Incentive Analysis of Bitcoin-NG, Revisited *

Jianyu Niu
School of Engineering
University of British Columbia
Kelowna, Canada
jianyu.niu@ubc.ca

Ziyu Wang
School of Cyber Science and Technology
Beihang University
Beijing, China
wangziyu@buaa.edu.cn

Fangyu Gai
School of Engineering
University of British Columbia
Kelowna, Canada
fangyu.gai@ubc.ca

Chen Feng
School of Engineering
University of British Columbia
Kelowna, Canada
chen.feng@ubc.ca

ABSTRACT

Bitcoin-NG is among the first scalable blockchain protocols by decoupling blockchain operation into two planes: leader election and transaction serialization. Its decoupling idea has inspired a new generation of blockchain protocols. However, the existing incentive analysis of Bitcoin-NG has several limitations. First, the impact of network capacity is ignored. Second, an integrated incentive analysis that jointly considers both key blocks and microblocks is still missing.

In this paper, we aim to address these two limitations. First, we propose a new incentive analysis that takes the network capacity into account, showing that Bitcoin-NG can still maintain incentive compatibility against the microblock mining attack even under limited network capacity. Second, we leverage a Markov decision process to jointly analyze the incentive of both key blocks and microblocks, showing that the selfish mining revenue of Bitcoin-NG is a little higher than that in Bitcoin only when the selfish miner controls more than 35% of the mining power. We hope that our in-depth incentive analysis for Bitcoin-NG can shed some light on the mechanism design and incentive analysis of next-generation blockchain protocols.

Keywords

Blockchains, Bitcoin, Bitcoin-NG, Nakamoto Consensus, Incentive Analysis, Markov decision process (MDP)

1. INTRODUCTION

Bitcoin—the largest and most influential cryptocurrency—has sparked many other cryptocurrencies like Ethereum [2] and Litecoin [10], gaining much attention from both academia and industry [7]. The key innovation behind Bitcoin is *Nakamoto Consensus* (NC), which is used to realize a distributed ledger known as a blockchain. Blockchains have unique features in decentralization, security and privacy, making them a fundamental trust infrastructure for supporting various future decentralized Internet applications, ranging from IoT [11], health care [6], to supply chain management [12].

Despite the popularity, Bitcoin and its variants have suffered from low throughput (e.g., 7 TPS[1] in Bitcoin). The low throughput of Bitcoin is mostly due to its choice of two system parameters: small block size (originally 1 MB) and long block interval (on average 10 minutes). Although increasing the block size or shortening the block interval can increase the throughput, this reduces the security level of Bitcoin because forks are more likely to occur [4, 8, 14]. Indeed, various studies show that redesigning the underlying NC (rather than fine-tuning the system parameters) is essential to improve the throughput without sacrificing security [3, 14].

Bitcoin-NG (Next Generation) [3] is among the first and the most prominent scalable blockchain protocols. Bitcoin-NG creatively employs two types of blocks: 1) a *key block* that is very similar to a conventional block in Bitcoin except that it doesn't carry any transactions, and 2) a *microblock* that carries transactions. Every key block is generated through the leader election process (often known as the mining process) in NC, and the corresponding leader will receive a block reward (if its key block ends up in the longest chain). In addition, this leader can issue multiple microblocks and receive the transaction fees until the next key block is generated. Unlike Bitcoin, Bitcoin-NG decouples leader election and transaction serialization. Intuitively, it is this decoupling that enables Bitcoin-NG to greatly improve the throughput, since the microblocks can be produced at a higher rate. Perhaps for this reason, Bitcoin-NG has been adopted by two cryptocurrencies: Waves[2] and Aeternity[3].

More importantly, this decoupling idea has inspired a new generation of blockchain protocols including ByzCoin [5], Hybrid consensus [9], Prism [1], and many others. Although these protocols are able to achieve lower latency and/or higher throughput than Bitcoin-NG, their incentive mechanism design and analysis still remain unclear. Such incentive analysis is particularly important for understanding

*This project has been funded in part through NSERC Discovery Grant RGPIN-2016-05310 as well as joint NSERC Engage and MITACS Accelerate grant EGP-538022-19 and IT14586.

IFIP WG 7.3 Performance 2020. Nov. 2-6, 2020, Milan, Italy

[1]TPS is short for transactions per second.
[2]Waves: https://docs.wavesplatform.com/
[3]Aeternity: https://aeternity.com/

incentive-based attacks, in which all the nodes are assumed to be rational and profit driven. Indeed, even the existing incentive analysis of Bitcoin-NG has several limitations, as we will explain shortly. As a starting point to bridge this research gap, we aim to provide an in-depth incentive analysis for Bitcoin-NG, hoping that it would shed some light on the mechanism design and incentive analysis of aforementioned next-generation blockchain protocols.

