European Journal of Computer Science and Information Technology, 13(45)130-140, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Assessing the Topological Vulnerabilities of Bitcoin's Lightning Network: Robustness Against Random Failures and Targeted Attacks

Kavya Pathuri
Independent Researcher, USA

doi: https://doi.org/10.37745/ejcsit.2013/vol13n45130140 Published June 26, 2025

Citation: Pathuri K. (2025) Assessing the Topological Vulnerabilities of Bitcoin's Lightning Network: Robustness Against Random Failures and Targeted Attacks, *European Journal of Computer Science and Information Technology*, 13(45)130-140

Abstract: *The Bitcoin Lightning Network (LN) provides an innovative solution for scaling Bitcoin transactions by enabling off-chain payments with minimal fees and near-instantaneous settlement. LN's structure consists of interlinked payment channels, forming a decentralized network to facilitate efficient and secure transaction routing. This article investigates the topological characteristics of LN and examines its resilience to random and targeted disruptions. The Lightning Network can be modeled as a weighted, undirected graph to analyze various metrics such as clustering coefficients, degree distribution, and centrality. Results reveal that LN exhibits scale-free properties, contributing to robustness against random node failures. However, the network's reliance on high-degree nodes also makes it vulnerable to targeted attacks, which can fragment the network and impair transaction routing. These insights highlight the need for network design optimizations to enhance LN's security and scalability. Future considerations could focus on strategic topology adjustments to fortify LN against adversarial threats, ensuring more reliable off-chain transaction capabilities.*

Keywords: lightning network, bitcoin, network topology, scale-free networks, robustness analysis

INTRODUCTION

Bitcoin [1], the world's previously decentralized digital money, has upset the worldwide financial and technological scene since its inception in 2008. Denoting its tenth commemoration, Bitcoin keeps encapsulating the standards of decentralization, straightforwardness, and restriction opposition. Its creative utilization of blockchain innovation has made it one of the most noticeable and compelling improvements of the 21st century. Bitcoin has gathered huge notoriety throughout the long term, drawing in people, organizations, and states, the same, due to its freely irrefutable, permissionless, and trustless nature. Be that as it may, this uncommon reception has likewise uncovered a few basic restrictions, especially regarding flexibility and exchange effectiveness.

The inherent scalability constraints of the Bitcoin network have become a significant barrier to its widespread adoption as a mainstream payment system. In its current form, the Bitcoin blockchain can process approximately 7 transactions per second (tps). Contrastingly, centralized payment processors like Visa and Mastercard can handle upwards of 40,000 tps during peak periods. This vast difference highlights the challenges faced by Bitcoin in competing with traditional payment systems for real-world, high-throughput use cases. Additionally, users often face obstacles such as high transaction fees and prolonged confirmation times. For a transaction to achieve a healthy level of security, users must wait to include at least six new blocks in the blockchain, resulting in delays that can span several minutes, making Bitcoin impractical for many time-sensitive applications.

Addressing these constraints is essential for Bitcoin to realize its vision of becoming a truly global, peer-to-peer electronic cash system. To mitigate the scalability bottlenecks, the Lightning Network (LN) was proposed in 2016 [2] and officially launched in January 2018. LN is a second-layer protocol that operates on top of the Bitcoin blockchain, enabling faster and more cost-effective transactions while preserving the security and decentralization of the underlying network. LN achieves this by facilitating off-chain transactions that don't require immediate inclusion in the blockchain, thus alleviating the congestion and throughput limits of the primary Bitcoin layer.
The central idea of LN revolves around bidirectional installment channels, which are developed utilizing a cryptographic instrument known as Hashed Timelock Agreements (HTLCs). These channels permit members to interact with each other off-chain, with just two on-chain exchanges required: one to open the channel and one more to close it. This plan decisively lessens the number of exchanges recorded on the blockchain, bringing down exchange costs and expanding handling proficiency. Members can execute many exchanges inside the channel without causing extra charges or delays when setting up an installment channel.

