BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model

Extended Abstract

Shoeb Siddiqui
International Institute of Information Technology
Hyderabad, Telangana
shoeb.siddiqui@research.iiit.ac.in

Ganesh Vanahalli
International Institute of Information Technology
Hyderabad, Telangana
ganesh.vanahalli@students.iiit.ac.in

Sujit Gujar
International Institute of Information Technology
Hyderabad, Telangana
sujit.gujar@iiit.ac.in

ABSTRACT

A blockchain, such as Bitcoin, is an append-only, secure, transparent, distributed ledger. A fair blockchain is expected to have healthy metrics; high honest mining power, low *processing latency*, i.e., low wait times for transactions and stable *price of consumption*, i.e., the minimum transaction fee required to have a transaction processed. As Bitcoin matures, the influx of transactions increases and the block rewards become insignificant. We show that under these conditions, it becomes hard to maintain the *health of the blockchain*. In Bitcoin, under these *mature operating conditions*, the miners would find it challenging to cover their mining costs as there would be no more revenue from merely mining a block. It may cause miners not to continue mining, threatening the blockchain's security. Further, as we show in this paper via simulations, the cost of acting in favor of the health of the blockchain, under mature operating conditions, is very high in Bitcoin. It causes all miners to process transactions greedily and leads to *stranded transactions*. To make matters worse, a compounding effect of these stranded transactions is the rising price of consumption. Such phenomena not only induce unfairness as experienced by the miners and the users but also deteriorate the health of the blockchain.

We propose BitcoinF transaction processing protocol, a simple, yet highly effective modification to the existing Bitcoin protocol to fix these issues of unfairness. BitcoinF resolves these issues of unfairness while preserving the ability of the users to express urgency and have their transactions prioritized.

KEYWORDS

blockchain, game theory, fairness, transaction fees

ACM Reference Format:
Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. 2020. BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model. In *Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), Auckland, New Zealand, May 9–13, 2020,* IFAAMAS, 3 pages.

1 INTRODUCTION

Blockchain, introduced in Bitcoin [12] by Nakamoto, is an append-only, secure, transparent, distributed ledger, storing data in blocks connected through immutable cryptographic links, with each block extending exactly one previous block. In blockchain technology, the *miners* validate transactions, that the *users publish* (create and broadcast), and add them into the next block(s).

In Bitcoin, for investing resources into mining, there are two types of rewards offered to the miners: *block rewards*, currency minted in every block, and *transaction fees*, incentives offered by the users to the miners to prioritize their transactions. It is due to this investment that miners benefit from the *health of the blockchain*.

To control inflation, block rewards are halved every four years in Bitcoin. Over time, the only incentive that remains for the miners is the transaction fee, i.e., the *transaction-fee-only model* (TFOM). When the block rewards can cover mining costs, the miners can afford to act in favor of the blockchain's health. This is not the case in TFOM. In [2], the authors show that in TFOM under low *influx* (incoming volume of transactions), the rational miners will *undercut* instead of following default strategy. While this analysis considers the impact of rational miners in TFOM w.r.t. *forking*, it does not consider the processing latency and the price of consumption.

We refer to the case when influx on an average is equal to the maximum outflux (processing capacity) of the blockchain as *standard influx*. The two conditions, TFOM and standard influx, inherently go hand-in-hand as the Bitcoin matures [1]. Thus, making it very important to study and contemplate such scenarios. In this paper, we analyze Bitcoin in TFOM and under standard influx, which we term as *mature operating conditions* (MOC), and show that it is unfair for both miners and users.

We solve these issues by proposing a novel protocol, BitcoinF. BitcoinF enforces a minimum transaction fee and uses two queues, instead of one to process transactions. While there have been many published works ([3–9, 11]) analyzing TFOM using collected data or using game-theoretic models, to the best of our knowledge this is the first formal attempt at solving these issues of unfairness.[1]

2 PRELIMINARY DEFINITION

Processing latency is the duration, in terms of blocks, between a user publishing a transaction and a miner processing it (publishing a block containing it).

Stranded transactions are those transactions, that experience unreasonably high processing latency (> 100 blocks).

Price of consumption is the minimum transaction fee, as perceived by the users, that must be paid for the transaction to be processed.

