*Selfish mining pools*

Analysis of AntPool and F2Pool

Isaac Vawter, Alexey Shablygin

College of Information and Computer Science

University of Massachusetts Amherst

Amherst, MA

ivawter@umass.edu, ashablygin@umass.edu

*Abstract*—In this paper we will analyze data from two biggest mining pools – AntPool and F2Pool. We will look for indication of selfish mining by each of these pools by looking at the theoretical probability and observed probability of mining *n* blocks sequentially given their respective mining power.

# Introduction

The objective of this paper is to observe if the frequency of sequential block discovery by individual bitcoin miners is indicative of honest or selfish mining. In order to do this we collected data about all of the blocks mined between December 1st, 2015 and April 20th, and blocks mined by each pool during that time period.

# Previous Work

This paper makes use of “***Majority Is Not Enough Bitcoin Mining Is Vulnerable***” by Eyal and Sirer, particularly their definition of selfish mining and findings on probability of selfish mining given computing power of a miner.

# Methods

We collected our data using three main sources – blockchain.info, antpool.com and f2pool.com. We scrapped blockchain.info to get all of the mined blocks for our time period. Antpool.com and f2pool.com both provided us with data about the blocks each pool mined respectively. We assume that both pools are honest and reported every mined block on their respective websites. After we collected all of block data, we focused on combining blocks into different sample sizes (2000, 1000, 500, 100 blocks) and performing a Monte Carlo simulation on each sample to determine expected number of sequential block discoveries of varying lengths based mining power of each pool.

# Results

# Conclusion

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in Eq. 1, using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

 

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “Eq. 1” or “Equation 1”, not “(1)”, especially at the beginning of a sentence: “Equation 1 is . . .”

# References

J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd