Abstract—XRP is one of the oldest, well-established cryptocurrencies. Despite the popularity of XRP, little is known about its underlying peer-to-peer network. The structural properties of a network impact its efficiency, security and robustness. We aim to close the knowledge gap by providing a detailed analysis of the XRP overlay network.

In this paper we examine the graph-theoretic properties of the XRP Network topology and its temporal characteristics. We crawl the XRP Network over two months and collect 1,300 unique network snapshots. We uncover a small group of nodes that act as a networking backbone. In addition, we observe a high network churn, with a third of the nodes changing every five days. Our findings have strong implications for the resilience and safety of the XRP Ledger.

Index Terms—Blockchain, XRP, Network Topology Analysis, Measurement

I. INTRODUCTION

XRP is one of the oldest, well-established cryptocurrencies. In 2022 it ranked seventh by market capitalization. The XRP Ledger is a decentralized peer-to-peer overlay network of nodes running the rippled software.

The goal of XRP is to provide high transaction throughput whilst maintaining security against Byzantine failures. The XRP Ledger Consensus Protocol is a type of Federated Byzantine Agreement protocol [1], in which each participant selects a Unique Node List (UNL) of validators. These validators are not necessarily trusted individually but are believed not to collude as a whole. As long as there is a minimum overlap between UNLs, the XRP Ledger will remain consistent [2].

The structure of the peer-to-peer overlay network of a blockchain affects its security, resilience, and efficiency. A corpus of research focuses on the study of structural properties of Bitcoin [3], [4] and Ethereum [5]–[7]. To the best of our knowledge, there are no works examining the overlay network of XRP.

In addition, by design [8], there are no direct incentives to run rippled software. Those who participate do so because they are interested in the long-term health and decentralisation of XRP.

The network is uniquely suited for study. Unlike other blockchains that focus on hiding their topology, XRP has native support for network crawling [9]. The public availability of data enables researchers to determine the network’s accurate topology.

In this paper, we present the results of a graph-theoretic analysis of the XRP peer-to-peer overlay network. We discuss the properties of an individual network snapshot and study its evolution over time. We use different metrics to identify a cluster of authoritative nodes in the peer-to-peer network.

The remainder of this paper is structured as follows. We discuss related work in Section II. In Section III we introduce the relevant aspects of the XRP network. We outline the data collection methodology in Section IV. We describe our findings in Section V. Finally, we discuss and conclude our work in Section VI.

II. RELATED WORK

We discovered a significant corpus dedicated to studying cryptocurrency networks, predominantly Bitcoin and Ethereum. We provide a summary of these works in this Section.

Miller et al. [3] were one of the first to determine the topology of the Bitcoin network. The authors discovered "extremely high-degree nodes", which persist in the network over time. Furthermore, the Bitcoin network is not purely random. Delgado-Segura et al. [4] inferred the topology of Bitcoin using orphaned transactions. Due to the limitations of their method, they performed measurements only in the Bitcoin testnet. Their results indicate that the testnet is not a random graph.

Paphitis et.al. [7] conducted a graph-theoretic analysis of several different blockchain overlay networks. The results indicate that blockchain overlays have varying network properties and degree distributions. Despite the significant variance, there is a strong correlation between the node’s session length and the degree. In addition, the networks have small average shortest paths, but they are not small-world. Finally, the overlay networks are resilient to random node failures, but targeted attacks can considerably affect their connectivity.

Similar studies focus on the Ethereum network. Zhao et al. [6] performed a temporal, evolutionary analysis of the Ethereum blockchain interaction networks. The authors found a link between anomalies in the structural properties and real-life events. Furthermore, they discovered that the network grows following a preferential attachment model.

In a later study, Gao et al. [5] conducted a graph-theoretic analysis of the peer-to-peer layer of the Ethereum network. They discovered an abundance of nodes that do not contribute
to the Ethereum network. Furthermore, they showed that the degree distribution does not follow a power-law. In contradic-
tion to the work of Paphitis et al., the authors found evidence of small-world property.

