LEDGER
ledgerjournal.org
ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

RESEARCH ARTICLE

Bitcoin Mining as a Contest

Nicola Dimitri*†

Abstract. This paper presents a simple game theoretic framework, assuming complete information, to model Bitcoin mining activity. It does so by formalizing the activity as an all-pay contest: a competition where participants contend with each other to win a prize by investing in computational power, and victory is probabilistic. With at least two active miners, the unique pure strategy Nash equilibrium of the game suggests the following interesting insights on the motivation for being a miner: while the optimal amount of energy consumption depends also on the reward for solving the puzzle, as long as the reward is positive the decision to be an active miner depends only on the mining costs. Moreover, the intrinsic structure of the mining activity seems to prevent the formation of a monopoly, because in an equilibrium with two miners, both of them will have positive expected profits for any level of the opponent's costs. A monopoly could only form if the rate of return on investment were higher outside bitcoin.

1. Introduction

Since its introduction in 2008,[1] Bitcoin has received significant attention as a peer-to-peer cryptocurrency based on blockchain technology.[2, 3, 4] Adoption of Bitcoin may exhibit advantages as well as critical aspects.[5, 6, 7] From an economic perspective, its use may facilitate exchange and possibly save on transaction costs. Because of its exchangeability with fiat currencies such as the dollar, advantages could also come from speculative activity based on oscillations of the exchange rate.[8]

However, one of its most distinguishing features is that the registration of transactions is done through the so-called *mining* activity undertaken by certain entities. Such activity consists of solving a puzzle requiring high computational power, since registration of a block of transactions can only take place once the puzzle has been solved. Providing the right economic incentives to solve the puzzle is very important for the transactions to be registered on the underlying ledger. This is why *miners* are compensated for this activity with two types of rewards: first, for any solved puzzle the miner will receive a fixed sum of bitcoins by the protocol (the *block reward*) and, moreover, individuals behind a transaction may offer a fee to the miners for its registration.[9, 10] The larger this fee, the higher the incentive for the miners to enclose the associated transaction in the next registered block. The fixed sum received from the protocol for each block of registrations will tend to decline over the years until its disappearance, after which only fees paid for transaction registration will reward the miners.

In this paper we focus on the mining activity as a source of economic profitability,[3] where the main strategic decision taken by miners is how much to invest in computational power to

† N. Dimitri (dimitri@unisi.it) is Professor of Economics at The University of Siena, Italy, and Corvers Chair in Innovation Procurement at the Maastricht School of Management, NL
*1N9ukmAq6EhhVigrAHiMMzSHdEwDAcLskP

solve the puzzle. Within a very simple static game theoretic framework, our model provides some interesting insights. Due to the assumption that the waiting time for obtaining the solution to a puzzle is an exponentially distributed random variable, the mining activity can be characterized as an *all-pay contest*—a conceptual framework widely adopted in social sciences. [11, 12] All-pay contests are competitions where winners are awarded a prize, specified in advance by the organizer. They require investments to participate, and this is what makes them all-pay, and victory by a contender typically occurs probabilistically. Therefore, those who obtain no prize lose their investments, unless these could be re-used in other contexts. Winning probabilities are often called *contest functions*.

Indeed, mining activity can be seen as a contest where participants are trying to come first in the competition for the solution of the puzzle, receiving as the prize the block reward and any fees from participants whose transactions were registered in the solved block.

At the Nash equilibrium of the mining game with perfect information, while the level of computational power chosen by an active miner depends also on how many bitcoins could be obtained solving the puzzle, the decision to become an active miner depends only on his own marginal costs as compared to his opponents' cost structure. That is, the decision to be an active miner depends only upon how efficient his competitors are and not on how many bitcoins will be obtained as rewards.

Moreover, still at a Nash equilibrium, a miner's expected profit would increase if, given the marginal costs of his opponents, his own marginal cost would decrease. Therefore, if expenditures to further reduce marginal costs of computational power would be lower than the increase in expected profits, then miners may find it optimal to make such investments to decrease their costs. Lowering one's marginal costs could also induce negative expected profits upon some of the miners, who for this reason would cease being active. However, the intrinsic structure of the game prevents the emergence of a monopoly in the mining activity, since at an equilibrium with only two miners they will always have positive expected profits for any level of their marginal costs. For this reason, a monopoly could form only if return on investment outside bitcoin was higher than within bitcoin.

