Technical Perspective

The Rewards of Selfish Mining

By Sharon Goldberg and Ethan Heilman

AMIDST ALL THE hype surrounding blockchain and cryptocurrency, it is worth stepping back to understand how cryptocurrency technology broke through to the mainstream. While the community has been developing digital currency systems since the 1980s, Bitcoin was the first to see widespread use. Bitcoin has two crucial properties that set it apart from prior proposals. First, Bitcoin is decentralized; instead of passing transactions through a central bank, Bitcoin uses a decentralized network of *miners* and a distributed consensus algorithm to agree on a single public ledger of transactions called the *blockchain*. The blockchain is just a list of blocks, each of which contains a set of confirmed transactions. Second, Bitcoin has baked-in incentives: miners compete to add a block to the blockchain by solving a computational puzzle, and the winning miner claims several bitcoins as a *mining reward*. This incentive structure has given rise to a thriving industry of bitcoin miners.

When the Bitcoin protocol was first announced, the community assumed that each time a miner successfully solved a computational puzzle, she would immediately announce her solution to the network. After all, if our miner delayed announcing her solution to the network, some other miner might find his own solution and preemptively claim the mining reward. As such, the 2009 Bitcoin white paper makes an implicit assumption of perfect information—that all miners have the same view of the blockchain, and each time a miner solves a puzzle, the puzzle solution and corresponding block is immediately known to all other miners.

The following paper by Eyal and Sirer was the first to question this assumption.

The authors made two crucial observations. First, they noticed that while Bitcoin miners were assumed to act independently, in practice, miners organized themselves in pools of

collective cooperation. These *mining pools* collectively work toward solving each puzzle while sharing the resulting mining rewards. Second, they observed that strategic information propagation could be exploited to increase mining rewards. Specifically, the authors find that mining pools can increase their cumulative mining rewards by *selfish mining*, or strategically sharing puzzle solutions within their own mining pool, while delaying the announcement of those solutions to the Bitcoin network at large.

This surprising result, which was also one of the earliest academic analyses of the Bitcoin protocol, flew in the face of the conventional wisdom of the time. The authors showed that it is not incentive-compatible for miners to “honestly” follow the Bitcoin consensus algorithm, an observation that has serious implications on the security of Bitcoin’s consensus algorithm.

This paper was controversial when it was first made public. Sirer announced this paper on November 3, 2013 by tweeting “You heard it here first: now is a good time to sell your Bitcoins” because “[Bitcoin is] fundamentally broken at the protocol layer.” The authors took an unusual step of publicly disclosing their selfish-mining attack without first informing the Bitcoin developers. More typically, with responsible disclosure, a

security vulnerability is disclosed to the public only after a period of time that allows the vulnerability to be patched.

The authors argue that there were several barriers to this type of responsible disclosure. First, because Bitcoin developers are a distributed organization that eschews traditional forms of governance, there was no clear point of contact for securely disclosing protocol vulnerabilities. Second, because some of the Bitcoin developers could be involved in Bitcoin mining, the authors worried that the developers could leak the attack to certain Bitcoin miners, who might then begin to exploit it. Third, there was no clear way to resolve this issue, since making changes to Bitcoin’s consensus algorithm requires the consensus of all the Bitcoin miners, and arriving at this consensus is no easy task.^a The confusion following the announcement of this paper highlighted a key issue that remains open today: What is the right process for responsibly disclosing security vulnerabilities to decentralized blockchain projects?

Beyond this, Eyal and Sirer’s work triggered a burgeoning area of academic research on blockchain consensus algorithms and security. We are currently in the midst of an unusually fast-moving period where academic research results are quickly transitioned into production blockchain projects. What better way to learn about this exciting space than by reading one of the papers that started it all.

Eyal and Sirer’s work triggered a burgeoning area of academic research on blockchain consensus algorithms and security.

^a Indeed, just last August, disagreements about changes to Bitcoin’s consensus algorithm caused Bitcoin to split into two blockchains—Bitcoin (BTC) and Bitcoin Cash (BCH).

Sharon Goldberg is an associate professor in the Department of Computer Science at Boston University, Boston, MA, USA, and co-founder/CEO of Commonwealth Crypto, Inc.

Ethan Heilman is a Ph.D. student in computer science at Boston University, Boston, MA, USA, and co-founder/CTO of Commonwealth Crypto, Inc.