The majority of research conducted in the context of XRP is about the XRP Ledger Consensus Protocol. Chase et al. [10] provide a detailed description and analysis of the Consensus Protocol. They demonstrate that at least a 90% overlap of the UNLs is required to ensure network safety. In a later study, Christodoulou et al. [11] show, when fewer than 20% of nodes are malicious, the overlap of UNLs can be relaxed. Otherwise, an overlap of 90-99% is required. In a similar study, Amores-Sesar et al. [12] demonstrate that, in the presence of Byzantine nodes, the ledger may fork under standard UNL overlap requirements. Furthermore, the authors show that a single Byzantine node may cause consensus protocol to lose liveliness.

In a different line of research, Roma et al. [13] studied the energy efficiency of an XRP validator. They found that the annual validator running cost is significantly lower than that of a miner.

Aoyama [14] provides a unique view of the XRP network from the perspective of its transactions. They found a clear divide between groups accepting transactions and groups receiving transactions.

To the best of our knowledge, we are not aware of previous studies about the topological properties of the XRP network. With this work, we aim to close this gap.

### III. BACKGROUND

The XRP Payment Network consists of nodes running the rippled [15] software. The interconnected rippled servers form the decentralized peer-to-peer overlay network.

The node owners configure it to accept some number of inbound and outbound connections. Each outgoing connection corresponds to an incoming connection at another node. When nodes connect, the communication over the link is bidirectional. We, therefore, represent the overlay network as a directed graph. The direction of an edge identifies the node that initiated the connection.

A node gets initial entry into the overlay network by connecting to several hardcoded bootstrapping hubs. These hubs share the addresses of other nodes with available inbound connections. The node continues to establish links to others until it reaches the desired limit of outgoing connections. When a node has reached its maximum number of inbound links, it rejects further connection attempts.

A node periodically advertises to its peers when it has open inbound connection slots. Nodes store this information and communicate it with their peers. As a result, available incoming connections propagate throughout the network.

### IV. METHODOLOGY

We used the XRP Ledger Crawler [16] to discover the nodes in the overlay network. The crawler is maintained by RippleX - the open-source development community from Ripple. The crawler starts by querying the peers of a single XRP server. It adds the new nodes to a list and calls every node with a listed IP address. The crawler repeats this process until it no longer discovers new nodes. We performed the network crawls at one-hour intervals, in keeping with other analysis.

We crawled the XRP Network for two months (05/01/2022 - 01/03/2022). In the end, we collected 1,290 snapshots. We made the datasets available online for further research [17].

### V. NETWORK ANALYSIS

We summarise the basic properties of the XRP network in Table 1. The network is relatively small. We observed 948 nodes and 15,010 on average. In comparison, Bitcoin has 50,000 nodes and Ethereum of 12,000 nodes [7]. We measured a fluctuation of 2% in the total node count and 1% in the edge count.

Each outgoing connection corresponds to an incoming one, and the nodes report only the active links (not the potential ones). Therefore, the means of incoming and outgoing degrees are equal. However, we observe a high standard deviation in the collected node degree values. It suggests that the low node variance had a non-negligible effect on the degree distribution.

The network is consistently connected, as indicated by the single connected component. However, this may also be due to the nature of the crawler. The crawler can only discover the nodes that are members of the same connected component as the initial entry node. Any node not connected to the core would not be able to participate in the Ledger.

Network Density is the proportion of the possible and actual connections in the network. The XRP network has a density of 0.03. In comparison, the density of Bitcoin and Ethereum are 0.002 and 0.0006, respectively [7].

Clustering Coefficient quantifies nodes tendency to form tightly knit groups characterised by relatively high density of ties. The low average shortest path and high clustering coefficient of XRP Network imply that it may exhibit the small-world property.

|        | Mean  | STD  |
|--------|-------|------|
| Nodes  | 948.53| 18.54|
| Edges  | 15010.26 | 508.92 |
| In-Degree | 15.82 | 45.62 |
| Out-Degree | 15.82 | 19.94 |
| Connected Component | 1 | 0.00 |
| Assortativity | -0.48 | 0.02 |
| Global Clustering Coefficient | 0.76 | 0.02 |
| Density | 0.03 | 0.00 |
| Avg. Shortest Path | 2.31 | 0.03 |
| Diameter | 5.1 | 0.33 |

**TABLE 1:** Basic XRP network properties.

#### A. Single Network

We conducted an in-depth analysis of a single XRP network snapshot. We selected an overlay whose node and edge counts are the closest to the mean of the dataset. In the remainder of this Section, we will discuss our findings.

