by cryptocurrencies. So until the market comes back down, it would seem that there will be continued demand for miners.

Miners also represent a unique and interesting population that is warrants further exploration. Since not all PoW cryptocurrencies are like bitcoin, it warrants that we should analyze miners across the different types of currencies. Ethereum for example places emphasis on smart contracts. If its blockchain is used for other applications than just exchange of currency, then the loss of the miners not only represents a slower transaction times but also any application built upon that network is also at risk.

Personal Bio

Chris Fennell is a second year PhD Student in Media and Information at Michigan State University and is currently pursuing research exploring the socio-techincal impacts of technology and cybersecurity. Chris is interested in why individuals are choosing to invest in cryptocurrencies and the miners that support the blockchains. He is also research assistant in the Behavior and Information Technology Lab (BITLab) at MSU and has been investigating how people learn about passwords.

REFERENCES

1. J Brito and Andrea Castillo. 2013. Bitcoin: A Primer for Policymakers. *Mercatus Center: Geroge Mason University.* 29, 4 (2013), 3–12. DOI: http://dx.doi.org/10.1017/CBO9781107415324.004

2. Luisanna Cocco, Giulio Concas, and Michele Marchesi. 2017. Using an artificial financial market for studying a cryptocurrency market. *Journal of Economic Interaction and Coordination* 12, 2 (2017), 345–365. DOI: http://dx.doi.org/10.1007/s11403-015-0168-2

3. Adam S. Hayes. 2017. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics* 34, 7 (2017), 1308–1321. DOI: http://dx.doi.org/10.1016/j.tele.2016.05.005

4. Timothy Lee. 2018. Bitcoin Plunges - now down 47 percent from December peak. (2018).

https://arstechnica.com/tech-policy/2018/01/bitcoin-plunges-now-down-42-percent-from-december-peak/

5. Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S. Rosenschein. 2015. Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems (AAMAS '15)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 919–927. http://dl.acm.org.proxy1.cl.msu.edu/citation.cfm?id=2772879.2773270

6. William J. Luther. 2016. Cryptocurrencies, Network Effects, and Switching Costs. *Contemporary Economic Policy* 34, 3 (jul 2016), 553–571. DOI: http://dx.doi.org/10.1111/coep.12151

7. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and cryptocurrency technologies*. Vol. 1. Princeton University Press.

8. Michal Polasik, Anna Iwona Piotrowska, Tomasz Piotr Wisniewski, Radoslaw Kotkowski, and Geoffrey Lightfoot. 2015. Price fluctuations and the use of bitcoin: An empirical inquiry. *International Journal of Electronic Commerce* 20, 1 (2015), 9–49. DOI: http://dx.doi.org/10.1080/10864415.2016.1061413

9. Samit Sarkar. 2018. Graphics card shortage leads retailers to take unusual measures. (2018). https://www.polygon.com/2018/1/26/16936984/graphics-card-gpu-prices-nvidia-amd-cryptocurrency-mining-stores

10. Uri Wilensky and William Rand. 2015. *An introduction to agent-based modeling: modeling natural, social, and engineered complex systems with NetLogo*. MIT Press.

11. Joon Ian Wong. 2017. China's Bitmain dominates bitcoin mining. Now it wants to cash in on artificial intelligence. (2017). https://qz.com/1053799/chinas-bitmain-dominates-bitcoin-mining-now/it-wants-to-cash-in-on-artificial-intelligence/