Toward Socially Optimal Bitcoin Mining

Zhen Li
Department of Economics and Management
Albion College, USA
Email: zli@albion.edu

Qi Liao
Department of Computer Science
Central Michigan University, USA
Email: liao1q@cmich.edu

***Abstract*—Bitcoin is a cryptocurrency for managing and transferring money in a distributed manner. The Bitcoin network creates a complex system of economic incentives that governs its inner working, impacting the network's security guarantees and its evolution. Recent development of Bitcoin as a speculative asset and the herein skyrocketing Bitcoin price greatly incentivize participation in the network. We posit that the expansion in Bitcoin miner population and speculative transactions may not be socially desirable. The increased competition in Bitcoin mining not only exacerbates energy consumption and environmental cost, but also makes the risky mining business much riskier. In addition to the risk of unstable reward flows, the fluctuation in Bitcoin price makes the profitability of mining more uncertain. This research studies an alternative socially optimal model for the Bitcoin market (and other cryptocurrencies in general). Through equilibrium analysis, we emphasize the need to limit speculation in Bitcoin transactions, improve efficiency, diversify currency portfolio, and minimize negative externalities of the Bitcoin mining business.**

***Index Terms*—Cryptocurrency, Bitcoin, mining, competition, blockchain, economics, pricing, optimization, social optimum.**

I. Introduction

As a decentralized cryptocurrency, Bitcoin adopts a distributed consensus protocol to maintain a block chain that stores transaction history. Users of Bitcoin broadcast the transactions over a peer-to-peer network and the so-called miners collect blocks of transactions, verify their integrity, and append them to the block chain. Miners are motivated by receiving reward with newly mined Bitcoin and transaction fee.

The decentralized nature of the Bitcoin network guarantees its security. The transactions and the blocks are chained via cryptographic hash functions which are too computationally expensive to forge and falsify. Mining is a process of verifying transactions and building new blocks. In seek of reward, miners may be tempted to mine multiple blocks. Consequently, the decentralized block chains generate competition among miners. To ensure fairness, Bitcoin protocol requires a proof of work.

The proof of work utilizes the pre-image and collision resistance properties of secure hash functions and forces mining nodes to a brute-force approach to solve artificially-made problems. When one miner finds the correct input value, the computation results by other nodes are all wasted. The most direct impact of such practice is the energy cost. Mining blocks causes huge energy waste and pollution. The energy consumption of mining is at least linearly increasing in the number of competing miners. If the miner population is big enough, the energy cost of mining Bitcoin would exceed the value of Bitcoin and become unsustainable, a less than ideal situation from the perspective of social optimum.

Cryptocurrency has seen tremendous growth in less than a decade and so was the price. The first known Bitcoin purchase for goods (10,000 bitcoins were used to purchase two pizzas) took place in May 2010 when Bitcoin got its value working as medium of exchange. In 2013, Bitcoin price hit $1,000 mark rising from just $10. Recently, Bitcoin price rose from $900 to $19,000 in the year of 2017. While there has been substantial growth in the number of Bitcoin transactions, the number does not represent transactions for goods and services but rather any movement of Bitcoin around the network. Bitcoin nowadays is largely perceived as a financial investment asset and speculation.

Like any good or service traded in the market, the price of Bitcoin is determined by joint forces of supply and demand. The supply of Bitcoin comes from block mining. Bitcoin's rate of block creation is kept constant by the protocol. With roughly constant supply rate of Bitcoin, the market price of Bitcoin is mainly determined by the demand for Bitcoin, comprising both transaction demand and speculative demand.

As the price of Bitcoin rises, mining becomes more lucrative as a whole. More participants find it profitable to join the group of miners, and, as a result, the difficulty of block creation via the proof-of-work increases. While the increased miner population induced by high Bitcoin price is generally to the advantage of security of the Bitcoin network, such practice also results in severe competition and a lose-lose consequence for individual miners and the society overall, especially in the case of rising speculative demand for Bitcoin.