1We used r.ripple.com as the starting node
1) Degree Distribution: The network degree distribution impacts many of its properties, such as message propagation delay and the resilience of the network [18]. Furthermore, random networks have binomial degree distributions, whereas real-world networks contain a small number of highly connected nodes that cannot be accounted for by random models [19].

In Figure 1a we illustrate the incoming and outgoing connection distribution among the nodes. We split the outgoing connections into two groups. The first group, indicated by the exponential portion of the curve, holds nodes whose out-degree is above the mean. It contains 15% of the nodes that account for 50% of all connections. The second group, indicated by the linear portion of the curve, holds the remaining 85% of the nodes. Finally, a deeper inspection revealed two outlier nodes with over 150 outgoing connections.

We similarly grouped the incoming connections. The first group, indicated by the sharp spike of the curve, dominates the overall network connectivity. It contains 11% of nodes with an in-degree above the mean. These nodes account for 85% of incoming connections. The second group, depicted by the short linear portion of the curve, contains 27% of nodes. They account for 15% of the incoming links. The final group, reflected by the plateau, holds nodes without incoming connections and accounts for the remaining 62% of nodes.

The incoming and outgoing connection distributions are heavy-tailed. However, they seem to have different shapes. We discuss which model best describes these distributions in the next Section. We also observe that a small subset of nodes holds the majority of connections. Our findings suggest that the network has a group of authoritative nodes.

2) Scale-Free Property: Across scientific domains, it is often claimed that real-world networks are scale-free. Details vary, but in general, a network is scale-free, when nodes with degree $k$ follow a power-law distribution $k^{-\alpha}$, where $\alpha$ is the scaling criterion $\alpha > 1$. However, other versions of this hypothesis have stronger restrictions, e.g. $2 < \alpha < 3$ [18]. Cohen et al. show that scale-free networks are highly resilient to random attacks but are vulnerable to targeted attacks [20]. Therefore, it is important to understand the type of degree distribution.

We used the fitter [21] Python library to find the most accurate model. We used the Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC) to determine the quality of a fit. A lower AIC or BIC value indicates a better fit. The analysis in Section V-A1 revealed that the in and out degrees are likely to have different distributions. Therefore we modelled the in, the out, and the combined distributions separately. We found that the in-degree distribution was best captured by the power-law distribution, with $\alpha \approx 1.2$. On the other hand, the out-degree was best described by the generalized normal distribution, with a heavy, long tail. Likewise, the overall degree distribution was also best described by the generalized normal distribution.

The ubiquity of scale-free networks in the real world has been questioned [19]. Therefore, we avoid claiming that the XRP network is scale-free, as a deeper analysis is required. However, our findings indicate that the XRP network is not random. Furthermore, the power-law distribution fit of the in-degree offers further evidence that the network relies on a subset of nodes for its connectivity.

3) Small-World Property: The well-studied small-world property indicates that a short path connects any two nodes in the network [18]. An average shortest path $l$ is considered to be short when $l \approx \frac{\ln N}{\ln(k)}$, where $N$ is the size of the network, and $\langle k \rangle$ is the average degree.

The effect was initially formalized by Manfred Kochen and Ithiel de Sola Pool [22] and later popularized by the well-known Milgram experiment that inspired the six degrees of separation phrase.

Network G is said to be small-world if it has a similar average shortest path length but a greater clustering coefficient than an equivalent random graph. Two graphs are equivalent when they have an equal number of nodes. Let $L_G$ be the mean shortest path length of $G$ and $C_G$ its clustering coefficient. Equivalent properties for a random graph are $L_{rand}$ and $C_{rand}$. [18]
Network G is said to be small-world if $L_g \geq L_{rand}$ and $C_g >> C_{rand}$.

A quantitative measure of small-worldness is expressed as follows: $\gamma_g = \frac{C_g}{C_{rand}}$ and $\lambda_g = \frac{\lambda_g}{\lambda_{rand}}$, where $\gamma_g$ is the clustering coefficient ratio and $\lambda_g$ is the average shortest path ratio of network G and an equivalent random graph. Then measure of small-worldness is expressed as $S = \frac{2\gamma_g}{\lambda_g}$. A network is considered small-world when $S > 1$ [23].