The paper is structured as follows: in Section 2 we introduce the basics of the model and the main Nash equilibrium of the game, while in Section 3 we briefly discuss the structure of the mining market. Section 4 concludes the paper.

2. The Model

Suppose $i = 1, 2, \dots, n$ is the generic *active* miner who has to choose his bitcoin investment in computational power h_i; a miner is said to be active if $h_i > 0$. We start considering $n \geq 2$, discussing the case of $n = 1$ in Section 2.1

The mining reward for solving the puzzle is given by $R \geq 0$ bitcoins, provided by both the Bitcoin protocol and the transaction fees. Due to the transaction fees, the reward may typically change across different puzzles and at different times; however, since our model is static this will not affect the main conclusions.

Let X_i be the waiting time of miner i for solving the puzzle, which we assume to be an exponentially distributed random variable with parameter $\frac{h_i}{d}$, where d is a numerical indicator of the difficulty for solving the puzzle. Parameter d is adjusted by the Bitcoin protocol to keep the expected time between the solutions for two consecutive puzzles fixed to a predetermined time interval. Hence, assuming X_i to be independent random variables then $X = \min(X_i)$ is

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

also exponentially distributed with parameter $\frac{h_{(n)}}{d}$, where $h_{(n)} = \sum_{i=1}^{n} h_i$ and with expected value $\langle X \rangle = \frac{d}{h_{(n)}}$. For the Bitcoin protocol, $\langle X \rangle = T$ with $T = 10$ minutes.

With no major loss of generality we assume constant returns of scale in the investment on computational power: that is, miner i's cost function is given by $C_i(h_i) = c_i h_i$, where c_i is the marginal, and average, cost for miner i to produce a unit of computational power. The assumption of constant returns to scale implies that fixed-cost investments on hardware are considered as given and that costs of computational power in this paper simply stand for operational variable costs such as energy consumption. In a static model like ours, this is without major loss of generality since a condition for an activity to be economically sustainable is coverage of the associated variable costs. Although operational costs are typically expressed in fiat currencies (dollars, euro, *etc*.), in the paper we express $C_i(h_i) = c_i h_i$ in bitcoins. This implies that the marginal cost c_i incorporates the current exchange rate between bitcoins and the fiat currency.

It follows that miner i's profit, $\Pi_i(h_i)$, is a random variable given by

$$\Pi_i(h_i) = \begin{cases} R - c_i h_i & \text{with probability } \frac{h_i}{h_{(n)}} & \text{if } h_i > 0 \\ -c_i h_i & \text{with probability } \frac{h_{-i}}{h_{(n)}} & \text{if } h_i > 0 \\ 0 & \text{with probability } 1 & \text{if } h_i = 0 \end{cases}$$

where the ratio $\frac{h_i}{h_{(n)}}$ is the contest function, representing the probability that miner i will be the first to solve the puzzle, such that $\frac{h_i}{h_{(n)}} = 0$ if $h_{(n)} = 0$. Moreover, $h_{-i} = h_{(n)} - h_i$. Therefore, miner i's expected profit is

$$\langle \Pi_i(h_i) \rangle = \frac{R h_i}{h_{(n)}} - c_i h_i, \quad i = 1, .., n. \tag{1}$$

We assume complete information on c_i, *i.e*., miners know each other's marginal costs. This is a simplifying assumption, however perhaps not too far from reality since the needed power to mine is currently so significant that only a few nodes on the Bitcoin network can afford being active. Given their limited numbers, it is not unrealistic to think that miners could make some reasonable guesses as to the opponents' hashing power as well as marginal costs. Maximization of Eq. (1) with respect to h_i leads to the following first order condition:

$$\frac{R h_{-i}}{{h_{(n)}}^2} = c_i \, . \tag{2}$$

Because second order conditions are met (*cf.* the appendix), assume, still without loss of generality, that $c_1 \leq c_2 \leq \ldots \leq c_n$. If $c_{(n)} = \sum_{i=1}^{n} c_i$ it follows that

$$h_{(n)} = \frac{R(n-1)}{c_{(n)}}, \tag{3}$$

and for each active miner the optimal level of computational power is

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

$$h_i = \frac{h_{(n)}\left[c_{(n)} - (n-1)c_i\right]}{c_{(n)}} = \frac{R(n-1)\left[c_{(n)} - (n-1)c_i\right]}{{c_{(n)}}^2}, \tag{4}$$

therefore $h_1 \geq h_2 \geq \ldots \geq h_n$.

