Bitcoin: A Natural Oligopoly

Nick Arnosti
Columbia University, New York City, NY, USA
nicholas.arnosti@gmail.com

S. Matthew Weinberg[1]
Princeton University, Princeton, NJ, USA
smweinberg@princeton.edu

Abstract

Although Bitcoin was intended to be a decentralized digital currency, in practice, mining power is quite concentrated. This fact is a persistent source of concern for the Bitcoin community.

We provide an explanation using a simple model to capture miners' incentives to invest in equipment. In our model, n miners compete for a prize of fixed size. Each miner chooses an investment q_i, incurring cost $c_i q_i$, and then receives reward $\frac{q_i^\alpha}{\sum_j q_j^\alpha}$, for some $\alpha \geq 1$. When $c_i = c_j$ for all i, j, and $\alpha = 1$, there is a unique equilibrium where all miners invest equally. However, we prove that under seemingly mild deviations from this model, equilibrium outcomes become drastically more centralized. In particular,

- When costs are asymmetric, if miner i chooses to invest, then miner j has market share at least $1 - \frac{c_j}{c_i}$. That is, if miner j has costs that are (e.g.) 20% lower than those of miner i, then miner j must control at least 20% of the *total* mining power.
- In the presence of economies of scale ($\alpha > 1$), every market participant has a market share of at least $1 - \frac{1}{\alpha}$, implying that the market features at most $\frac{\alpha}{\alpha-1}$ miners in total.

We discuss the implications of our results for the future design of cryptocurrencies. In particular, our work further motivates the study of protocols that minimize "orphaned" blocks, proof-of-stake protocols, and incentive compatible protocols.

2012 ACM Subject Classification Theory of computation → Quality of equilibria

Keywords and phrases Bitcoin, Cryptocurrencies, Rent-Seeking Competition

Digital Object Identifier 10.4230/LIPIcs.ITCS.2019.5

Related Version Full version available on arXiv at `https://arxiv.org/abs/1811.08572`.

[1] Supported by NSF CCF-1717899.

© Nicholas Arnosti and S. Matthew Weinberg;
licensed under Creative Commons License CC-BY

10th Innovations in Theoretical Computer Science (ITCS 2019).
Editor: Avrim Blum; Article No. 5; pp. 5:1–5:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany