Optimal Design of Bitcoin Mining

ZIYI YE

ABSTRACT

Bitcoin is a peer-to-peer electronic currency without central bank controlling. Nowadays, increasing amount of people are engaged in the mining of Bitcoin for great profits. However, in the Bitcoin system, the more participants in the system, the greater computation power of the whole network and the less efficiency in the output of the coin, since large computational power of the whole Bitcoin system will lead to increased difficulty for a single miner to mine a new data block. At the same time, when more than 51% computing power is controlled by a single node, it could destroy the Bitcoin system. In order to reduce ineffective mining behaviors, one would wish to employ the optimal selection mechanism of different miners. This paper will mainly develop the model in which small miners (those who have relative smaller computational power in a block mining) join the major ones based on revenue, computational power cost, and other elements of the process comparing to the current model (when they work separately).

KEYWORDS

Bitcoin, mining strategy, miner, pool.

INTRODUCTION

A detailed overview of Bitcoin and its development

Bitcoin is a virtual currency that relies on electronic signature technology and peer-to-peer network technology (P2P) to prevent double expenses, it is currently the most successful block chain application scenario.

In general, the term "Bitcoin" refers to the whole bitcoin system, while the term "bitcoin," or "BTC," indicates the unit of account of the bitcoin system. The definition of bitcoin was first mentioned by an obscure individual named Satoshi Nakamoto in his paper titled Bitcoin: A Peer-to-peer Electronic Cash System in November 2008. This paper introduced a new kind of transaction "without relying on trust."[2] Bitcoin does not have any physical presence like gold or coins. It is also the first decentralized currency, which means that no central bank or government controls its issuance and circulation. Ever since the appearance of the first Bitcoin, the price of the Bitcoin has been increased dramatically. As of November 2017, it has reached $7,000 for the first time.

Ziyi Ye, University of California, Los Angeles, Los Angeles CA 90024, USA, clover1869@gmail.com.
The introduction of Bitcoin Mining and Miners

Each Bitcoin transaction data will be packed into a data block, which is the basis for the fundamental structure of Bitcoin, the block chain. Each data block contains the following information: Data version named version, hash value of previous data block named pre-hash, hash value to be written to transaction named merkle-root, record update time named ntime, and the current difficulty named nbits.

Mining refers to the process of generating a data block by calculating a "minimum hash value" math problem and then the transaction is finally confirmed. The data contained in the data block will be used to calculate the x value:

\[
\text{SHA256} (\text{SHA256} (\text{version} + \text{pre-hash} + \text{merkle-root} + \text{ntime} + \text{nbits} + x)) < \text{Difficult} \quad (1)
\]

The Difficult values are adjusted according to the output of the current bitcoins.

According to the bitcoin protocol, the difficulty of mining a block is changed every 2016 blocks. The expected time of mining those 2016 blocks is exactly 2 weeks, suggesting the time to mine one block is exactly 10 minutes. If the current mining time for 2016 blocks is less than the expected total time, then the difficulty of mining the following 2016 blocks will increase accordingly. The average time to find a block under certain difficulty is represented by:

\[
\text{Time} = \frac{\text{Difficulty}^{2016}}{\text{HashRate}} \quad (2)
\]

From equation 2, with increasing difficulty for mining, the time for a single miner (people who do the mining process) who have lower devices and lower computational power will increase dramatically. Therefore, as one solution, a numerous amount of miners work together to mine the block and split the reward based on contributions during mining. Such a platform for miners mining together are called pools.
For the purpose of the modeling, the large miners are defined as miners who have relatively large computational power within one pool, and small miners are defined as miners who have relatively small computational power compared with other miners in the pool. The computational power of miners is measured by how many hashes can run per second.

In general, this paper will address the following question: within one pool, is it better for small miners and large miners to work together to mine one block, or is it more profitable for them to work separately?

SURVEY OF RELEVANT LITERATURE

In the sustainability of bitcoin and bitcoins, Harald Vranken investigates the exact cost of bitcoin, including the cost for hardware and electricity. The author concludes that "the order of magnitude of energy consumption is 100MW"[5], using the latest hardware ASICs to mine the bitcoins. However, the exact cost of mining bitcoins may vary dramatically due to the differences in electricity cost in different areas and different hardware costs. As a result, this article would simply assume that there will be certain amount of cost in average time, denoted as C dollars per second.

