We might walk together, but I run faster: Network Fairness and Scalability in Blockchains

Extended Abstract

Anurag Jain
Machine Learning Lab,
International Institute of Information Technology
Hyderabad, India
anurag.jain@research.iiit.ac.in

Shoeb Siddiqui
Machine Learning Lab,
International Institute of Information Technology
Hyderabad, India
shoeb.siddiqui@research.iiit.ac.in

Sujit Gujar
Machine Learning Lab,
International Institute of Information Technology
Hyderabad, India
sujit.gujar@iiit.ac.in

ABSTRACT

Blockchain-based Distributed Ledgers (DLs) promise to transform the existing financial system by making it truly democratic. In the past decade, blockchain technology has seen many novel applications ranging from the banking industry to real estate. However, in order to be adopted universally, blockchain systems must be scalable to support a high volume of transactions. As we increase the throughput of the DL system, the underlying peer-to-peer network might face multiple levels of challenges to keep up with the requirements. Due to varying network capacities, the slower nodes would be at a relative disadvantage compared to the faster ones, which could negatively impact their revenue. In order to quantify their relative advantage or disadvantage, we introduce two measures of network fairness, p_f, the probability of frontrunning and α_f, the publishing fairness. We show that as we scale the blockchain, both these measures deteriorate, implying that the slower nodes face a disadvantage at higher throughputs. It results in the faster nodes getting more than their fair share of the reward while the slower nodes (slow in terms of network quality) get less. Thus, fairness and scalability in blockchain systems do not go hand in hand.

In a setting with rational miners, lack of fairness causes miners to deviate from the "longest chain rule" or *undercut*, which would reduce the blockchain's resilience against byzantine adversaries. Hence, fairness is not only a desirable property for a blockchain system but also essential for the security of the blockchain and any scalable blockchain protocol proposed must ensure fairness.

KEYWORDS

Distributed Ledgers, Scalable Blockchains, Fairness, Peer-to-Peer Networks

ACM Reference Format:
Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. 2021. We might walk together, but I run faster: Network Fairness and Scalability in Blockchains: Extended Abstract. In *Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), Online, May 3–7, 2021*, IFAAMAS, 3 pages.

Proc. of the 20th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2021), U. Endriss, A. Nowé, F. Dignum, A. Lomuscio (eds.), May 3–7, 2021, Online.

1 INTRODUCTION

Blockchain-based *Distributed Ledgers* (DLs) promise to transform the existing financial system. The idea behind such a transformation is to replace centralized institutions that govern the system by a *decentralized* peer-to-peer network of nodes. The key idea behind a DL system is that it offers the right incentives to the nodes to act honestly according to the blockchain protocol's rules. Thus, any node can voluntarily choose to participate in the system and incur a computational cost in the expectation of being rewarded. If a decentralized system is not *fair*, i.e., the nodes do not receive proportionate incentives, they will prefer not to join the system [3, 5]. Consequently, the system will not remain democratic and decentralized if it excludes some nodes. Although the fairness properties that we describe appear to be healthy for current blockchain systems, they deteriorate quickly as we scale the system.

Overview Although cryptocurrencies like Bitcoin and Ethereum are quite popular today, they still lag behind centralized payment systems like Visa in terms of transaction rates and time to finality. As of February 2021, Bitcoin's and Ethereum's network processes an average of 3-4 and 10 transactions per second (TPS), respectively. In contrast, Visa's global payment system handled a reported 1,700 TPS [6]. For a cryptocurrency to be adopted universally, it must be able to scale to process transactions at much higher throughput, i.e., TPS rate. Hence, blockchain protocols must be scalable to be suitable for widespread adoption.

We consider a setting in which nodes are honest and show that disparities in the connection to the peer-to-peer network can make the system unfair. In such a case, nodes with a better connection will be able to grab a larger share of the reward while those with slower connections might lose out. We show that this disparity becomes significant as we increase the throughput of the system.

In literature, it is typically assumed that all the nodes have equal access to the network, albeit with some finite delay. However, this is seldom the case in practice where some nodes may have better network connections than others. For the first time, we introduce asymmetry in modeling network connections by assuming different delays for different nodes. Hence, faster nodes would have shorter delays, while slower nodes would have longer delays which in turn results in asymmetry in the rewards collected by these nodes. We define two new measures of fairness that try to quantify this disparity and show that they deteriorate when we increase the throughput of the blockchain. We also discuss possible behavior that a lack of network fairness could elicit from rational nodes

and show that their behavior could potentially hurt the stability of the system and reduce the effective throughput of the system. This could have adverse effect on the resilience of the blockchain against byzantine adversaries, making it less secure. Hence, even though we scale the system to increase the throughput, we might not find much practical advantage due to these issues. Thus, the potential of blockchain technology may be hindered by the limitations of the underlying networking infrastructure.

2 DIFFERENT NOTIONS OF FAIRNESS

In this paper, we analyze network fairness and establish measures independent of the computational power of the nodes we are comparing. Hence, we base our definitions on network events. We introduce two measures of fairness based on network events associated with broadcasting a transaction and broadcasting a block.

Frontrunning (p_f) (in this context) occurs when a node confirms a transaction before someone else hears about the transaction. We measure p_f, the probability of this event happening between two fractions of the network. To capture it more formally, we denote $\{p_f\}_m^M$ as the probability of the frontrunning between the top M percentile and the bottom $1-m$ percentile of nodes in terms of network delays, i.e., the probability that some node in the top M percentile manages to frontrun all nodes in the bottom $1-m$ percentile. If p_f is high, the faster nodes would consistently be able to grab high-value transactions while the slower ones would only be able to pick low-value ones left out by others. Thus, a high p_f would negatively impact some nodes' revenue.