We used the Erdős–Rényi (ER) model to generate random graphs. To ensure the robustness of the small-worldness calculation, we used Monte Carlo sampling of 1000 equivalent ER graphs. We measured $S = 8.3$ for the XRP Network. We therefore conclude that the XRP network has the small-world property.

4) In/Out Degree Analysis: Link analysis is a method to identify authoritative nodes in a network [24], [25]. We use it to identify selfish nodes that do not reciprocate the connections they establish by accepting incoming links.

We express the link ratio as $\lambda = \frac{I_{out+1}}{O_{out+1}}$. All degrees are incremented by 1 to account for no incoming or outgoing connections. A high ratio $\lambda > 1$ suggests that a node is altruistic - it establishes more incoming connections than outgoing ones. Conversely, $\lambda < 1$ indicates nodes that consume more connectivity than they provide.

We illustrate the ratio distribution in Figure 1b. We observe that 15% of nodes have $\lambda << 1$. Interestingly, we find that a significant percentage of nodes have a $\lambda = 0.1$. These are nodes that use the default rippled configuration, with ten outgoing and zero incoming connections. In contrast, only about 10% of nodes have more incoming than outgoing connections, and only 3% $\lambda >> 1$.

There are no direct incentives to participate in the XRP network. However, running a node that accepts incoming connections requires significant investment. Such a server has to be reliable and available. Therefore, we see that majorities of nodes connect to the network as consumers, and only relatively few behave altruistically. In the next section, we will discuss the preference of nodes to connect to other similar nodes.

5) Degree Correlation: The degree correlation captures the preference of nodes to form connections with others that are similar in some way [18]. In the context of this study, we consider similarity in terms of node degree. A network is assortative when nodes tend to connect to others with a similar degree. In a disassortative network, small-degree nodes prefer to link with high-degree nodes, and hubs tend to avoid each other. Finally, a network is considered neutral when the wiring between the nodes is random.

The degree correlation has an impact on the robustness of a network [26]. In an assortative network, node removal causes little fragmentation, as high-degree nodes form a core group and are redundant. In contrast, disassortative networks are easier to fragment. High-degree nodes connect to many small-degree nodes, which become disconnected once a high-degree node is removed.

Degree correlation coefficient $r$ characterizes degree correlation using a single number $r$ [27]. In general it varies between $-1 \leq r \leq 1$ [18]. For $r > 0$ the network is assortative, for $r = 0$ the network is neutral, and for $r < 0$ the network is disassortative. We compute the degree correlation coefficient and display it in Table I. The XRP network is disassortative. In comparison, the degree correlation of an equivalent ER network is zero. This reveals that XRP has a hub-and-spoke network structure, and may be vulnerable to targeted attacks.

B. Temporal Analysis

We summarise the network properties that appear to be stable over time. We observe that the preference of small-degree nodes to connect to high-degree nodes remains constant over time. Likewise, the global clustering coefficient and average shortest path are stable. Furthermore, all network snapshots have the small-world property. These findings suggest that there were no significant disruptions in the network during the observation period.

The relatively small change in the size of the network had a non-negligible effect on the average incoming and outgoing degree, as indicated by the standard deviation. We dedicate the rest of this section to discussing these changes.

1) Degree Distribution: We illustrate the complementary cumulative distribution function (CCDF) of the node degrees in Figure 2. Overall, both distributions have long tails, and their shapes remain stable. However, we see some variance over time in both figures, as indicated by the changing thickness of the plots.

We plot the CCDF of incoming connections in Figure 2a. Our first observation is that consistently 60% of nodes do not accept incoming connections. Likewise, we see little variance at the tail-end of the spectrum. We see slightly more variance in nodes close to the mean and nodes whose degree is in the range 250-300. We observe the largest variance in nodes with in-degree between 50-150. Our observations suggest that the nodes at the ends of the distribution are saturated. They cannot accept new peers. Therefore, nodes in the middle of the distribution handle the new connections to the network. Furthermore, the majority of new nodes do not accept incoming links.