Building upon this foundation, LN facilitates the creation of a decentralized payment channel network. In such a network, two nodes don't need to share a direct payment channel to transact. Instead, payments can be routed through a series of interconnected channels, enabling seamless transactions between any two nodes in the network. This routing mechanism enhances scalability and adaptability, allowing LN to support a much larger volume of transactions than the base Bitcoin network. Importantly, LN ensures that payments are processed without introducing counterparty risk, maintaining the trustless principles of blockchain technology. However, despite these advantages, developing efficient, scalable, and privacy-preserving payment routing algorithms remains an open challenge [3].

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

Property	Value
Number of nodes	2344
Number of payment channels	16617
Average degree	7.0891
Connected components	2
Density	0.00605
Total BTC held in LN	543.61855B
s-metric	0.6878
Maximal independent set	1564
Bridges	530
Diameter	6
Radius	3
Mean shortest path	2.80623
Transitivity	0.1046
Average clustering coefficient	0.304
Degree assortativity	−0.2690

The Lightning Organization isn't just a specialized development but also a likely impetus for more widespread Bitcoin adoption. By empowering instant and minimal-cost microtransactions, LN opens the way for new use cases, like micropayments, streaming installments, and cross-line settlements. Notwithstanding, its prosperity relies upon addressing a few basic difficulties, including network dependability, installment steering productivity, and protection from assaults.

Contributions

This paper presents a comprehensive empirical observation of the Lightning Network's topology. Specifically, it examines the structural properties, robustness, and strength under various scenarios, including random failures and targeted attacks. The results provide valuable insights into the strengths and vulnerabilities of the network, highlighting areas where its design can be improved to unlock its full potential. Furthermore, the document proposes actionable recommendations for enhancing the network's resilience, efficiency, and security. By shedding light on these aspects, this information aims to contribute to the ongoing development of LN as a critical component of the Bitcoin ecosystem.

Lightning Organization's Topology

The Lightning Organization (LN) can be officially addressed as a weighted, undirected diagram G = (V, E), where V represents the arrangement of hubs and E represents the arrangement of bidirectional connection channels between these hubs. Each edge in the diagram has a related weight, not entirely set in stone by the installment channel's ability. The organization's geography, in this manner, straightforwardly impacts its proficiency, adaptability, and power. Understanding these properties is vital for assessing LN's capacity to help a developing number of clients and exchanges.

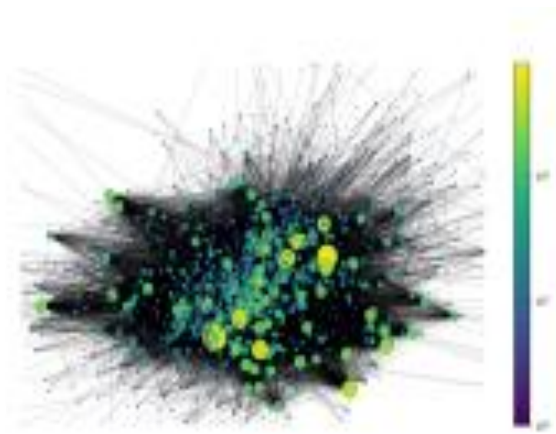

Fig. 1: LN's topology. Nodes with higher degrees are highlighted with lighter colors and larger circles.

A snapshot of LN's geography taken on Bitcoin's tenth commemoration, January 3, 2019, was utilized for this observation. This depiction incorporates 2344 hubs and many edges addressing dynamic installment channels. While the organization's geography is dynamic, continually developing as new hubs and channels are added or taken out, observations across different depictions indicate that the basic topological properties, like thickness, normal degree, transitivity, and degree circulation, remain generally stable over the long term. These predictable attributes provide important information about the underlying underpinnings of LN. Future work could also investigate LN's geography's transient advancement and dynamic properties.

