Topological Analysis of Bitcoin's Lightning Network

István András Seres[1], Dániel A. Nagy[1], and Péter Burcsi[1]

[1]Department of Computer Algebra, Eötvös Loránd University

January 6, 2019

Abstract

Bitcoin's Lightning Network (LN) is a scalability solution for Bitcoin, which allows transactions to be issued with negligible fees and settle transactions instantly at scale. In order to use LN funds need to be locked in payment channels on the Bitcoin blockchain (Layer-1), that one may use them in LN (Layer-2). LN is comprised of many payment channels forming a payment channel network. A few payment channels already enable anyone to efficiently, securely and privately route payments across the whole network. In this paper we argue that LN's current topological properties largely harms its value proposition and potential.

Keywords: Bitcoin, Lightning Network, Network Topology, Payment Channel Network

1 Introduction

Recently the Bitcoin [2] network celebrated its 10th anniversary. During these years Bitcoin gained a huge popularity due to its publicly verifiable, decentralized, permissionless and censorship-resistant nature. This tremendous popularity and increasing interest in Bitcoin pushed its network's throughput to its limits. Without further advancements, the Bitcoin network can only settle 7 transactions per second (tps), while mainstream centralized payment providers such as Visa and Mastercard can process approximately 40,000 tps in peak hours. Moreover one might need to pay large transaction fees on the Bitcoin network, while also need to wait 6 new blocks to be published in order to be certain enought that the transaction is included in the blockchain.

To alleviate these scalability issues the Lightning Network (LN) is designed in 2016 [3], and launched in 2018, January. The main insight of LN is that transactions can be issued also off-blockchain in a trust-minimized manner achieving instant transaction confirmation times with negligible fees, whilst retaining the security of the underlying blockchain.

Bidirectional payment channels can be formed on-chain using a construction called Hashed Timelock Contracts (HTLC). Later several payments can take place in a payment channel. The main advantage of payment channels is that one can send and receive thousands of payments with essentially only 2 on-chain transations: the opening and closing channel transactions.

Using these payment channels as building blocks one might establish a payment channel network, where it is not necessary to have direct payment channels between nodes to transact with each other, but they could simply route their payments through other nodes' payment channels. Such a network can be built, because LN achieves payments to be made without any counterparty risk, however efficient and privacy-preserving payment routing remains a challenging algorithmic task [4].

Our contributions. We empirically measure and describe LN's topology and show that it is utterly centralized and fragile against both random failures and targeted attacks. These findings suggest that LN, unlike Bitcoin, is far from being reliable, censorship-resistant, decentralized and private.

2 Lightning Network's Topology

LN can be described as a weighted graph $G = (V, E)$, where V is the set of LN nodes and E is the set of bidirectional payment channels between these nodes. We took a snapshot[1] of LN's topology

[1] https://graph.lndexplorer.com

on the 10th birthday of Bitcoin, 2019 January 3rd. In the following we are going to analyze this dataset.

LN gradually increased adoption and attraction throughout 2018, which resulted in 3 independent client implementations and 2344 nodes joining LN as of 2019, January 3rd. The density of a graph is defined as $D = \frac{2|E|}{|V||V-1|}$ which is the ratio of present and potential edges. As it is shown in Figure 1. LN is quite a parse graph. This is further justified by the fact that LN has 530 bridges, edges which deletion increases the number of connected components. Although LN is consisted of 2 components, the second component has only 3 nodes. The low transitivity, fraction of present and possible triangles in the graph, highlights the sparseness of LN as well.

Number of nodes	2344
Number of payment channels	16617
Connected components	2
Density	0.00605
Total BTC held in LN	543.61855₿
s-metric	0.6878
Maximal independent set	1564
Bridges	530
Diameter	6
Radius	3
Transitivity	0.1046
Average clustering coefficient	0.304
Degree assortativity	-0.2690

Figure 1: LN at a glance: basic properties of the LN graph.

However LN also exhibits somewhat scale-free properties as the s-metric suggests. S-metric was first introduced by Lun Li et al. in [1] and defined as $s(G) = \sum_{(u,v)\in E} deg(u)deg(v)$. The closer to 1 s-metric of G is, the more scale-free the network. Diameter and radius of LN suggests that LN is a small world. Somewhat scale-freeness is also exhibited in the degree distribution of LN. Majority of nodes have very few payment channels, although there are a few hubs who have significantly more connections as it can be seen in Figure ??.

