

The Gap Game

Itay Tsabary
Technion
Haifa, Israel
itaytsabary@gmail.com

Ittay Eyal
Technion
Haifa, Israel
ittay@technion.ac.il

CCS CONCEPTS

• **Security and privacy** → **Distributed systems security**;

KEYWORDS

Blockchains; Cryptocurrency; Mining Gap; Centralization; Game Theory

Blockchain-based cryptocurrencies secure a decentralized consensus protocol by incentives. The protocol participants, called miners, generate (mine) a series of blocks, each containing monetary transactions created by system users. As incentive for participation, miners receive newly minted currency and transaction fees paid by transaction creators. Blockchain bandwidth limits lead users to pay increasing fees in order to prioritize their transactions. However, most prior work focused on models where fees are negligible. In a notable exception, Carlsten et al. [1] postulated in CCS'16 that if incentives come only from fees then a mining gap would form — miners would avoid mining when the available fees are insufficient.

In this work, we analyze cryptocurrency security in realistic settings, taking into account all elements of expenses and rewards. To study when gaps form, we analyze the system as a game we call *the gap game*. We analyze the game with a combination of symbolic and numeric analysis tools in a wide range of scenarios.

Our analysis confirms Carlsten et al.'s postulate; indeed, we show that gaps form well before fees are the only incentive, and analyze the implications on security. Perhaps surprisingly, we show that different miners choose different gap sizes to optimize their utility, even when their operating costs are identical. Alarming, we see that the system

incentivizes large miner coalitions, reducing system decentralization. We describe the required conditions to avoid the incentive misalignment, providing guidelines for future cryptocurrency design.

REFERENCES

- [1] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 154–167. <https://doi.org/10.1145/2976749.2978408>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
SYSTOR, 2018, Haifa, Israel

© 2018 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.

ACM ISBN 123-4567-24-567/08/06...\$15.00

https://doi.org/10.475/123_4