Graph Thickness and Sparsity

The thickness of a chart is a proportion of its edge-to-hub proportion and is given by D =2|E||V |(|V |−1) , where |E| is the complete number of edges, and |V | is the total number of hubs. As displayed in Figure 1, LN shows low thickness, affirming that it is a scanty diagram. The presence of 530 span edges additionally features this sparsity, the evacuation of which would build the quantity of associated parts. Notwithstanding this, LN remains largely associated, comprising just two significant parts, with the subsequent part comprising only three hubs.

Another sign of sparsity is the organization's transitivity, characterized as the proportion of existing triangles (three-hub coteries) to all potential triangles in the diagram. LN's low transitivity shows that most hubs in the organization don't frame thickly associated clusters, which is a sign of meager geographies.

Degree Appropriation and Center Point Spoke Structure

One of the characterizing elements of LN's geography is its negative degree assortativity, which shows that low-degree hubs will generally associate with high-degree hubs instead of other low-degree hubs [4]. This disassortative blending design recommends that LN follows a center point and talks engineering, where a couple of profoundly associated "center" hubs rule the organization. In contrast, most of the hubs have a couple of associations. This perception is additionally upheld by the degree dispersion displayed in Figure 4, where most hubs have a low degree, yet few hubs show excessively high degrees.

The typical briefest way length of LN, determined as 2.80623 (overlooking channel limits), recommends that installments can generally be directed across the organization with a couple of bounces. However, this effortlessness is confounded by the need to represent channel limits during installation steering, making the genuine directing issue non-pantry.

Centrality Measures and Special Attachment

When new hubs join LN, they should conclude which existing hubs to interface with. In the "lnd" execution, one of the essential objectives for new hubs is to advance their centrality by associating with profoundly focal hubs. This technique cultivates a particular connection design, where new associations are bound to frame with currently highly associated hubs, supporting the center point talked structure. Different executions, for example, c-lightning and eclair, depend on clients physically making channels. This frequently brings about comparable behavior, as clients normally like to interface with deep-rooted centers.

Two key centrality measures further provide insight into LN's geography: betweenness centrality and closeness centrality. The betweenness centrality of a hub v, characterized as *g(v) = Ps≠v≠tσst(v)σst*, measures the degree to which v lies on the briefest ways between different hubs. Hubs with high betweenness centrality frequently act as basic mediators in the organization. Closeness centrality, characterized as CC(u) = PNu≠v d(u,v), measures how close a hub is to any remaining hubs in the organization. Hubs with high closeness centrality are normally more productive in dispersing data or installments.

Small-World Properties and Clustering

LN displays little world properties, described by high bunching coefficients and short normal way lengths [5]. The nearby grouping coefficient of a hub u, characterized as *C(u) = 2|{(v,w):v,w∈N(u)∧(v,w)∈E}| deg(u)(deg(u)−1)*, measures the degree to which u's neighbors structure a total subgraph. The circulation of neighborhood grouping coefficients in LN uncovers a particular construction: an exceptionally associated center of hubs encompassed by a scantily associated outskirts. This focal faction is the organization's foundation, supporting productive steering and strength. At the same time, the approximately associated external hubs take special care of edge cases and specialty use cases.

Subsectionscale Attributes and S-Metric Analysis. LN's certificate circulation proposes that it might display without scale properties. The s-metric, presented in [6], gives a quantitative proportion of scale-freeness and is characterized as *s(G) = P(u,v)∈E deg(u)deg(v)*. A high s-metric worth, drawing nearer 1, demonstrates a more sans scale organization. For LN, the s-metric affirms its propensity toward sans scale conduct.We applied the greatest probability assessment technique from [7] to approve this perception to fit a power-regulation conveyance to the observational degree information. The best-fit power-regulation example was viewed as $\gamma = -2.1387$, with a Kolmogorov-Smirnov test yielding a p-worth of $p = 0.8172$. This high p-esteem upholds the speculation that LN's certification dispersion follows a sans scale model.