To deal with the dilemma, a number of protocols [1]–[4] have been proposed to either modify or replace the proof-of-work for better sustainable energy consumption. Instead of tackling the implementation of protocols themselves, we provide an alternative economic solution to such problem. In particular, we build an economic model based on individual decision-making in the mining business, and derive an equilibrium solution of mining participation rate that is not only utility maximization for miners but can also be used to achieve social optimum.

Through equilibrium analysis, we suggest that price leverage be used to deal with the miner population dilemma. As a virtual currency, the true value of Bitcoin comes from its

function serving as medium of exchange. Through restriction of speculative trade and diversification of virtual currencies, we can improve efficiency and reduce uncertainty, thus reducing wasteful competition in cryptocurrency mining business.

The rest of the paper is organized as follows. Section II reviews background and related work. Section III analyzes the supply and demand of Bitcoin market. Section IV formulates the optimization problem, and analyzes individual miner's decision-making and socially optimal level of mining participation. Various factors determining the model solutions are identified, especially the role of Bitcoin price. Finally, Section V concludes the paper.

II. Background and Related Work

Miners in cryptocurrency networks contribute computational power to maintain, secure, and extend the networks. However, there have been growing competitions among mining communities of cryptocurrency such as Bitcoin. A Bitcoin transaction is only considered valid once the system obtains proof that a sufficient amount of computational work has been exerted by authorizing nodes. To achieve this, miners constantly attempt to solve cryptographic puzzles in the form of a cryptographic hash computation. The only known method to find the hash is by random search or brute force approaches. When miners compete to mine a block, with no cooperation, only one miner will be rewarded, and the rest will gain nothing. In addition, only transactions on the longest chain are considered valid, so the volume of transactions the Bitcoin network can process depends on the rate of block appended to the longest chain, but not the total number of blocks mined.

The expansion in miner population increases the cost to individual miners and the society concerning energy consumption. There is an incentive to increase the amount of computing power that any individual user is contributing to increase their chances of finding a new block. In such an environment with no property rights assigned for future Bitcoin, there is likely to be overprovision of computing power, and the majority of mining effort is futile. The competitive environment derived from the difficult adjustment algorithm through the proof-of-work results in huge energy waste, which has been recognized in early research. Technical approaches have been suggested such as variants of protocol [1], [2], proof of something [3], or proof of useful work by solving practical problems [4].

In addition to energy waste, competitions among the growing mining populations also lead to large variance in reward for miners. One possible approach is to join mining groups. Since mining reward is not guaranteed, especially in the current competitive environment, miners who desire a steady income flow collaborate in pooling strategies where they jointly mine for Bitcoin and share the reward. Geometric pay pool is found optimal [5] out of pooling strategies in use. The pool presents itself as a single powerful node to the Bitcoin network thus it is able to gain an advantage over outsiders. In recent years, efforts of mining intensified to such a degree that most mining quickly transitioned to dedicated computer farms that use specialized gears. Nevertheless, it may be hard to distribute the pool's reward among members in a stable way so that miners would not switch pools. Such instability increases as the network processes high transaction loads [6]. While pooling strategies smooth income flows to member miners to certain degree, they do not reduce energy use of mining.

The increasing mining competition is related to the high price of Bitcoin. Empirical findings show that market forces of supply and demand have an important impact on Bitcoin price [7]. The supply side does not have significant effect [8], while the demand-side drivers such as the popularity of Bitcoin affect its price formation more significantly [9]. An increase in trade volume is correlated with Bitcoin price [8].

As a virtual currency, Bitcoin operates collaboratively without the need of financial intermediaries [10]. As an investment asset, Bitcoin is found to have a role in portfolio diversification [11]. Most users treat their Bitcoin investment as speculative assets rather than as means of payment [12]. Bitcoin is found to be a unique asset possessing properties of both a standard financial asset and a speculative one [8]. Bitcoin is largely detached from fundamentals and behaves as a speculative bubble [13]. The success of Bitcoin hinges on its ability to reduce the potential negative implications of speculations and expand the use of Bitcoin in trade and commerce [7].