The above can be summarized by the following proposition:

Proposition. *The unique pure strategy Nash equilibrium of the Bitcoin mining game, with complete information on the contenders' marginal costs, is the profile* $(h_1, .., h_n)$*, where* h_i *is given by Eq. (4).*

Eq. (4) suggests some interesting observations. First, for a miner to be active, that is for $h_i > 0$, it is necessary that $c_{(n)} - (n-1)c_i > 0$, which means that the mining activity depends on his own cost structure only, as compared to the other miners, and not on the reward for the mining activity R (which exclusively affects the optimal level of deployed computational power. Of course, the condition $R > 0$ is necessary for any positive investment by the miners.)

Replacing Eq. (2) and Eq. (3) in Eq. (1) implies that miner i's expected profit is given by

$$\langle \Pi_i(h_i) \rangle = R\left[\frac{c_{(n)} - (n-1)c_i}{c_{(n)}}\right]^2 = R\left(\frac{h_i}{h_{(n)}}\right)^2,$$

hence, expected profits are a share of the same share of the reward R. Consistent with intuition, the expected profit is decreasing in c_i and increasing in R. However, the expected rate of return (productivity) defined as

$$\langle r_i(h_i) \rangle = \frac{\langle \Pi_i(h_i) \rangle}{c_i h_i} = \left[\frac{c_{(n)} - (n-1)c_i}{(n-1)c_i}\right] > 0$$

is independent of R though decreasing in c_i as well. Moreover, it follows that

$$\langle r_i(h_i) \rangle = \left[\frac{c_{(n)} - (n-1)c_i}{(n-1)c_i}\right] > \left[\frac{c_{(n)} - (n-1)c_i}{c_{(n)}}\right] = \frac{h_i}{h_{(n)}}.$$

That is, while each active miner i obtains a share $\frac{h_i}{h_{(n)}}$ of the reward R, at the Nash equilibrium each miner's productivity rate is higher than this ratio.

We conclude this section considering the specific case of symmetric marginal costs, that is $c_i = c$ for all $i = 1, .., n$. Then it is easy to see that $h_{(n)} = \frac{R(n-1)}{cn}$, $h_i = h = \frac{R(n-1)}{cn^2}$, $\langle \Pi_i(h) \rangle = R\left(\frac{1}{n}\right)^2$ and $\langle r_i(h) \rangle = \frac{1}{(n-1)} > \frac{1}{n} = \frac{h}{h_{(n)}}$, with both profit and productivity being independent of the marginal cost. Moreover, both are decreasing in n, obtaining as highest values $\langle \Pi_i(h) \rangle = \frac{R}{4}$ and $\langle r_i(h) \rangle = 1$ at $n = 2$, which indicates that with a small number of miners the mining activity could be economically more attractive than with a higher number. This point will be further developed in Section 4.

2.1. One Active Miner—Suppose now that $n = 1$, that is, the mining activity is conducted by miner 1 only. In this case his profit $\Pi_1(h_1)$ would be defined as

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

$$\Pi_1(h_1) = \begin{cases} R - c_1 h_1 & \text{with probability } 1 \text{ if } h_1 > 0 \\ 0 & \text{with probability } 1 \text{ if } h_1 = 0 \end{cases}$$

Therefore, for $h_1 > 0$ his expected profit is $\langle \Pi_1(h_1) \rangle = R - c_1 h_1$, which for small enough $h_1 = \varepsilon > 0$ becomes $\langle \Pi_1(h_1 = \varepsilon) \rangle = R - c_1 \varepsilon > 0 = \langle \Pi_1(h_1 = 0) \rangle$. As a result, if for some reason there is only one active miner, it is optimal to invest a small amount of resources, what is just enough to mine successfully. As for the rate of return, in this case it would be

$$\langle r_1(h_1) \rangle = \frac{\langle \Pi_1(h_1) \rangle}{c_1 h_1} = \frac{R}{c_1 \varepsilon} - 1,$$

which is very high for small enough ε.