Implications for Organization Strength and Future Work

The center point talked about design and the little world proper ties of LN have critical ramifications for its strength and effectiveness. While the focal centers upgrade availability and lessen steering intricacy, they address potential weak spots or attacks. Understanding these compromises is basic for planning a stronger and versatile organization. Future work should focus on powerful parts of LN, for example, how its geography develops after some time, and the effect of client conduct on network proficiency and security.

Fig. 2: Local clustering coefficient of LN

Robustness of LN

The heartiness of an organization is a basic inquiry in network science. LN, like Bitcoin, is a permissionless and dynamic organization where hubs can join, leave, or change their channels whenever. This unique nature raises basic worries about its flexibility against arbitrary disappointments and purposeful assaults. Notwithstanding this ease, the Lightning Organization displays momentous dependability in its topological attributes. In this part, we discuss LN's power and research its capacity to endure irregular hub disappointments and designated assaults.
Estimating the vigor of an organization includes methodically eliminating hubs or potentially edges from the diagram and seeing how the organization pieces into detached parts. A basic measurement utilized in this setting is the permeation edge, signified as fc, which addresses the negligible portion of hubs that should be eliminated for the monster part to break down into more modest separated parts. For genuine organizations, the permeation limit is often assessed by the place where the size of the goliath part falls beneath 1% of its unique size [8].

Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

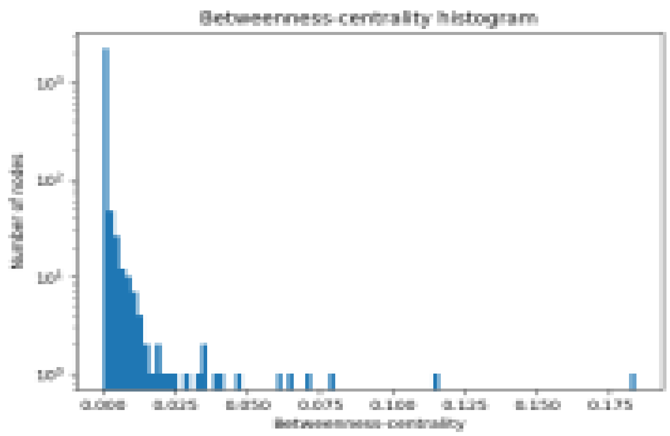

Fig. 3: LN's betweenness centrality

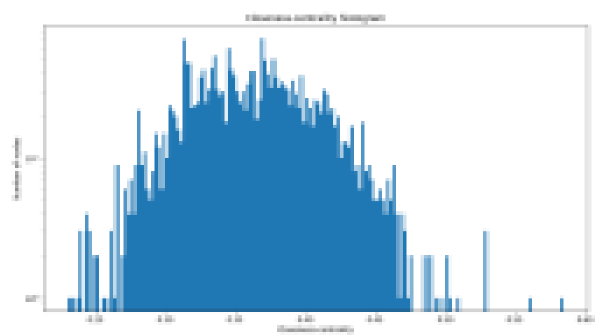
Fig. 4: LN's closeness centrality

Random Failures

Irregular disappointments address a sensible disappointment mode in LN. Hubs might go disconnected because of unfortunate organizational availability, equipment failures, or other reasons, successfully eliminating them and their related edges from the organization. For sans scale networks with degree circulation $Pk = k^{-\gamma}$, where $2 < \gamma < 3$, the Molloy-Reed models can determine the permeation limit. In particular, it is given by: fc = 1 −1γ−2 3−γ kγ−2min k3−γmax − 1, where kmin and kmax are the base and most extreme hub degrees, separately. Applying this recipe to LN under irregular disappointments yields $f_c = 0.9797$, which adjusts intimately with recreation results (see Table 2). This high permeation limit shows that LN exhibits critical strength against irregular disappointments. This flexibility originates from LN's without scale geography, where most of the hubs have low availability and are hence less basic to the organization's general construction. Irregular hub evacuation is subsequently far-fetched to disturb the organization's monster part's availability, as outlined by the degree dispersion in Figure 5.