III. Analysis of the Bitcoin Market

Given the predetermined rate of Bitcoin reward, Bitcoin price plays an essential role in determining miner population. Like other markets, Bitcoin market price is determined by the joint forces of supply and demand. In this section, we conduct a supply-demand analysis to study the determination of Bitcoin price and its fluctuations.

There are two main types of agents participating in the Bitcoin network: traders who trade in the virtual currency, and miners who validate Bitcoin transactions. The miners supply newly mined Bitcoin to the market, but they do not control the rate at which Bitcoin supply increases. The supply of Bitcoin is predetermined and perfectly inelastic. The traders demand for Bitcoin. To model the demand side of the Bitcoin market, we focus on the payment and investment features of Bitcoin and include two components of demand: transaction demand and speculative demand.

Since early days, Bitcoin has been used as an online medium of exchange, i.e., using Bitcoin to exchange for real goods. The demand for Bitcoin as a medium of exchange depends on customers and merchants to accept Bitcoin as one of the payment methods. In recent years, Bitcoin has developed into an investment asset. People trade Bitcoin for speculative purpose. It is unusual for an asset to function both as a medium of exchange and a speculative asset. The emergence of Bitcoin market actually changes the nature of Bitcoin from being a medium of exchange to a pure asset. Since Bitcoin becomes a good by itself, using Bitcoin to buy other goods becomes barter trade.

Different from conventional goods and services, the embedded value of Bitcoin is the possibility that it is accepted as a medium of exchange. How widely is Bitcoin accepted

TABLE I: Symbols in modeling analysis.

Symbol	Description
B	units of Bitcoin rewarded to the winning miner (supply)
P_B	current dollar value per unit of Bitcoin
P_B^E	expected price of Bitcoin in the future
P	general price level of goods and services
Y	quantity of goods and services traded using Bitcoin as medium of exchange
V	velocity of Bitcoin (the frequency at which one unit of Bitcoin is used for purchasing goods and services)
S	unit of Bitcoin demanded for speculative purpose
R	risk-adjusted return on Bitcoin investment
N_i	mining attempts per second for miner i
D	total mining attempts per lifetime of mining equipment
F	mining equipment replacement cost
c	average energy consumption per mining attempt
a	degree of risk aversion
p	success rate of each mining attempt
M	miner population
M_s	socially optimal miner population

determines its inherent value. When Bitcoin is traded as an asset, the inherent value becomes its fundamental value. Investors of Bitcoin reserve the right of using Bitcoin to buy although they largely seek potential capital gains. The purchasing power of Bitcoin depends on the current market price of Bitcoin.

We extend the classical Quantity Theory of Money to find the equilibrium price of Bitcoin. The transaction demand for the units of Bitcoin is defined as $\frac{PY}{P_BV}$ (refer to Table I for the explanations of symbols). The equilibrium condition between Bitcoin supply and demand satisfies

$$B = \frac{PY}{P_BV} + S \tag{1}$$

Therefore, the Bitcoin price is

$$P_B = \frac{PY}{(B-S)V} \tag{2}$$

Apparently, as the speculative demand for Bitcoin increases, the dollar value of Bitcoin increases. Investors desire a risk-adjusted return of R on Bitcoin investment, i.e., $R = \frac{P_B^E - P_B}{P_B}$. Accordingly, we can write the current Bitcoin price in the following way:

$$P_B = \frac{P_B^E}{1+R} \tag{3}$$

The speculative demand for Bitcoin is essentially from the expected increase in future Bitcoin price, which is further related to the expected expansion in the fundamentals (the use of Bitcoin to buy goods and services).

Combining Equations (2) and (3), we solve for the units of Bitcoin investors demand for speculative purpose:

$$S = B - \frac{PY(1+R)}{EP_BV} \tag{4}$$

According to Equation (4), the speculative demand for Bitcoin increases as the market expects the Bitcoin price to rise. It also provides a plausible explanation regarding how the transaction demand for Bitcoin may affect speculative demand for Bitcoin. In particular, as the transaction need increases, the price of Bitcoin increases. Given expected Bitcoin price, the speculative demand for Bitcoin would decrease. In total, the combined demand for Bitcoin must be equal to the fixed supply of Bitcoin.