However, how likely would a monopoly be? The next section discusses the issue.

3. "Market Structure" of the Mining Activity

The above considerations suggest that those miners who could profitably reduce their marginal costs would do it. To see this consider the following numerical example. Suppose there are three active miners $i = 1, 2, 3$ with $c_1 = 3, c_2 = 4$ and $c_3 = 5$, so that $c_{(3)} = 12$, $h_{(3)} = \frac{R(n-1)}{c_{(3)}} = \frac{2R}{12} = \frac{R}{6}$ and $\langle \Pi_1(h_1) \rangle = R\left(\frac{c_{(3)} - 2c_1}{c_{(3)}}\right)^2 = \frac{R}{4}$ which implies that $\langle r_1 \rangle = \frac{\langle \Pi_1(h_1) \rangle}{c_1 h_1} = 1$. Therefore, for each bitcoin invested the mining activity would generate to miner 1 an additional bitcoin, with a return (interest) rate on investment of 100%.

Suppose now miner 1 would be able to reduce his own marginal cost from $c_1 = 3$ to $c_1 = \frac{1}{2}$. Then it is easy to see that miner 3 would no longer be active as the condition $c_{(3)} - (n-1)c_3 > 0$ ceases to hold, since now it would be $\frac{19}{2} - 10 < 0$. As a consequence, only miners 1 and 2 could remain active. Therefore, now $i = 1, 2$ with $c_1 = \frac{1}{2}, c_2 = 4$ so that $c_{(2)} = \frac{9}{2}$, $h_{(2)} = \frac{2R}{9} > \frac{R}{6} = h_{(3)}$ and $\langle \Pi_1(h_1) \rangle = R\left(\frac{8}{9}\right)^2 = \frac{64R}{81} > \frac{R}{4}$ which implies $\langle r_1 \rangle = \frac{\langle \Pi_1(h_1) \rangle}{c_1 h_1} = 8$. Hence, if reduction of the marginal cost to $\frac{1}{2}$ would need less than $\frac{64R}{91} - \frac{R}{4}$ bitcoins, then it would be profitable for miner 1 to do so and exclude miner 3 from being active. It is interesting to notice that, even though now the number of active miners decreased by one unit, the total investment in computational power increased because losing one active miner is more than compensated for by the decrease in the total marginal cost.

If the example suggests that there could be an incentive by some active miners to cut down their marginal costs to exclude competitors, and in so doing increase their own expected profit and return rate, the protocol guarantees that at least two miners would always have positive expected profit.

Indeed, with $i = 1, 2$ expression $c_{(n)} - (n-1)c_i > 0$ becomes $c_{(2)} - c_i > 0$, implying that with two active miners, none of them could exclude the other by cutting down his own marginal costs. This is summarised by the following corollary:

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

Corollary. *At a unique pure strategy Nash equilibrium of the Bitcoin mining game with two active miners, both of them will have positive expected profit regardless of the opponent's marginal cost.*

That is, the intrinsic structure of the Bitcoin mining game seems to prevent the emergence of a monopolistic mining activity. However if the rate of return, for one of the players, were to become lower than the market interest rate, then a miner may find it convenient to stop mining and invest resources in alternative activities.

Finally, it is worth pointing out that when only two miners remain active, whenever their marginal costs are different one of them will certainly have more than 50% of the computational power.

4. Conclusion

In this paper, we proposed to model the Bitcoin mining activity as a simple static game with complete information. Despite its simplicity, the model seems to provide some interesting insights on the underlying motivation for being an active miner. The mining game is modelled as an all-pay contest, in the sense that miners compete for the reward by investing resources, victory is probabilistic and if they lose the competition energy consumption will be wasted. The model suggests that the main motivation for active mining is given by the miners' cost structure, while the reward for solving the puzzle affects only the optimal level of computational power but not the decision to be active. Finally, the mining activity seems to be intrinsically monopoly-proof, in the sense that if only two miners were to be active, their profits would always be positive regardless of the marginal cost of the opponent. For this reason, none of the two could exclude the other by cutting down his own costs, unless activities other than Bitcoin mining would have a higher rate of return.