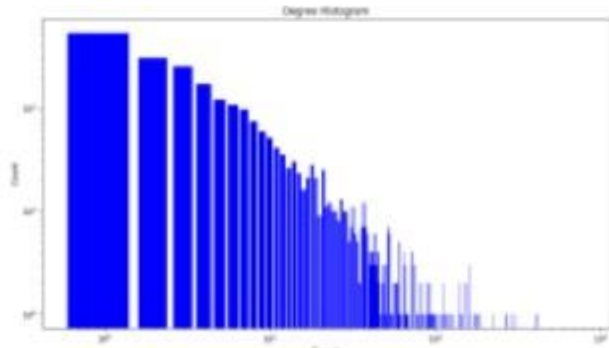

Fig 5: LN's degree distribution

Network	f_c
Internet	0.92
WWW	0.88
US Power Grid	0.61
Mobil Phone Call	0.78
Science collaboration	0.92
E. Coli Metabolism	0.96
Yeast Protein Interactions	0.88
LN	0.96

Fig 6: Random failures in networks. Values of critical thresholds for other real networks are taken from [8].

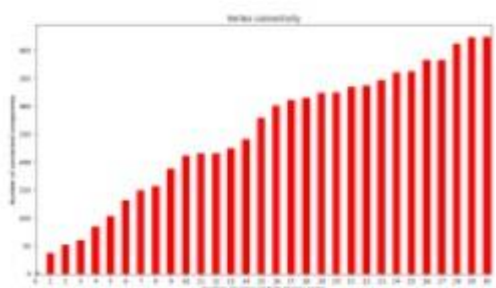

Fig 7: LN's vertex connectivity when all the 30 largest hubs are removed one by one.

Targeted Attacks

Unlike irregular disappointments, designated assaults represent a huge danger to LN. The expulsion of serious-level hubs or hubs with high betweenness centrality can seriously affect network availability. LN's experiences have shown this. For example, on Walk 21, 2018, a Conveyed Refusal of Administration (DDoS) assault cut down 20% of LN hubs [?].

In our most memorable assault situation, we recreated the evacuation of the 30 most significant level hubs individually, recalculating the organization's associated parts after every expulsion. The outcomes, displayed in Figure 8, uncover that eliminating even the single most significant level hub sections the LN diagram into 37 associated parts. Eliminating all 30 biggest centers results in 424 parts, a large portion of which are disconnected vertices. This extreme discontinuity is principally because of LN's disassortative nature, where center points are bound to be associated with fringe hubs as opposed to different centers.

We likewise examined the effect of eliminating hubs in light of their betweenness centrality, a proportion of a hub's significance in working with communication between different hubs. In this situation, we recalculated betweenness centrality after every hub evacuation to guarantee the greatest effect. We saw that the permeation edge was lower for betweenness-based assaults (fc = 0.1409) compared with degree-based assaults (fc = 0.1627), as displayed in Figure 11. This shows that focusing on high-betweenness hubs is a more compelling system for network disturbance.

Hub blackouts additionally influence the normal most limited way lengths. While irregular hub disappointments insignificantly affect way lengths, designated assaults against center points increment the distance between residual hubs. The expulsion of serious level hubs decreases accessible liquidity and expands the number of bounces expected for installment steering, as outlined in Figure 10. This could prompt a higher disappointment rate for installments because of longer and more complicated courses.