The prior work of Bitcoin-NG found that Bitcoin-NG cannot maintain the incentive compatibility[4] of microblocks when an adversary controls more than 29% of the total computation power [3, 16]. In addition, an adversary in Bitcoin-NG can gain a higher share of block reward than in Bitcoin, making Bitcoin-NG more vulnerable [15]. Despite these important findings, previous incentive analysis of Bitcoin-NG has the following limitations. First, previous analysis completely ignores the impact of network capacity [3, 16, 15]. *How can we take into account the network capacity constraints*? Second, previous analysis mostly focuses on microblocks. *How can we take into account the effect of key blocks*?

To answer the first question, we develop a new probabilistic analysis that takes network capacity into account. In particular, we model the interval between two consecutive key blocks as an exponential random variable and introduce the generation rate of microblocks to capture the impact of network capacity. Then, we apply the Chernoff-type bounding techniques to derive the long-term average revenue of the adversary. We find that by choosing suitable system parameters, Bitcoin-NG can still maintain incentive compatibility even under network capacity constraints. In other words, introducing network capacity constraints doesn't make it harder to maintain the incentive compatibility. More specifically, when the adversary controls less than 29% of the mining power, the incentive compatibility of Bitcoin-NG can be maintained for all types of transactions. When the adversary controls more than 29% of the mining power, the incentive compatibility can be maintained for regular transactions but not for whale transactions with high fees.

To address the second question, we leverage a Markov decision process (MDP) model to jointly analyze the incentive of key blocks and microblocks. Although similar analysis has been conducted by Sapirshtein et al. [13] in the context of Bitcoin[5], the microblock structure in Bitcoin-NG introduces additional complexity for the MDP design (e.g., more mining strategies and rewards). To make the MDP tractable, we confine our analysis to a family of selfish mining strategies. Our results show that the optimal selfish mining revenue in Bitcoin-NG is only a little higher than that in Bitcoin when the selfish computation power is greater than 35%.

Contributions: The contributions of this paper are summarized as follows:

- We propose a new incentive analysis of Bitcoin-NG considering the network capacity constraints. Our results show that Bitcoin-NG can still maintain incentive compatibility against the microblock mining attack.
- We model the selfish mining of key blocks and microblocks jointly into an MDP. Our results show that the selfish mining revenue in Bitcoin-NG is a little higher than that in Bitcoin only when the selfish mining power α is greater than 35%.
- We show the distribution of transaction fees by scanning transactions in a recent block history of Bitcoin, which supports our assumptions in our system model.

[4]The expected relative revenue of a miner should be proportional to its mining power.

[5]Due to the similarity, the MDP can be directly used to model the key-block mining in Bitcoin-NG.

2. REFERENCES

[1] Bagaria, V. K., Kannan, S., Tse, D., Fanti, G. C., and Viswanath, P. Prism: Deconstructing the blockchain to approach physical limits. In *CCS 2019*, pp. 585–602.

[2] Buterin, V., et al. A next-generation smart contract and decentralized application platform. *white paper* (2014).

[3] Eyal, I., Gencer, A. E., Sirer, E. G., and Renesse, R. V. Bitcoin-NG: A scalable blockchain protocol. In *NSDI 2016*, pp. 45–59.

[4] Garay, J. A., Kiayias, A., and Leonardos, N. The Bitcoin backbone protocol: Analysis and applications. In *EUROCRYPT 2015* (2015), pp. 281–310.

[5] Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., and Ford, B. Enhancing Bitcoin security and performance with strong consistency via collective signing. In *USENIX Security 2016*, pp. 279–296.

[6] Mettler, M. Blockchain technology in healthcare: The revolution starts here. In *IEEE Healthcom 2016*.

[7] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Working Paper* (2008).

[8] Pass, R., Seeman, L., and Shelat, A. Analysis of the blockchain protocol in asynchronous networks. In *EUROCRYPT 2017*, pp. 643–673.

[9] Pass, R., and Shi, E. Hybrid consensus: Efficient consensus in the permissionless model. In *DISC 2017*, vol. 91, pp. 39:1–39:16.

[10] Reed, J. *Litecoin: An Introduction to Litecoin Cryptocurrency and Litecoin Mining*. 2017.

[11] Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. On blockchain and its integration with IoT. challenges and opportunities. *Future generation computer systems* (2018).

[12] Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research* (2019), 2117–2135.

[13] Sapirshtein, A., Sompolinsky, Y., and Zohar, A. Optimal selfish mining strategies in Bitcoin. In *FC 2016*, pp. 515–532.

[14] Sompolinsky, Y., and Zohar, A. Secure high-rate transaction processing in Bitcoin. In *FC 2015*, pp. 507–527.

[15] Wang, Z., Liu, J., Zhang, Z., Zhang, Y., Yin, J., Yu, H., and Liu, W. A combined micro-block chain truncation attack on Bitcoin-NG. In *ACISP 2019*, pp. 322–339.

[16] Yin, J., Wang, C., Zhang, Z., and Liu, J. Revisiting the incentive mechanism of Bitcoin-NG. In *ACISP 2018*, pp. 706–719.