We depicted the CCDF of the outgoing connections in Figure 2b. The long, thin tail of the distribution suggests the existence of a few stable nodes with a high number of outgoing connections. We see a much higher variance in the group of nodes with an out-degree between 50 and 100. Finally, the majority of new nodes had an out-degree under the mean.

During the data collection, two new versions of the rippled software were released. Some of the observed variances may be explained by nodes leaving the network to update their version. However, overall the network has a stable member group.

2) In/Out Degree Analysis: In Figure 3 we display the degree ratio plot for all captured snapshots. We observe little change in the overall degree ratio. The majority of nodes establish more outgoing than incoming connections. Only 10% of nodes establish more incoming than outgoing connections.
The lack of change in the shape of the curve confirms our initial observation that nodes do not reciprocate the connections they consume.

3) **Churn:** Over the collection period, we discovered 3,000 unique nodes. In Figure 4, we outline the lifespan of these nodes. The green, striped bar indicates nodes with the shortest lifespan. These nodes were present in around 5% of all network snapshots. On the other side of the plot, the blue crossed bar represents the most stable nodes. They were present in at least 95% of all the snapshots. The remaining 1/5th of the nodes have a gradually decreasing lifespan.

We further analysed the presence of the top 10% of the highest in-degree nodes in the network over time. The group of the first network snapshot contains 95 nodes. The last network snapshot group holds 98 nodes. However, 23 nodes or 24% from the first group are not present in the second group. Four nodes changed their IDs but had the old IP addresses and similar degree profiles. However, we did not find the other 19.

VI. **DISCUSSION & CONCLUSION**

A decentralized peer-to-peer overlay network forms the backbone of the XRP Ledger. In this paper, we provided an in-depth analysis of the graph-theoretic properties of this overlay.

We use a publicly available crawler to capture 1,290 snapshots of the underlying overlay network over two months. We find that it is significantly smaller than other blockchain overlay networks. The nodes are connected via short paths and are tightly clustered. Furthermore, the clusters tend to have a hub-and-spoke structure, as shown by the high assortativity of the network. Unlike other blockchain overlay networks, XRP has a small-world topology.

XRP does share some similarities with other blockchains. The network degree distribution has an exponential-like shape. We did not find conclusive evidence that it is scale-free. However, like other blockchains, the topology is not random.

Overall, the size of the network is consistent over time. However, we captured a significant amount of churn. Given these observations, we suspect that many nodes join the network to conduct their business and leave shortly.

The XRP overlay network may be vulnerable to targeted attacks. We discovered the existence of a small subset of influential nodes that provide the backbone of the network connectivity. Furthermore, a malicious actor can use the publicly available topology to identify these nodes.
We revealed a vast disparity between nodes that accept incoming connections and nodes that do not. Furthermore, link analysis showed that many nodes do not accept incoming connections. These nodes increase the dependence on the influential nodes. Thus, contributing to the network centralization. We suspect that a lack of financial incentive contributes to this behaviour, as there are significant costs associated with running a reliable node. Natural centralization is a common problem in decentralized peer-to-peer networks [28] [29]. A common solution is to introduce communal incentives or mandatory behaviour.

Our results raise further questions about the security and vulnerability of the XRP network. Research works [20] [30] show that networks with a long-tail degree distribution are susceptible to targeted attacks. For future work, we intend to evaluate the resilience of the XRP network to random and targeted attacks, and to identify mitigation strategies.

ACKNOWLEDGMENT
This work was supported by Ripple UBRI.

REFERENCES
[1] G. Antonio, F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. Airam, C. De Souza, O. Carlos, and M. B. Duarte, “Security and Performance Analysis of Quorum-based Blockchain Consensus Protocols.”
[2] I. Amores-Sesar, C. Cachin, and J. Mičić, “Security analysis of ripple consensus,” arXiv preprint arXiv:2011.14816, 2020.
[3] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, “Discovering bitcoin’s public topology and influential nodes,” et al, 2015.
[4] S. Delgado-Segura, S. Bakshi, C. Pérez-Solá, J. Litton, A. Pachulski, A. Miller, and B. Bhattacharjee, “Exprobe: Discovering bitcoin’s network topology using orphan transactions,” 2018. [Online]. Available: https://arxiv.org/abs/1812.00942
[5] Y. Gao, J. Shi, X. Wang, Q. Tan, C. Zhao, and Z. Yin, “Topology Measurement and Analysis on Ethereum P2P Network,” Proceedings - IEEE Symposium on Computers and Communications, vol. 2019-June, 2019.
[6] L. Zhao, S. S. Gupta, A. Khan, and R. Luo, “Temporal analysis of the entire ethereum blockchain network; temporal analysis of the entire ethereum blockchain network,” p. 12. [Online]. Available: https://doi.org/10.1145/3442381.3449916
[7] A. Papaditis, N. Kourtellis, and M. Sirivianos, “A first look into the structural properties and resilience of blockchain overlays,” arXiv preprint arXiv:2104.03044, 2021.
[8] “Running an XRP Ledger Validator,” Apr 2022. [Online]. Available: https://xrp.org/blog/2020/running-an-xrp-ledger-validator.html
[9] “Peer Crawler” XRPL.org, Jan 2022. [Online]. Available: https://xrp.org/peer-crawler.html
[10] B. Chase and E. MacBrough, “Analysis of the xrp ledger consensus protocol,” 2018.
[11] K. Christodoulou, E. Josif, A. Inglezakis, and M. Themistocleous, “Consensus crash testing; exploring ripple’s decentralization degree in adversarial environments,” Future Internet, vol. 12, no. 3, p. 53, 2020.
[12] I. Amores-Sesar, C. Cachin, and J. Mičić, “Security analysis of ripple consensus,” 2020.
[13] C. A. Roma and M. A. Hasan, “Energy consumption analysis of xrp validator,” in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020, pp. 1–3.
[14] H. Aoyama, “Xrp network and proposal of flow index,” in Proceedings of Blockchain in Kyoto 2021 (BCK21), 2021, p. 011003.
[15] ripple, “rippled,” Jan 2022. [Online]. Available: https://github.com/ripple/rippled
[16] spring_eng, “rippled-network-crawler,” Jan 2022. [Online]. Available: https://github.com/spring-eng/rippled-network-crawler
[17] “XRP Network Snapshots,” Apr 2022. [Online]. Available: https://drive.google.com/drive/folders/1SY4lencQSi0FCiagLOdSyNIOYlmQ6SLdg
[18] A.-L. Barabási and M. Pósfai, Network science. Cambridge: Cambridge University Press, 2016. [Online]. Available: http://barabasi.com/networksciencebook/
[19] A. D. Broido and A. Clauset, “Scale-free networks are rare.” [Online]. Available: http://arxiv.org/abs/2011.12938
[20] G.-S. Peng, S.-Y. Tan, J. Wu, and P. Holme, “Trade-offs between robustness and small-world effect in complex networks OPEN,” 2016.
[21] A. D. Broido and A. Clauset, “Scale-free networks are rare.” [Online]. Available: http://arxiv.org/abs/2011.12938
[22] M. E. J. Newman, “Mixing patterns in networks,” 2003.
[23] M. D. Humphries and K. Gurney, “Network ‘small-world-ness’: A quantitative method for determining canonical network equivalence,” PLoS ONE, vol. 3, no. 4, apr 2008.
[24] J. Kleinberg and S. Lawrence, “The structure of the web,” Science, vol. 294, no. 5548, pp. 1849–1850, 2001. [Online]. Available: https://www.sciencemag.org/doi/abs/10.1126.science.1067014
[25] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, “Measurement and analysis of online social networks,” in Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, ser. IMC ’07, p. 29–42. [Online]. Available: https://doi.org/10.1145/1298360.1298311
[26] A. Vázquez and Y. Moreno, “Resilience to damage of graphs with degree correlations,” 2003.
[27] M. E. Newman, “Mixing patterns in networks,” 2003.
[28] M. Karakaya, I. Korpeoglu, and O. Ulusoy, “Free riding in peer-to-peer networks,” IEEE Internet computing, vol. 13, no. 2, pp. 92–98, 2009.
[29] D. Hughes, G. Coulson, and J. Walkerdine, “Free riding on gnutella revisited: the bell tolls?” IEEE distributed systems online, vol. 6, no. 6, 2005.
[30] G.-S. Peng, S.-Y. Tan, J. Wu, and P. Holme, “Trade-offs between robustness and small-world effect in complex networks OPEN,” 2016.