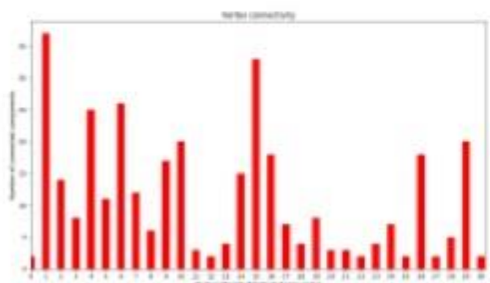

Fig 8: LN's vertex connectivity if only one high-degree node is removed from the graph.

Network	f_c
Internet	0.16
WWW	0.12
Facebook	0.28
Euroroad	0.59
US Power Grid	0.20
Mobil Phone Call	0.20
Science collaboration	0.27
E. Coli Metabolism	0.49
Yeast Protein Interactions	0.16
LN	0.14

Fig 9: Real networks under targeted attacks. Values of critical thresholds for other real networks are taken from [8] and [9].

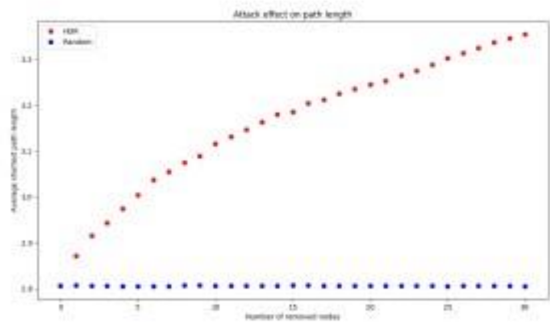

Fig 10: High degree removal (HDR) attack effects average shortest path lengths.

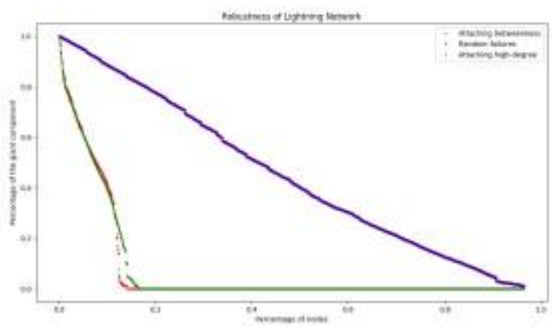

Fig 11: Percolation thresholds for various attack scenarios: fHDRc = 0.1627, fHBRc = 0.1409, fRNDc = 0.9645.

Enhancing LN's Resilience

Planning networks that are robust against irregular failures and designated assaults is a difficult enhancement issue [8]. For instance, a star geography is exceptionally versatile to irregular failures, as removing fringe hubs doesn't influence the focal point. Nonetheless, a similar geography is helpless against designated assaults on the focal point.

To improve LN's flexibility, systems from past explorations on vigor advancement [10] could be adjusted. These methodologies balance vigor and availability by decisively changing the organization's geography. Although a point-by-point observational assessment of these techniques with regard to LN is beyond the scope of this paper, future work could investigate their execution in LN client programming.

One more way to deal with improve LN's vigor is to increment network among fringe hubs. Current LN executions urge new hubs to interface principally to all around associated centers. All things considered, client programming could command associations with a blend of centers and haphazardly chose fringe hubs. This technique would make elective pathways and lessen the organization's dependence on center points, subsequently working on its flexibility to counterattacks.

All in all, while LN shows impressive heartiness to arbitrary disappointments because of its small-scale nature, it stays helpless against designated assaults on serious levels and high-betweenness hubs. By adopting techniques to increment fringe availability and upgrading the organization's geography, LN's strength against both disappointment modes can be improved.

CONCLUSION

Understanding and observing the fundamental organization geography is essential for improving the power of mind-bending frameworks, for example, the Lightning Organization (LN). The versatility of an organization is intrinsically attached to its primary properties, and LN's geography, which intently aligns with the sans scale model, shows qualities that direct its conduct under various disappointment and assault situations. The article reaffirms that LN is strikingly strong against irregular hub disappointments, a characteristic common to many small-scale organizations. This strength originates from the exceptionally heterogeneous degree of circulation, where an enormous number of low-degree hubs contribute negligibly to the general availability, guaranteeing that irregular disappointments limited affect the organization's uprightness.