As to the reward for mining bitcoins, we simplify the model in Incentive Compatibility of Bitcoin Mining Pool Reward Functions [4]. Although the current reward model, which divides the reward of mining one block to several miners according to their contribution in calculating the solution to that block, (in other words, according to the proportion of their computational power compared to the total computational power of all miners), has certain defects in motivating miners to report their blocks immediately as showed in [4], this paper still applies the proportional reward method in calculating the total revenue. Since the proportional reward method is the most popular and widely-used method for almost all the mining pools, applying such a method to the model would have more implications and more related to the current mining strategy.

STRATEGY DESIGN

Background introduction

As mentioned in previous sections 1.2, this paper wishes to explore the possible outcome of small miners and large miners cooperating together to mine the same block in terms of revenue, which means the reward from successfully mining the block minus the total cost of that process.

To build the model, one first assumes the following:

1) Assume that inside one pool, there are only two miners, the large miner who has relatively large proportions of computational power, and the small miner who has small proportions of computational power compared to the large miner.

2) The costs of mining, which are measured by dollars per second, are constant for the same miner.

3) Although the price for bitcoins (which also can be seen as the reward) is constantly changing as previously mentioned in 1.1, for simplicity sake, this paper supposes that the reward for successfully mining one block does not change during the
mining process since prices are not the main variable one cares about. Moreover, it
does not have any impacts on the model we are going to build.

(4) The standard for the possibility of small miner and large miner cooperation is
revenue, which is measured using the reward minus the cost (the unit will also be
dollar per second)

Model Construction and Analysis

We assume the initial difficulty of mining is D0 and the reward for successfully
mining a block is V dollars. Although the price of bitcoin, which also can be seen as
the reward for mining a block successfully, is continuously changing, here for the
purpose of modeling, we assume that the price does not change during the time of
mining.

Additionally, though the cost of mining depends on numerous elements, (such as
electricity and hardware costs we discussed in section 3.1) we simply assume that the
cost for the small miner is C1 dollars/sec while the cost for the large miner is C2
dollars/sec. Furthermore, the hash rate, which largely depends on the cost, will be H1
hashes/sec and H2 hashes/sec, below is the table for the assumed variables.

In this paper, we would compare the revenue in different situation in dollars/sec.

When mining separately. Applying equation 2, we can calculate the average time
for small miner to mine a block, which is

\[ T_1 = \frac{D_0 \cdot 2^{32}}{H_1} \]  

(3)

So, the average revenue for small miner is

\[ R_1 = \frac{H_1 \cdot V}{2^{32}} - C_1 \]

(4)

Similarly, the average time and revenue for large miner is:

\[ T_2 = \frac{D_0 \cdot 2^{32}}{H_2} \]

(5)

\[ R_2 = \frac{H_2 \cdot V}{2^{32}} - C_2 \]

(6)

When mining together. When the small miner and large miner cooperate to mine
the same block, the time they use is:

\[ T_{\text{cooperate}} = \frac{D_0 \cdot 2^{32}}{H_1 + H_2} \]

(7)

And the corresponding total revenue in dollars per second is:

\[ R_{\text{cooperate}} = \frac{(H_1 + H_2) \cdot V}{2^{32}} - (C_1 + C_2) \]

(8)

Thus, the average revenues for small miner is:
TABLE 1: Table of Variables Used.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Small Miner</th>
<th>Large Miner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost (dollar/sec)</td>
<td>(C_1)</td>
<td>(C_2)</td>
</tr>
<tr>
<td>Hash Rate (hash/sec)</td>
<td>(H_1 = f(C_1))</td>
<td>(H_2 = f(C_2))</td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
<td>(D_0)</td>
</tr>
<tr>
<td>Reward (dollar/block)</td>
<td>(V)</td>
<td></td>
</tr>
</tbody>
</table>

\[
R_3 = \frac{H_2}{H_2 + D_2} \cdot R_{cooperate} \quad (9)
\]

Which can be simplified to

\[
R_3 = \frac{H_2 V}{D_0 + 2V} - \frac{1}{1 + \frac{H_2}{D_0}} \cdot (C_1 + C_2) \quad (10)
\]

As a result, since we assumed that \(H_1 \ll H_2\) if \(H_1 \ll H_2\), we have

\[\frac{1}{1 + \frac{H_2}{D_0}} (C_1 + C_2) \to 0\].

Thus, \(R_3 = \frac{H_2 V}{D_0 + 2V} \cdot \frac{D_0}{D_0} \cdot (C_1 + C_2) \to R_1\) which means that in any cases, small miners are willing to cooperate with large miners.

Likewise, the revenue for large miner under the situation cooperation is:

\[
R_4 = \frac{H_2 V}{D_0 + 2V} - \frac{1}{1 + \frac{H_2}{D_0}} \cdot (C_1 + C_2) \quad (11)
\]

Since \(H_1 \ll H_2\), we have \(\frac{1}{1 + \frac{H_2}{D_0}} (C_1 + C_2) \to (C_1 + C_2)\).

Thus, \(R_4 = \frac{H_2 V}{D_0 + 2V} \cdot (C_1 + C_2) \ll R_3\) which means that in any cases, large miners are not willing to cooperate with small miners.

Therefore, we can write the following proposition:

Proposition 1: When keeping the difficulty for mining a block and the reward for mining a block successfully constant, for \(H_1 \ll H_2\), the small miner will always intend to cooperate with large miner while large miner are not willing to do so.

\(C_1\) and \(H_1\) represent the cost (dollars/sec) and the hash rate (hashes/sec) for the small miner, while \(C_2\) and \(H_2\) represent the cost (dollars/sec) and the hash rate (hashes/sec) for the small miner.

As a result, it is impossible for small and large miner to work together without hurting anyone’s interests.

**Considering difficulty change.**

As we discussed in the previous sections, the difficulty of mining blocks will change every 2016 blocks corresponding to the change in time for mining those 2016 blocks comparing to the expected time. If the total time of mining 2016 blocks significantly increases comparing to the expected time, the difficulty for the next 2016 blocks will thus decrease to compensate those lost time. On the other hand, if the total time of mining decreases, the future difficulty will increase correspondingly.

To discuss the change in difficulty, we first assume the average time for mining 2016 blocks with initial difficulty is the average time of \(T_1\) and \(T_2\), when small and large miner mine the block separately, times 2016:
Which can be simplified into:

\[ T_3 = \frac{1}{2} (T_1 + T_2) \cdot 2016 \]  

On the other hand, the total time for mining 2016 blocks when the small and large miner work together is:

\[ T_4 = T_2 \cdot 2016 \]

Therefore, the percentage of change in time is:

\[ p = \frac{T_4 - T_3}{T_3} \]

Which is equal to:

\[ p = -\frac{(H_e - H_s)^3}{(H_e + H_s)^3} \]

Since the numerator and denominator are both squares of certain terms, the percentage change in time is definitely smaller than zero, which means the time used to mine 2016 blocks decrease under the cooperation model. Therefore, the corresponding change in the difficulty of mining the next 2016 blocks will increase by \( p \):

\[ D_1 = D_0 \cdot \left(1 + \frac{(H_e - H_s)^3}{(H_e + H_s)^3}\right) \]

For \((H_e + H_s)^2 \ll 2H_1^2 + 2H_2^2\), that is, \(2H_1H_2 \ll H_1^2 + H_2^2\), which means that when small miners and large miners work together, they will get much lower difficulty than the initial one. On the other hand, for \(2H_1H_2 \gg H_1^2 + H_2^2\), it means that if they cooperate, they will get much higher difficulty than the previous one.

Consequently, the total revenue (dollar/sec) for small and large miner combined for the following 2016 blocks is:

\[ R_{new} = \frac{(H_e + H_s)^3}{2H_1D_0} \cdot \frac{(H_e + H_s)^3}{2H_2D_0} - (C_1 + C_2) \]

And the revenue (dollar/sec) for small miner is:
\[ R_b = \frac{H_b}{H_1 + H_2} \cdot R_{new} \]
\[ = \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_b V}{2H_1 D_0} - \frac{H_b}{H_1 + H_2} (C_1 + C_2) \]
\[ = \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_b V}{2H_1 D_0} - \frac{1}{H_1 + H_2} (C_1 + C_2) \]  
(19)

Since \( H_1 \ll H_2 \), we have \( \frac{1}{H_1 + H_2} (C_1 + C_2) \to 0 \). Thus

\[ R_b = \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_b V}{2H_1 D_0} \]  
(20)

While the revenue (dollar/sec) for large miner is:

\[ R_v = \frac{H_v}{H_1 + H_2} \cdot R_{new} \]
\[ = \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_v V}{2H_1 D_0} - \frac{H_v}{H_1 + H_2} (C_1 + C_2) \]  
(21)

Since \( H_1 \ll H_2 \), we have \( \frac{1}{H_1 + H_2} (C_1 + C_2) \to (C_1 + C_2) \). Thus

\[ R_v = \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_v V}{2H_1 D_0} - (C_1 + C_2) \]  
(22)

When \( R_b \gg R_v \), equivalently,

\[ \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_b V}{2H_1 D_0} \gg \frac{H_v V}{2H_1 D_0} \]
\[ \implies \frac{(H_1 - H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{V}{2H_1 D_0} < \frac{C_1}{H_1} \]  
(23)

only then small miners are willing to cooperate with large miners.

Similarly, when \( R_b \gg R_2 \), equivalently,

\[ \frac{(H_1 + H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{H_b V}{2H_1 D_0} \gg (C_1 + C_2) \gg \frac{H_v V}{2H_1 D_0} \]
\[ \implies \frac{(H_1 - H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{V}{2H_1 D_0} \gg \frac{C_1}{H_1} \]  
(24)

Since \( \frac{(H_1 - H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{V}{2H_1 D_0} > 0 \) and \( -\frac{C_1}{H_1} < 0 \), the equation above does not exist, meaning that in any cases, large miners will not be willing to cooperate with small miners.

Therefore, the best way for small miners is to cooperate with large miners, while the large miner should do the mining by themselves.
Proposition 1 When considering the changes in difficulty, the small miners will cooperate with large miners if and only if

\[
\frac{(H_1 - H_2)^2}{2H_1^2 + 2H_2^2} \cdot \frac{1}{C_2} < H_2
\] (25)

While the large miner will refuse to cooperate under every circumstance, of whose behavior resembles the selfish mining strategy.

\[C_1 \text{ And } H_1\] represent the cost (dollars/sec) and the hash rate (hashes/sec) for the small miner, while \[C_2 \text{ and } H_2\] represent the cost (dollars/sec) and the hash rate (hashes/sec) for the small miner.

Analysis

To answer the question that whether there will be greater profits when the large and small miners cooperate, we first assume that there are only two people within one pool, the person who has relatively large computational power and the person who has relatively small computational power. Then, while keeping the reward for one block (the price of one bitcoin), and the difficulty of mining constant, the model suggests that small miner are likely to help when his computational power is much smaller than that of the large miner while the large miner will refuse to cooperate under every circumstances. When considering the change of difficulty over time, we find out that the small miner will choose to work with large miner if and only if their computational power, costs and revenue satisfy equation 25 while it is still impossible for large miner to cooperate without hurting his profits.

With all those results, we can keep predicting that it is impossible for us to come with a model that small miners and large miners work together to mine the block without hurting each party's interests. On the other hand, it is for the small miner's best interest to work with other large miners under certain constraints.

Error Analysis

The possible improvement for the model will be considering eliminating the assumptions mentioned in 3.1. Further studies can be done considering the model under the pool with large amount of people, or considering the fluctuating of price and difficulty over time. Additionally, our model eliminates all the possibilities of double-spending, or the 51% attack. Future studies can be done regarding the possibility of small miners and large miners work together while under ellipse attack or applying the selfish mining strategy. Last but not the least, for more precise modeling, one should consider apply the simulation to test the conclusion of the model.

CONCLUSION

This paper mainly focuses on the possibility that people who have relative small proportion computational power to cooperate with others who have large computational power to calculate the solution for the same block. After studying the related materials with bitcoin mining, we first build the model under the assumption that there will be no fluctuating in the price of bitcoin or in the difficulty of mining the
bitcoin, and conclude that under no circumstances that large miners will choose to work with people who have much smaller computational power than theirs, while it is best for small miners to work with people who have much larger computational power than their own. We further explore the possibility of large miners and small miners working together considering the fluctuation of difficulty in mining while keeping the award constant. The conclusion is quite similar: that large miners will not cooperate with small miners while the small miners will choose to work with large miners under certain limits.

REFERENCES