

Optimal Mining Pool Contract

Moran Koren

February 20, 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 its colleagues.

The "proof of work" is solving a calculation that requires high processing power. The stronger the miner's hardware is, the higher 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 miners such that block authorization time will be 10 minutes.

The miner now provides the solution and receives 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 amount 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 miners 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, miners started organizing in pools. Each pool has 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 currency 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