IV. Bitcoin Price and the Scale of Mining

We are motivated by the question: does there exist an equilibrium mining participation rate? In this section, we relate the supply and demand modeling analysis in the previous section and study how pricing may affect miners' utility maximization problems.

Since miners differ in terms of computational power, suppose Miner i can make N_i attempts per second. At Bitcoin price P_B, the value of reward is P_BB. For the entire M miner population, the total number of attempts per second is $\sum_{i=1}^{M} N_i$. Currently, the Bitcoin protocol allows Bitcoin reward to be mined in roughly every 10 minutes so the total number of attempts necessary to mine new Bitcoin is $\sum_{i=1}^{M} N_i \times 600$. At the fixed time interval necessary to receive reward, the total number of attempts is increasing in the miner population. After these attempts, a random miner receives reward, and the other miners gain nothing.

Mining cost is modeled by energy consumption and equipment depreciation. The per-attempt cost of mining is defined as $\frac{F}{D} + c$. For simplicity, we assume such cost structure applies to all miners.

The value of Bitcoin to the society lies in its function to serve as medium of exchange. The financial investment use of Bitcoin, however, does not add value to the society because the capital gains and losses result in merely transferred wealth among Bitcoin investors. The social optimum requires the scale of miner population M_s to equilibrate the social benefit and cost of mining:

$$P_B(B-S) = (\sum_{i=1}^{M_s} N_i)(\frac{F}{D} + c) \tag{5}$$

where $(B-S)$ is the part of Bitcoin reward used for purchasing goods and services. In Equation (5), the time interval required to release reward is normalized to one. Since it is held constant internally by the protocol, the simplification does not affect model conclusions.

To the mining business nevertheless, the reward from mining is P_BB regardless whether Bitcoin is used as medium of exchange or speculative purpose, thus for the whole mining business to reach equilibrium:

$$P_BB = (\sum_{i=1}^{M} N_i)(\frac{F}{D} + c) \tag{6}$$

Comparing Equations (5) and (6), $M_s < M$. When there exists speculative demand for Bitcoin, the scale of mining will be higher than socially desirable. The over-mining phenomenon can be more severe if we also consider *external* costs of Bitcoin mining such as pollution.

For the whole miner population, there is no uncertainty in the payoff since after some preset amount of time, a certain amount of Bitcoin is rewarded. However, for individual miners, mining is highly risky. The release of reward is a random process with a large variance, especially as competition gets fierce.

A miner makes repeated attempts to solve a computationally difficult puzzle in order to win reward. Each attempt is independent so that at each renewed attempt, the miner has the same probability of receiving reward. If every attempt is a Bernoulli trial with success rate p, then the number of reward out of N_i attempts by Miner i has a Binomial distribution with expectation pN_i and variance $p(1-p)N_i$. The value of reward of each attempt is pP_BB, and pN_iP_BB for all N_i attempts.

The miner's goal is to maximize net expected reward from mining. Suppose the miner is risk averse with a concave utility function $U(x) = x^a$. The miner's decision-making is therefore:

$$\max_{N_i} U(N_i) = (pN_iP_BB)^a - (\frac{F}{D} + c)N_i \tag{7}$$

where $U(N_i)$ is the net expected utility for Miner i out of N_i mining attempts. The parameter $0 < a < 1$ measures the degree of risk aversion. $p = \frac{1}{\sum_{i=1}^{M} N_i}$ so that all M miners combined will receive a sure reward of P_BB, i.e., $\sum_{i=1}^{M}(pN_iP_BB) = P_BB$. In Equation (7), the reward is a risky reward, and the cost is a sure cost. The miner's control variable is the number of mining attempts.

From the first order condition of Equation (7), the utility-maximizing number of mining attempts for Miner i is

$$N_i^* = (\frac{a(pP_BB)^a}{\frac{F}{D} + c})^{\frac{1}{1-a}} \tag{8}$$

The derived solution in Equation (8) suggests key factors determining individual miner's choice of mining participation:

- The quantity of Bitcoin rewarded per fixed time interval (B): more Bitcoin rewarded incentivizes mining attempts.
- Mining cost ($\frac{F}{D} + c$): increasing costs of mining equipment and energy use discourage mining.
- The level of risk aversion (a): more risk averse miners mine less.
- Mining competition ($p = \frac{1}{\sum_{i=1}^{M} N_i}$): Competition increases as the miner population increases, which decreases success rate and makes mining less appealing.
- Market value of Bitcoin (P_B): higher price of Bitcoin induces more miners to join mining and existing miners to mine more.