In its simplicity the model is omitting a number of elements, which could be investigated in future research. Among them the current debate and interest on the block size, [9, 10] which may affect the main conclusions of the paper at least in so far as the number of potentially active miners is concerned. An explicit consideration of time, as well as of the uncertainty on transaction fees, is also missing. Moreover, miners could pursue goals other than expected profit maximization. For this reason the paper's conclusions are limited to some early insights on the determinants of mining profitability.

Appendix

In this appendix, for completeness, we spell out the very simple derivations for Eqs. (2), (3) and (4). Starting from the expected profit $\langle \Pi_i(h_i) \rangle = \frac{Rh_i}{h_{(n)}} - c_i h_i$ consider the first order condition

$$\frac{d}{dh_i} \langle \Pi_i(h_i) \rangle = \frac{R(h_{(n)} - h_i)}{h_{(n)}^2} - c_i = \frac{Rh_{-i}}{h_{(n)}^2} - c_i = 0,$$

where $h_{-i} = h_{(n)} - h_i$. The second derivative of the expected profit is given by

$$\frac{d^2}{(dh_i)^2} \langle \Pi_i(h_i) \rangle = -\frac{2Rh_{-i}}{h_{(n)}^3} < 0.$$

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96

Solution of the above first order condition leads to Eq. (2), which, because the second order condition is satisfied, identifies a maximum of the expected profit. Since $\frac{R(h_{(n)}-h_i)}{h_{(n)}^2} = c_i$ then $\sum_{i=1}^{n} \frac{R(h_{(n)}-h_i)}{h_{(n)}^2} = \sum_{i=1}^{n} c_i = c_{(n)}$. But $\sum_{i=1}^{n} \frac{R(h_{(n)}-h_i)}{h_{(n)}^2} = \frac{nR}{h_{(n)}} - \frac{R}{h_{(n)}} = \frac{(n-1)R}{h_{(n)}}$ and so Eq. (3), $h_{(n)} = \frac{(n-1)R}{c_{(n)}}$, follows. Finally, from $\frac{R(h_{(n)}-h_i)}{h_{(n)}^2} = c_i$ it is $R(h_{(n)} - h_i) = c_i h_{(n)}^2$ which solved in h_i gives $h_i = h_{(n)} - \frac{c_i h_{(n)}^2}{R} = h_{(n)}\left(1 - \frac{c_i h_{(n)}}{R}\right)$. Replacing $h_{(n)} = \frac{(n-1)R}{c_{(n)}}$ into this last expression provides $h_i = h_{(n)}\left[1 - \frac{(n-1)c_i}{c_{(n)}}\right] = h_{(n)}\left[\frac{c_{(n)}-(n-1)c_i}{c_{(n)}}\right]$, which is Eq. (4).

Notes and References

[1] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." No Publisher (2008) https://bitcoin.com/bitcoin.pdf

[2] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., Felten, W. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." *IEEE Symposium on Security and Privacy* (2015) https://doi.org/10.1109/SP.2015.14

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press (2016)

[4] Antonopoulos, A. *Mastering Bitcoin*, 2nd ed., Sebastopol, CA: O'Reilly (2017)

[5] Evans, D. "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms." *Coase-Sandor Institute for Law and Economics Working Paper* **685** (2014) https://ssrn.com/abstract=2424516

[6] Böhm, R., Christin, N., Edelman, B., Moore, T. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* **29** 213-238 (2015) https://doi.org/10.1257/jep.29.2.213

[7] Athey, S., Parashkevov I., Sarukkai, V., Xia, J. "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence." *Stanford Business School Working Papers* **3469** (2016) https://ssrn.com/abstract=2826674

[8] Garratt, R., Wallace, N. "Bitcoin 1, Bitcoin 2, ... : An experiment in privately issued outside monies." Working Paper, Department of Economics University of Santa Barbara (2016) https://escholarship.org/uc/item/91c7x1js

[9] Rizun, P. "A Transaction Fee Market Exists Without a Block Size Limit." Block Size Limit Debate Working Paper (2015) https://www.bitcoinunlimited.info/resources/feemarket.pdf

[10] Houy, N. "The Bitcoin mining game." *Ledger* **1** 53-68 (2016) https://doi.org/10.5195/ledger.2016.13

[11] Konrad, K. *Strategy and Dynamics in Contests*. Oxford: Oxford University Press (2009)

[12] Vojonovic, M. *Contest Theory*. Cambridge: Cambridge University Press (2015)

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2017.96