Analyzing Frontrunning Let d be the time advantage offered to the top M fraction of the nodes, p is the probability of query being successful, and H be the hash rate of the network.

Theorem 2.1 (Lower bound of $\{p_f\}_m^M$). $\{p_f\}_m^M > M\lambda d - \frac{1}{2}(M\lambda d)^2$

Theorem 2.1 shows that $\{p_f\}_m^M$ increases monotonically with increasing the block creation rate λ when we scale the blockchain protocol since its lower bound increases monotonically. Although, it may seem that the lower bound is independent of the bottom m percentile selected but this would have been incorporated in d since d increases as m decreases.

Publishing Fairness (α_f) quantifies the advantage a node might have over others in broadcasting a block. If a node is able to propagate its block faster than others, in case of an eventual fork, its block would have a higher probability of being accepted. Since at higher throughputs forks become more common [2], faster nodes would be able to get more blocks accepted while those of slower nodes would frequently be orphaned. Thus, the slower nodes, would not be able to even gather the fixed block rewards. Consider two nodes A and B that mine a block simultaneously. α_f quantifies the advantage of A in terms of publishing a block and claiming the associated reward. It is formally defined in Equation 1. The intuition behind this definition is that over multiple rounds, this would be the ratio of their conflicting blocks getting accepted.

$$\alpha_f(A,B) = \frac{P(\frac{\text{A's block getting accepted}}{\text{A and B mine a block simultaneously}})}{P(\frac{\text{B's block getting accepted}}{\text{A and B mine a block simultaneously}})} \tag{1}$$

Analysis of Publishing Fairness We assume that the execution happens in "rounds" in which the nodes make q queries each to the Hash Function, each of which may be successful with probability p. At the boundaries of rounds, the nodes can communicate with their neighboring nodes. If ϕ_A^i and ϕ_B^i are the fraction of network accepting A and B at the i^{th} round and H be the total hashrate of the network. Then, α_f can be approximated by Theorem 2.2.

Theorem 2.2 (Approximation of α_f).

$$\alpha_f = \frac{\psi}{1-\psi} \tag{2}$$

where $\psi = \sum_{i=1}^{\infty}\left[\prod_{j=0}^{i-1}[(1-fail(\phi_A^j))(1-fail(\phi_B^j)) + fail(\phi_A^j)fail(\phi_B^j)] \times (1-fail(\phi_A^i))fail(\phi_B^i)\right]$
and $fail(\phi) = (1-p)^{\phi H}$

3 FAIRNESS AND STRATEGIC DEVIATIONS

Both the fairness measures deteriorate as with increased throughput due to which, small variations in network access may lead to the system becoming unfair for the slower nodes. This could certainly impact the profitability of the nodes that earn less since they still need to pay for the costs associated with mining. Thus, it may lead to drop in the nodes maintaining the DL since nodes that are unable to accumulate enough reward to break even the mining costs might shut down their mining operation or they might adopt strategic behavior to collect more rewards than that obtained by following the protocol honestly, either of which would reduce the security of the blockchain [3].

For analysis, we divide the network into two portions: *slow* and *fast*. The fast nodes can receive messages broadcasted by any node in the previous round, but the slow nodes have higher communication delays. Each node can choose from the following strategies:

(1) `petty`: The petty mining strategy described in [1]. Given two forks, it picks the one which offers a greater reward. It weakly dominates the default strategy in Bitcoin but it is not harmful to the security of the blockchain on its own.
(2) `minor_undercutting`: A node will undercut if the longest chain's reward is below a certain threshold. However, it would leave out a small constant reward as an incentive for the subsequent nodes that pick the block.
(3) `major_undercutting`(κ): Same as `minor_undercutting` but it would leave out a significant portion of the reward (κ) as an incentive for the subsequent nodes that pick the block.

To study these strategic deviations at high throughputs, we developed a simulator and made the following observations:

(1) The blockchain system would have been secure against any strategic deviations if (`petty`, `petty`) had been an equilibrium strategy due to lack of publishing fairness.
(2) In all equilibria strategies, all nodes choose `major_undercutting`. This would be even worse for the slower nodes in terms of fairness since they grab an even smaller share of reward as compared to the strategy where all players act honestly.

Thus, if nodes act rationally not only would security of the blockchain be adversely affected, the lack of fairness among the rewards received by the slower miners would also be exacerbated.

We request the reader to refer to the full version of this paper for a more detailed discussion [4].

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*. 154–167.

[2] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2014. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765. https://eprint.iacr.org/2014/765.

[3] Anurag Jain and Sujit Gujar. 2020. Block Rewards, Not Transaction Fees Keep Miners Faithful In Blockchain Protocols. In *Workshop on Game Theory in Blockchain at WINE 2020 (GTiB@WINE 2020)*. Beijing, China.

[4] Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. 2021. We might walk together, but I run faster: Network Fairness and Scalability in Blockchains. arXiv:2102.04326 [cs.DC]

[5] Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. 2020. BitcoinF: Achieving Fairness For Bitcoin In Transaction Fee Only Model. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems* (Auckland, New Zealand) *(AAMAS '20)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2008–2010.

[6] Visa Inc. [n.d.]. VisaNet Booklet. https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/visa-net-booklet.pdf.