One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner (Poster Abstract)

Ethan Heilman(✉)

Boston University, Boston, USA
heilman@bu.edu

1 Abstract

In "Majority is not Enough: Bitcoin Mining is Vulnerable", Eyal and Sirer study a Bitcoin mining strategy called selfish mining [1]. Under selfish mining, miners strategically withhold blocks to cheat Bitcoin's mining incentive system. This represents a 'tragedy of the commons' in which selfish behavior is incentivized over honest behavior, eventually causing most miners to adopt the selfish strategy, despite it being harmful to Bitcoin [2] as a whole.

The success of selfish mining depends on two parameters: α, the mining power of the selfish cartel and γ, the ratio of honest mining power that, during a block race, mines on a block released by the selfish cartel. We can view the minimum value of α, such that selfish mining is successful, as the security threshold for a particular γ.

Using Eq. 1, Eyal and Sirer show, if $\gamma = 0$, then selfish mining is profitable at $\alpha \geq 0.33$ or 33 %, whereas if $\gamma = 0.99$, then selfish mining is profitable at $\alpha \geq 0.009$. Eyal and Sirer propose a defense against selfish mining which fixes $\gamma = 0.5$. This raises the threshold for a selfish cartel to be profitable to at least 25 % or $\alpha \geq 0.25$.

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2} \tag{1}$$

We introduce a new defense, called FP (Freshness Preferred), improving on the previous best result of Eyal and Sirer. FP changes the Bitcoin protocol by adding unforgeable timestamps to blocks and preferring blocks with more recent blocks to blocks with older timestamps. We use Random Beacons [3] to prevent miners from faking timestamps from the future. Thus, as selfish mining is based on the strategic withholding of blocks, our strategy decreases the profitability of selfish mining because withheld blocks will lose block races against newly minted or "fresh" blocks.

Under FP we show that γ can be found as a function of t, $\gamma = 1 - e^{-\frac{(1-\alpha)}{600} \times t}$, where t is the refresh rate of the random beacon. We plug our equation for γ into Eq. 1 to find Eq. 2, the equation for the threshold of mining power to successfully selfishly mine within FP.

R. Böhme et al. (Eds.): FC 2014 Workshops, LNCS 8438, pp. 161–162, 2014.
DOI: 10.1007/978-3-662-44774-1_12

$$\text{threshold of } \alpha \text{ needed} = \frac{1 - (1 - e^{-\frac{(1-\alpha)}{600} \times t})}{3 - 2 \times (1 - e^{-\frac{(1-\alpha)}{600} \times t})} \quad (2)$$

Using the NIST random beacon [5], which generates random 512-bit strings every 60 s, as our model, we set $t = 60$ s and find that under all $\alpha \leq 0.32$, selfish mining is less profitable than honest mining, raising the mining power to selfishly mine to 32 % [4].

Next, we consider the mining power to selfishly mine within FP, assuming a cartel that can forge timestamps. Using the heuristic of "overestimate the attacker and underestimate the defender", we assume the cartel has no propagation delay, that it learns about honest blocks instantly, and that the honest miner has a lengthy propagation delay of 100 s and a block race window of 120 s. Under these assumptions, we find that the threshold for selfish mining with forgeries is 30 %.

FP with forgeable timestamps, while resistant to selfish mining, enables a new attack we call slothful mining. A slothful miner chooses timestamps slightly greater than the current time. The slothful miner can then withhold and mine on any block they discover, until the timestamp matches the current time, without hurting their chances of winning a block race. Slothful mining is not possible if the timestamps are unforgeable and therefore slothful mining motivates the use of unforgeable timestamps in FP.

We propose a incentive-compatible deployment scheme for FP. If the default miners significantly outnumber the FP miners, FP miners are at a disadvantage because if there is a block race between default miners and FP miners, the FP miners will likely lose. To solve the incentive problem, FP miners initially use the default block preference behavior, but they still add timestamps. When more than half of the most recent blocks in the blockchain for 30 days include unforgeable timestamps, then FP miners begin preferring the most recent blocks, as this behavior has become incentive-compatible. See our full report for details [4].

Acknowledgments. We thank Sharon Goldberg for comments and suggestions on drafts of this paper.

References

1. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. arXiv:1311.0243 (2013). http://arxiv.org/abs/1311.0243
2. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. The Cryptography Mailing List (2008). http://Bitcoin.org/Bitcoin.pdf
3. Rabin, M.: Transaction protection by beacons. J. Comput. Syst. Sci. **27**(2), 256–267 (1983). (Elsevier, Amsterdam)
4. Heilman, E.: One Weird Trick to Stop Selfish Miners: Fresh Bitcoins. A Solution for the Honest Miner. Cryptology ePrint Archive, Report 2014/007 (2013). https://eprint.iacr.org/2014/007.pdf
5. Iorga, M.: NIST, NIST Randomness Beacon (2013). http://www.nist.gov/itl/csd/ct/nist_beacon.cfm