CCIT Report #923 May 2018

Game of Coins

Alexander Spiegelman
Electrical Engineering
Technion IIT
Haifa, Israel
sashas@campus.technion.ac.il

Idit Keidar
Electrical Engineering
Technion IIT
Haifa, Israel
idish@ee.technion.ac.il

Moshe Tennenholtz
Industrial Engineering
Technion IIT
Haifa, Israel
moshet@ie.technion.ac.il

Abstract

We formalize the current practice of strategic mining in multi-cryptocurrency markets as a game, and prove that any better-response learning in such games converges to equilibrium. We then offer a reward design scheme that moves the system configuration from any initial equilibrium to a desired one for any better-response learning of the miners. Our work introduces the first multi-coin strategic attack for adaptive and learning miners, as well as the study of reward design in a multi-agent system of learning agents.

1 Introduction

Cryptocurrencies are an arms race. Hundreds of digital coins have crept into the worldwide market in the last decade [6], including more than a dozen with over a billion dollar Market Cap, e.g., [11, 1, 8, 3, 9]. The vast majority of cryptocurrencies are based on the notion of proof of work (PoW) [25]. As a result, the major strategic players in the context of cryptocurrencies are *miners* who devote their power to solving computational puzzles to find PoWs [25, 11].

The miners for a particular coin usually gain rewards that are proportional to the power they invest in the coin out of the total invested power (in the coin) by all miners. Each coin, therefore, can be viewed as having some *weight* that reflects the reward it divides among its miners. In practice, a coin's weight (or reward) depends on its transaction rate, transaction fees, and its fiat exchange rate.

While the above description is not complete, it does capture the fundamental decision faced by the miner: where should I mine? One indication for reward-based coin switching can be found online in websites like www.whattomine.com [10], where miners enter their mining parameters (technology, power, cost, et cetra) and get a list of coins they can mine for, ordered by their profitability. Another interesting example happened on November 12 (2017) [5], when a dramatic change in the Bitcoin to Bitcoin Cash [1] (a spin-off from Bitcoin) exchange rate led to a major inrush of miners from Bitcoin to Bitcoin Cash (see Figure 1).

All in all, the structure of the cryptocurrency market suggests that we face here a game among miners, where each miner wishes to mine coins of heavy weights while avoiding competition with other miners. In this paper we introduce for the first time the study of the cryptocurrency market as a game, consisting of a set of strategic players (miners) with possibly different mining powers and a set of coins with possibly different rewards (weights). The miners are free to choose to mine for any coin from the set, and we consider general better-response learning of the miners. That is, whenever

Preprint. Work in progress.