Optimal Mining Pool Contract

Moran Koren

February 21, 2014

1 Introduction

This is where you will write your content.

2 Stylized Facts

in the Bitcoin Protocol, transactions are approved by nodes connected in a network. If the majority of the network agrees a transaction is valid , the transaction will be added to the block.

To avoid false approvals, each block of transactions is added to the chain only after a miner provided a *"Proof of work"* to it's colleagues.

The "proof of work" is solving a calculation that requires high processing power. The strongest the miner's hardware is, the highest the probability he will be first to provide the solution to the calculation.

The difficulty of the calculation required is automatically set based on the number of available miner such that block authorization time will be 10 minutes.

The miner how provides the solution receive payment for his work. The payment is comprised from two separate elements.

The first, a fixed amount of new bitcoins are generated and sent to the winner's wallet. The ammount of "new" bitcoins is automatically determined as part of the protocol and is decreasing as the number of bitcoins in circulation increases promising a fixed amount of bitcoins will be reached in the future.

The second source of income to the winning miner is the sum of the transaction fees in the block he authorized. Transaction fees are optional at the current stage of the bitcoin network but they should provide the main incentive for miner as the network matures.

Each miner can decide what transactions to include in the block he is trying to authorize. Different miners can choose different composition of blocks. Unclaimed transactions are left to be processed.

To get more processing power, miner started organizing in pools. each pool have a pool manager (usually the strongest node) that sets the rules and workers. The idea is that by increasing the number of participants , they can increase the probability of solving the calculation faster and receiving the payment.

The common contract in minig pools is of relative revenue sharing - each of the participants receives an income worth to his relative contribution to the pool.

Raulo (2011) showed that this method is open to abuse. The optimal strategy for a worker is to divide it's processing time between the pool and independent mining. Several pools have adjusted their

contracts in an effort to lower the incentive for abuse.

Bitcoin started as a currancy with distributed authorization. As we can see on:
https://blockchain.info/pools

around 80% of the hashrates where mined by one of the 4 largest mining pools, while only 10% where mined by smaller miners so clearly there is an advantage for size in the mining process.

3 Theoretical Model

Let J be the numinal amount of bitcoins that will be transfered to the winning miner and D the difficulty level[1]

Miner i is characterized by his processing power θ_i and the cost of processing he endores c_i.

For simplicity we assume the probability of winning the lottary is proportional to his proccesing power and the relevant difficulty.

Working alone the profit of a miner can be formulated as:

$$\frac{\theta_i}{D} J - c_i \tag{1}$$

We will differentiate between two types of minders , A strong miner noted with the subscript s and a weak miner noted with the subscript w.

Miner of type s can become a pool manager by dividing $(1-\rho)$ of his resources to managing a pool.

Once s decides to manage a pool he offers a contract to w. The contract can be either a transfer of fixed amount of bitcoins we will note W or a cut in the winnings of the pool based on his relative expected contribution to the pool $\frac{\theta_w}{\rho\theta_s+\theta_w}$

Miner of type w can choose whether or not to join a pool and wether he wants to abuse the pool or to be an honest participant.

3.1 Case 1 - Both miner types are small relative to the total processing power of the minning network

In this case we say $\theta_s/D \to 0$

If the type w miner chooses to be independent he can expect a profit of:

[1] We do not differentiate between the source of J at this point. D is essentialy the number of potential hashs a miner has to cover in oreder to find the solution with probability 1.

$$\frac{\theta_w}{D} J - c_w \tag{2}$$

If he joins the pool he can divide his time between indepentent work and submitting shares to the pool.

Following Raulo(2011) we know the optimal strategy for a worker is to devote a share $\gamma > 0$ of his resources to independent mining.

Using this strategy the profit of the worker will be

$$\frac{\gamma\theta_w}{D} J + \frac{\theta_w}{\rho\theta_s + \theta_w} \frac{\rho\theta_s + (1-\gamma)\theta_w}{D} J - c_w \tag{3}$$

For simplicity we will treat the most extreme case of pool abuse Raulo(2011), Where we assume the worker can recive the maximum wage without devoting any affort to the pool meaning $\gamma = 1$.

$$\frac{\theta_w}{D} J + \frac{\theta_w}{\rho\theta_s + \theta_w} \frac{\rho\theta_s}{D} J - c_w \tag{4}$$