The maximized net expected utility earned by Miner i is

$$U(N_i^*) = (\frac{N_i^* P_BB}{\sum_{i=1}^{M} N_i^*})^a - (\frac{F}{D} + c)N_i^* \tag{9}$$

Miner i will remain in mining business if $U(N_i^*) \geq 0$. In Figure 1, miners are ranked according to their utility-maximizing number of mining attempts from the lowest to the highest. The concave curve is expected utility and the linear curve is the cost function. The vertical distance between the two curves is the expected net utility at each individual mining level. The intersection of the two curves corresponds to the marginal miner M who breaks even. The equilibrium total mining attempts of the business is $\sum_{i=1}^{M} N_i^*$. An increase in Bitcoin price will shift up the concave utility curve and leads to an increase in the overall scale of mining.

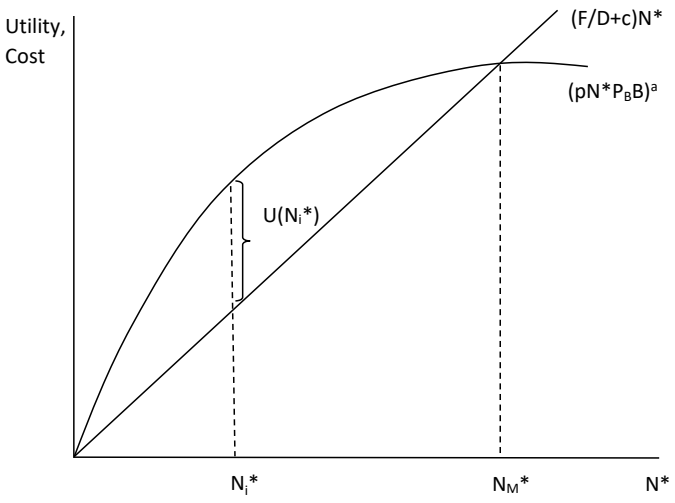

Fig. 1: Expected-net-utility-maximizing number of mining attempts across miner population.

The miner receiving the highest expected payoff is not necessarily the miner with the most mining attempts. As computational power increases, the expected reward increases. In the mean time, the mining cost increases and reward uncertainty increases. Nevertheless, if mining business has internal economies of scale so that the average cost curve is decreasing, then miners would always want to go big. Empirical study found that some miners can benefit disproportionately from mining, and the unbalanced reward allocation of this sort creates a bias in favor of larger miners [14].

Self-interested Miner i chooses the mining attempts of N_i^* to maximize individual net expected utility of Bitcoin mining. For the entire mining industry, the miner population M is the number of miners who at least break even, i.e., with $U(N_i^*) \geq 0$. Such miner population would be socially optimal if Bitcoin were used only as virtual medium of exchange: in a speculation-free environment (i.e., $S = 0$), $M_s = M$.

The existence of speculative demand for Bitcoin makes the mining industry equilibrium deviate from social optimum. The larger is the fraction of Bitcoin used for speculative purpose, the more net-expected-utility-maximizing level of mining will exceed social optimum, resulting in over-mining, over-competition and over-energy-consumption.

The modeling analysis combining the Bitcoin market and the mining business highlights the key role of Bitcoin price in determining miner population and the scale of mining. Rising Bitcoin price intensifies mining competition. Currently Bitcoin mining is highly competitive. Since it is not uncommon for

miners to receive huge energy bills, the only possibility for miners to have the financial incentive to participate in mining to maintain the Bitcoin system is the high market value of Bitcoin.