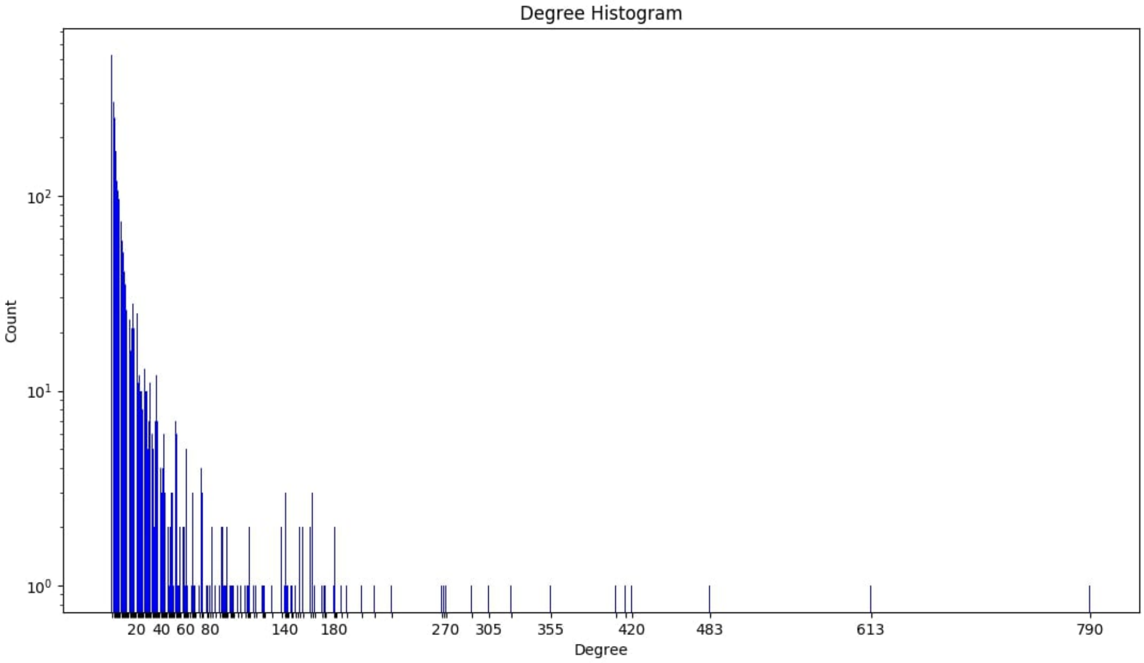

Figure 2: LN's degree distribution

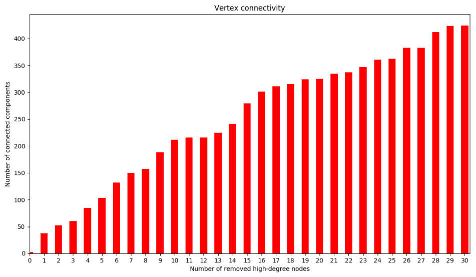

Figure 3: LN's vertex connectivity

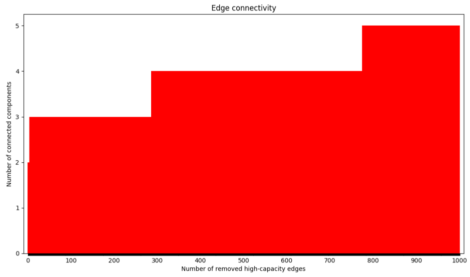

Figure 4: LN's edge connectivity

3 Robustness of LN

3.1 Random Failures

3.2 Targeted attacks

3.3 Fixing LN's resilience against attacks

percolation threshold

4 Privacy

topological anomalies have privacy implications, low usage of tor, even tor can not help

5 Conclusion

6 Acknowledgements

References

[1] Lun Li, David Alderson, John C Doyle, and Walter Willinger. Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4):431–523, 2005.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. *See https://lightning. network/lightning-network-paper. pdf*, 2016.

[4] Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate, and Ian Goldberg. Settling payments fast and private: Efficient decentralized routing for path-based transactions. *arXiv preprint arXiv:1709.05748*, 2017.