GBBC Global Blockchain Business Council

Open Learning Forum

On the Instability of Bitcoin Without the Block Reward

Miles Carlsten; Harry Kalodner; S. Matthew Weinberg; and Arvind Narayanan
Princeton University
Date Published: 10/2016

Executive Summary written by GBBC

Introduction

Bitcoin miners generate revenue for themselves through both block rewards and transaction fees. As the system matures, block rewards revenue decreases, which many assume will be offset by an increase in transaction fee revenue. The block reward is halved every four years, as miners approach the 21,000,000-bitcoin limit. The security of Bitcoin is directly related to the actions of miners, which could become more complicated as block rewards continue to decrease.

The Mining Gap

"Without a block reward, immediately after a block is found there is zero expected reward for mining but nonzero electricity cost, making it unprofitable for any miner to mine." Without the block reward and with constant energy costs, miners will not profit until they process a certain number of transactions. This creates a mining gap that would cause rational miners to mine for shorter periods of time between new blocks; this would decrease the network's hash power and make it easier for nefarious actors to fork.

New Strategies

Without the block reward, miners will employ new strategies to generate the greatest possible revenue in transaction costs. According to the simulation, miners will first discover that they achieve greater revenue by mining on a block with the greatest number of unclaimed transaction fees, as opposed to mining on the oldest block. Next, nefarious miners will begin to intentionally fork the chain and incentivize transaction-fee-seeking miners to mine on their own block, rather than the oldest. This strategy is known as "undercutting," and the simulation (in which all miners are strategic learners) suggests it will continue until miners reach an equilibrium in which they are all using the same undercutting strategy.

Selfish Mining

Selfish mining is a strategy in which a miner does not publish a new block after it is found. This is done in the expectation that other miners will waste mining power on soon-to-be-orphaned blocks. The simulation found that selfish mining becomes more profitable when the block reward is eliminated. Most worryingly, it "strictly and always outperforms… default mining." Greater adoption of selfish mining would have serious negative consequences for the security of Bitcoin.

Lessons for Cryptocurrencies

Clearly, the transition from mining for a block reward to mining for transaction fees will not be simple for Bitcoin. The paper identified multiple strategies that could be implemented as miners look for new ways to generate as much revenue as possible. These strategies would diminish the effective hash power of honest miners while making a 51% attack "possible with much less than 51% of the hash power." The authors suggest that a permanent block reward and the ensuing inflation could be an acceptable tradeoff for improved security and stability. The most prominent blockchain with a permanent block reward is Ethereum.