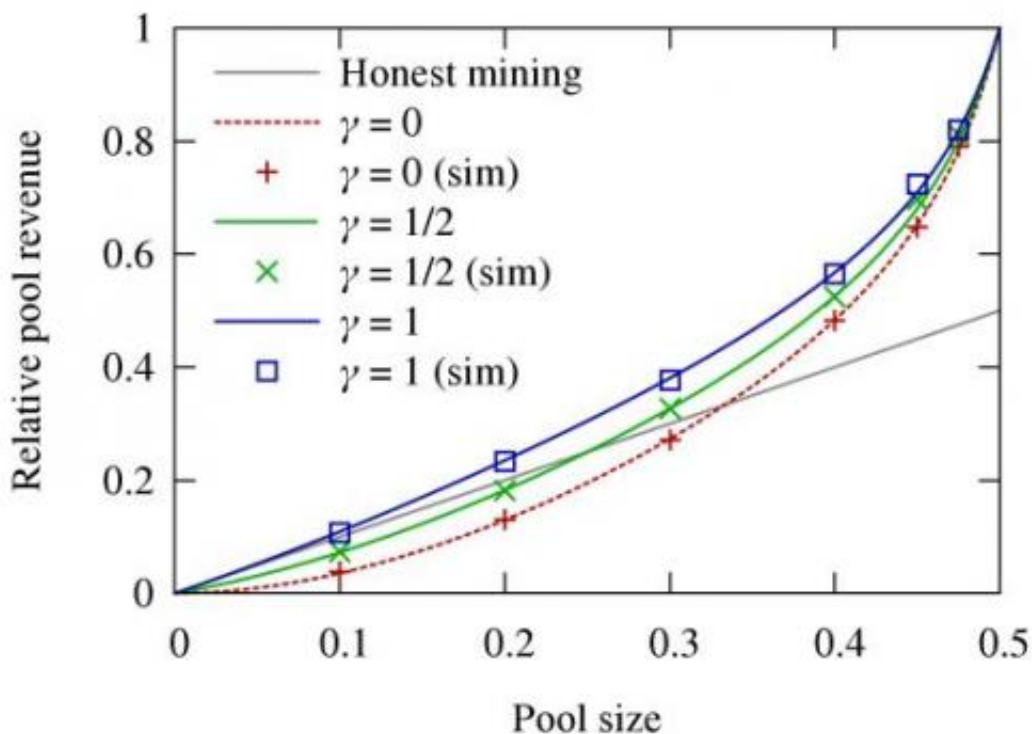


Cornell researchers teach Bitcoin attack lesson in selfish mining

November 6 2013, by Nancy Owano



Pool revenue using the Selfish-Mine strategy for different propagation factors, compared to the honest Bitcoin protocol. Simulation matches the theoretical analysis, and both show that Selfish-Mine results in higher revenues than the honest protocol above a threshold. Credit: arXiv:1311.0243 [cs.CR] .

(Phys.org) —Bitcoin is a digital currency that has, well, gained currency, as a medium of exchange. Now two computer science researchers from Cornell find that this extensive ecosystem can be undermined and they

outline how in a paper that they have posted on arXiv.

The paper, "Majority is not Enough: Bitcoin Mining is Vulnerable," is by Ittay Eyal, a postdoc member of the Computer Sciences department at Cornell and Emin Gun Sirer, associate professor at Cornell. According to the two researchers, "Empirical evidence shows that Bitcoin miners behave strategically and form pools. Specifically, because rewards are distributed at infrequent, random intervals miners form mining pools in order to decrease the variance of their income rate. Within such pools, all members contribute to the solution of each cryptopuzzle, and share the rewards proportionally to their contributions. To the best of our knowledge, so far such pools have been benign and followed the protocol." Nonetheless, they describe a strategy that could be used by a minority pool to obtain more revenue than the pool's fair share, that is, more than its ratio of the total mining power. "The key idea behind this strategy, called Selfish Mining, is for a pool to keep its discovered blocks private, thereby intentionally forking the chain," they wrote. This selfishness can come out of people getting together to siphon off more money than a fair share for mining activities.

The authors wrote that central to Bitcoin operations is a public log called the blockchain where all transactions are recorded. The security of the blockchain is established by a chain of cryptographic puzzles solved by a loosely organized network of participants called miners. The two researchers present an attack with which colluding miners obtain a revenue larger than their fair share. "This attack can have significant consequences for Bitcoin," they warned, where rational miners join selfish miners and the colluding group increases increase in size until it becomes a majority. At this point, they said, the Bitcoin system ceases to be a decentralized currency.

A *Scientific American* report on their findings further explained how damage might occur: Instead of releasing solutions to solved

cryptopuzzles. The selfish crew can mine a branch in secret, hiding it from honest miners. The group would then get a higher share of coins than is fair for the resources they have contributed because they have forced other miners to waste computing power on the original chain. The problem gets worse as the selfish group recruits extra members.

Elsewhere, the two were asked if they were trying to take Bitcoin down with their sober warning. "We're Bitcoin supporters," they blogged, "and are working to make the currency stronger against a broader set of possible misbehaviors than what has been considered so far." They proposed in their paper a practical modification to the Bitcoin protocol that protects against selfish mining pools. Can Bitcoin remain a viable currency? Sirer said, "Probably. We have shown that as long as selfish miners are below a certain threshold, they will not succeed."

More information: Majority is not Enough: Bitcoin Mining is Vulnerable, arXiv:1311.0243 [cs.CR]: arxiv.org/abs/1311.0243
[hackingdistributed.com/2013/11 ... /faq-selfish-mining/](http://hackingdistributed.com/2013/11/.../faq-selfish-mining/)
[www.newscientist.com/article/d ... irtual-currency.html](http://www.newscientist.com/article/d...irtual-currency.html)

© 2013 Phys.org

Citation: Cornell researchers teach Bitcoin attack lesson in selfish mining (2013, November 6) retrieved 3 April 2024 from <https://phys.org/news/2013-11-cornell-bitcoin-lesson-selfish.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.