Health of a blockchain is characterized by (i) fraction of honest mining power, (ii) *processing latency*, and (iii) *price of consumption*.

[1] For details, please refer to the full version [14]

Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), B. An, N. Yorke-Smith, A. El Fallah Seghrouchni, G. Sukthankar (eds.), May 9–13, 2020, Auckland, New Zealand.

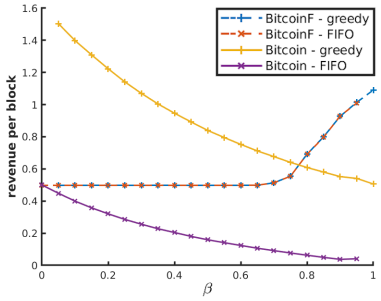

Figure 1: Difference in revenue

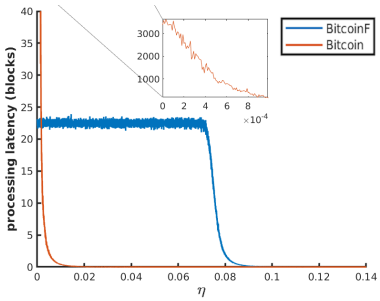

Figure 2: Processing latency vs η

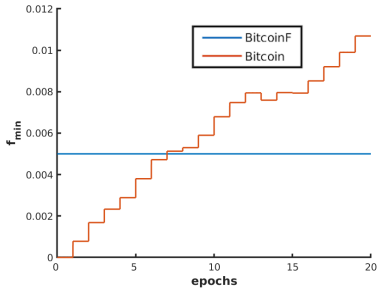

Figure 3: f_{min} vs steps

Individual fairness for the miners is satisfied, if the rewards from a block are at least the cost of mining a block.

Fairness for the users is satisfied, if the users experience (i) reasonable processing latency, (ii) stable price of consumption, and (iii) decreasing average processing latency with increasing aggression towards higher transaction fee.

We say that the blockchain ecosystem is fair if it satisfies individual fairness for the miners and fairness for the users. To quantify game theoretic properties, we use ϵ-Expected Dominant Strategy Equilibrium and ϵ-Expected Nash Equilibrium concepts, which mean that a deviation does not benefit by more than an ϵ fraction.

3 MODEL

We simulate the execution of the Bitcoin protocol in steps of 10 mins, i.e., a block is published every 10 mins. A block can contain a maximum $bs_{max} = 1000$ ([10, 13]) number of transactions. The number of transactions that arrive in each step is a *Poisson* with mean bs_{max}.

We split the transaction fee offered by the user as, $f_{txn} = f_{min} + f_{extra}$. f_{min} reflects the price of consumption as perceived by the users. The minimum transaction fee set by the protocol, $f^0_{min} \leq f_{min}$, is the initial f_{min}. f^0_{min} is 0 in Bitcoin. $f_{extra} = e^{\eta} - 1$ is the extra prioritization fee, where $0 \leq \eta < \infty$ is the aggression parameter of the user. We use an *exponential distribution* with rate parameter of 3 to represent the fraction of users having aggression level towards f_{extra} as η.

In Bitcoin, the strategy space is $S = \{FIFO, greedy\}$. In FIFO processing, the miners add transactions to the block in a *First-In-First-Out* manner. In *greedy* processing, the miners add the highest valued transactions to the block. We use granularity of 0.05 for the size of miners in terms of their relative mining power, and $0 \leq \beta \leq 1$ to be the fraction of miners that follow *greedy*, while the rest follow FIFO.

We assume that all miners are *honest but rational*. Since the health of the blockchain is crucial to the value miners obtain from mining, and that all miners inherently understand this, miners act in favor of sustaining the health of the blockchain, i.e., follow FIFO processing, if the cost of doing so is marginal.

When users, at the end of an observation epoch of length 1000 steps, observes transactions, below a certain threshold of fees, being stranded, they concede to making the presumption that this threshold of fees is the new f_{min}. This is because a user will not attempt to publish a transaction if they do not expect it to be processed.