Nonetheless, this vigor comes at the expense of an increased weakness to designated assaults. The purposeful expulsion of serious-level hubs or those with high centrality measurements can bring about critical fracture, decreasing the organization's viability and possibly risking its functional dependability. It is essential to take note of that significant level visual portrayals of LN's geography, like Figure 2, can frequently give an excessively hopeful impression of the organization's power and security. While such portrayals grandstand the interconnectedness and dynamism of the organization, they neglect to catch the innate primary shortcomings that objective enemies could take advantage of. As exhibited in this article, LN's vulnerability to designated assaults highlights the requirement for stronger plans in Layer-2 blockchain arrangements.

To address these weaknesses, future endeavors should focus on improving organization geographies that balance adaptability, execution, and versatility. Methodologies for improving LN's vigor might incorporate cultivating more noteworthy availability among fringe hubs, enhancing association inclinations to lessen reliance on center points, and consolidating improvement strategies that reinforce the organization's resilience to arbitrary disappointments and designated assaults. Such upgrades could draw motivation from existing work on strength advancement and could be carried out at the convention or programming level to guarantee versatility without compromising security.

All in all, while LN addresses a huge progression in working with off-chain exchanges and scaling blockchain networks, its drawn out progress relies upon tending to its underlying shortcomings. Vigorous Layer-2 arrangements like LN and Raiden require a comprehensive way to deal with network configuration, underscoring strength to ill-disposed conduct and unexpected disappointments. By zeroing in on these perspectives, the blockchain local area can assemble safer, stable, and dependable foundations, preparing for boundless reception and confidence in decentralized advances.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. https://bitcoin.org/bitcoin.pdf
[2] J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments,” 2016. https://lightning.network/lightning-network-paper.pdf
[3] S. Roos, P. Moreno-Sanchez, A. Kate, and I. Goldberg, “Settling payments fast and private: Efficient decentralized routing for path-based transactions,” 2017. https://arxiv.org/pdf/1709.05748
[4] M. E. J. Newman, “Assortative mixing in networks,” arxiv, 2002. https://arxiv.org/pdf/cond-mat/0205405
[5] Duncan J. Watts & Steven H. Strogatz, “Collective dynamics of ‘small-world’ networks,” Nature, vol. 393, no. 6684, p. 440, 1998. https://www.nature.com/articles/30918
[6] Lun Li, David Alderson, Reiko Tanaka, John C. Doyle, and Walter Willinger, “Towards a Theory of Scale-Free

Graphs: Definition, Properties, and Implications (Extended Version)," *Internet Mathematics*, vol. 2, no. 4, pp. 431–523, 2006. https://doyle.caltech.edu/images/doyle/f/fc/IM06.pdf

[7] A. Clauset, C. R. Shalizi, and M. E. Newman, "Power-law distributions in empirical data," *SIAM Review*, vol. 51, no. 4, pp. 661–703, 2009. https://pdodds.w3.uvm.edu/files/papers/others/2009/clauset2009b.pdf

[8] A.-L. Barab´asi *et al.*, "Network science, " Cambridge University Press, 2016. https://assets.cambridge.org/97811070/76266/frontmatter/9781107076266_frontmatter.pdf

[9] Y. Lin, W. Chen, and Z. Zhang, "Assessing percolation threshold based on high-order non-backtracking matrices," in Proceedings of the 26th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, 2017, pp. 223–232. https://www.microsoft.com/en-us/research/wp-content/uploads/2017/02/www17_percolation.pdf

[10] B. Shargel, H. Sayama, I. R. Epstein, and Y. Bar-Yam, "Optimization of robustness and connectivity in complex networks," *Physical Review Letters*, vol. 90, no. 6, p. 068701, 2003. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.90.068701