With predetermined supply of Bitcoin, the price of Bitcoin is largely driven by demand. The transaction demand for Bitcoin derives from its virtual currency nature, but the speculative demand for Bitcoin has limited (if any) welfare gain to the society rather than wealth transfer among Bitcoin investors.

In our modeling analysis, mining costs include only costs private to miners but not external to the society such as pollution. Bitcoin mining is an activity with negative externalities so that the actual scale of mining is more than socially desirable. The speculative demand for Bitcoin induces mining activities to go even beyond the social optimum. Restricting the speculative component of Bitcoin transactions will improve efficiency.

There are multidimensional approaches to restrict speculative demand. First, it may be feasible to modify the Bitcoin protocol so that there is unlimited supply of bitcoins. Second, it is socially beneficial to diversify portfolio by encouraging the use of other virtual currencies such as Litecoin, Ripple, etc. Diversification in cryptocurrency markets is helpful in reducing speculative demand and unreasonably high price of any individual currency. Third, it may also be helpful to reduce media coverage of Bitcoin. Empirical data suggests that frequent media reports elevate Bitcoin price [9]. Overoptimistic media coverage of Bitcoin may prompt waves of novice investors to pump up Bitcoin price.

V. Conclusion

Competition mechanism built in decentralized cryptocurrency such as Bitcoin faces an inherent tradeoff between security and efficiency. The fast growing mining participation and over-competition create huge energy waste, uncertainty and reduced rewards for mining community, and are less desirable from social perspective. We build an economic model in order to understand such mining behavior and formulate optimization problem through utility maximization. The equilibrium solution provides key insights on the socially optimal mining participation. We believe that the speculative demand for Bitcoin increases the inefficiency in Bitcoin mining and proposed to reduce the speculative demand of cryptocurrency in general for a more sustainable cryptocurrency ecosystem.

The total number of Bitcoin will converge at 21 million, and about 80% of the total Bitcoin has been mined by 2017. Over time, Bitcoin mining may transit to a different business model, e.g., rely more on transaction fees. Our future work is to study the simultaneous determination of Bitcoin price and transaction fees, and how the price factors affect the social optimum of mining business.

References

[1] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014.

[2] P. Jacquet and B. Mans, "Green mining: toward a less energetic impact of cryptocurrencies," *arxiv.org*, 2018.

[3] A. Shoker, "Sustainable blockchain through proof of exercise," in *Proceedings of the 16th IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, October 30-November 1 2017, pp. 393–401.

[4] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, "Proofs of useful work," *IACR Cryptology ePrint Archive: 203*, 2017.

[5] B. A. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Web and Internet Economics: 13th International Conference, WINE 2017 Proceedinds*, Bangalore, India, December 17-20 2017, pp. 205–218.

[6] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, Istanbul, Turkey, May 04-08 2015, pp. 919–927.

[7] P. Ciaian, M. Rajcaniova, and d'Artis Kancs, "The economics of bitcoin price formation," *Applied Economics*, vol. 48, no. 19, pp. 1799–1815, 2016.

[8] L. Kristoufek, "What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis," *PLOS ONE*, vol. 10, no. 4, April 2015.

[9] M. Polasik, A. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, "Price fluctuations and the use of bitcoin: An empirical inquiry," *International Journal of Electronic Commerce*, vol. 20, no. 1, pp. 9–49, November 2017.

[10] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.

[11] A. Kajtazi and A. Moro, "Bitcoin and portfolio diversification: Evidence from portfolios of U.S., European and Chinese assets," *SSRN Electronic Journal*, 2018.

[12] F. Glaser, K. Zimmermann, M. Haferkorn, M. C. Weber, and M. Siering, "Bitcoin - asset or currency? revealing users' hidden intentions," in *Proceedings of the 22nd European Conference on Information Systems (Tel Aviv)*, Israel, June 9-11 2014, pp. 1–14.

[13] J. Bouoiyour and R. Selmi, "What does bitcoin look like?" *Annals of Economics and Finance*, vol. 16, no. 2, pp. 449–492, 2015.

[14] Y. Sompolinsky and A. Zohar, "Bitcoin's underlying incentives," *Queue*, vol. 15, no. 5, pp. 50:29–50:52, October 2017.