4 BITCOINF

Our approach is two-fold: (i) we enforce a minimum fee of f^0_{min} that is to be included in every transaction. (ii) We introduce a section in the block that only accepts transaction instances with $f_{txn} = f^0_{min}$, called the FIFO section of the block. So now, there are two sections in the block: FM and FIFO. The FIFO section has a size of $\alpha \cdot bs_{max}$, whereas FM has the remaining. Since a transaction may be included in either section, the users publish two instances of each transaction: one that offers $f_{txn} = f^0_{min}$, another that offers $f_{txn} = f_{min} + f_{extra}$. The miners collect these transactions instances and add them to two separate queues, from which they respectively process these instances into the two sections. Once an instance of a transaction has been processed, the other is invalidated; thus, a transaction can be added to either the FM section or the FIFO section. In our simulation of BitcoinF, we set $\alpha = 0.2$ and $f^0_{min} = 0.005$.

In BitcoinF, the strategy space again is $S = \{FIFO, greedy\}$. S affects only the FIFO section of the block. The FM section is filled with the highest valued transactions in both FIFO and *greedy* processing. In FIFO processing, the miners add transactions to the FIFO section in a FIFO manner. In *greedy* processing, the miners add the least valued transactions to the FIFO section of the block, in the hopes of processing the higher valued transactions through the FM section later on. We also consider another strategy where the miner might process a transaction, that is about to be processed through the FIFO section, through the FM section; although this attack is not discussed here, we show that it yields negligible benefit.

5 RESULTS

The results of our simulations are depicted in Fig. **??**. From the Fig. 1, we see that: in BitcoinF it is *ϵ-Expected Nash Equilibrium* with $\epsilon = 0.00037$ for all miners to follow FIFO processing, which is in favour of the blockchain; while in Bitcoin it is *ϵ-Expected Dominant Strategy Equilibrium* with $\epsilon = 0$ to follow *greedy* processing of transactions. This results in transactions getting stranded in Bitcoin, which does not happen in BitcoinF, refer Fig. 2. The compounding effect of stranded transactions, the rising price of consumption, is visible in Fig. 3. Fig. 3 also implies that when the influx has not been *standard* for long enough, Bitcoin cannot ensure that mining costs will be covered, i.e., individual fairness for miners is not guaranteed, whereas individual fairness for miners is guaranteed in BitcoinF. Thus, we conclude that BitcoinF is a fair blockchain, whereas Bitcoin is not.

REFERENCES

[1] blockchain.com. 2019. Mempool Transaction Count. https://www.blockchain.com/charts/. (2019). Accessed: 15-November-2019.

[2] 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*. ACM, 154–167.

[3] David Easley, Maureen O'Hara, and Soumya Basu. 2019. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics* (2019).

[4] Nicolas Houy. 2014. The economics of Bitcoin transaction fees. *GATE WP* 1407 (2014).

[5] Gur Huberman, Jacob Leshno, and Ciamac C Moallemi. 2019. An economic analysis of the Bitcoin payment system. *Columbia Business School Research Paper* 17-92 (2019).

[6] Shoji Kasahara and Jun Kawahara. 2016. Effect of Bitcoin fee on transaction-confirmation process. *arXiv preprint arXiv:1604.00103* (2016).

[7] David Koops. 2018. Predicting the confirmation time of bitcoin transactions. *arXiv preprint arXiv:1809.10596* (2018).

[8] Joshua A Kroll, Ian C Davey, and Edward W Felten. 2013. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, Vol. 2013. 11.

[9] Juanjuan Li, Yong Yuan, Shuai Wang, and Fei-Yue Wang. 2018. Transaction Queuing Game in Bitcoin BlockChain. In *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 114–119.

[10] Bitcoin Magazine. 2019. What Is the Bitcoin Block Size Limit? https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit. (2019). Accessed: 15-November-2019.

[11] Malte Möser and Rainer Böhme. 2015. Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees. In *International Conference on Financial Cryptography and Data Security*. Springer, 19–33.

[12] Satoshi Nakamoto et al. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

[13] Peter R Rizun. 2015. A transaction fee market exists without a block size limit. *Block Size Limit Debate Working Paper* (2015).

[14] Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. 2020. BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model. *arXiv preprint arXiv:2003.00801* (2020).