ARTICLE IN PRESS

Telecommunications Policy xxx (xxxx) xxx

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

A centrality analysis of the Lightning Network

Philipp Zabka [a,*], Klaus-T. Förster [b], Christian Decker [c], Stefan Schmid [d,e]

[a] University of Vienna, Faculty of Computer Science, Waehringer Str. 29, 1090, Vienna, Austria
[b] TU Dortmund, Department of Computer Science, Otto-Hahn-Str. 16, 44227, Dortmund, Germany
[c] Blockstream, Zurich, Switzerland
[d] TU Berlin, Faculty of Electrical Engineering and Computer Science, Einsteinufer 17, 10587, Berlin, Germany
[e] Weizenbaum Institute, Berlin, Germany

ARTICLE INFO

Keywords:
Lightning Network
Betweenness centrality
Gini coefficient
Historic analysis

ABSTRACT

Blockchain technology has a huge impact on our digital society by enabling a more decentralized economy and policy making. This decentralization is also pivotal in payment Payment channel networks (PCNs), including the Lightning Network, have emerged as a promising solution to the scalability challenges that many blockchain-based cryptocurrencies, like Bitcoin, grapple with. These PCNs, while innovative, also inherit the rigorous dependability demands of the blockchain. A pivotal aspect of this dependability is the need for a high degree of decentralization, essential for mitigating liquidity bottlenecks and on-path attacks.

Driven by this imperative, our research embarks on an empirical centrality analysis of the Lightning Network, with a keen focus on the betweenness centrality distribution of its routing system. Utilizing an extensive dataset, sourced from several millions of broadcasted messages via the gossip protocol, we introduce the TimeMachine tool, an innovative method that allows for a temporal exploration of the network's evolution.

Our findings reveal that while the Lightning Network exhibits a commendable level of decentralization, there is a discernible skew: a limited set of nodes command a significant portion of the transactions. Alarmingly, over the past two years, the network's centrality has surged, with the inequality, as gauged by the Gini index, rising by over 15 uptick of approximately 5 in. This research not only uncovers critical insights into the Lightning Network's structural dynamics but also raises the question about strategies and policies that ensure its sustained decentralization in the face of evolving challenges such as security vulnerabilities, potential monopolistic tendencies, liquidity bottlenecks, the risk of transaction censorship and many more.

1. Introduction

Blockchain technology is currently revamping our digital society by enabling more decentralized economy, financial and telecommunication systems, as well as collective policy- and collective decision making. The technology enables mistrusting entities to cooperate without involving a trusted third party and underlies cryptocurrencies such as Bitcoin and Ethereum. However, with

---

* Corresponding author.
Linkedin: philippzabka (P. Zabka), Linkedin: christiandecker (C. Decker).
E-mail addresses: philipp.zabka@univie.ac.at (P. Zabka), klaus-tycho.foerster@tu-dortmund.de (K.-T. Förster), decker.christian@gmail.com (C. Decker), stefan.schmid@tu-berlin.de (S. Schmid).
URLs: https://gitlab.cs.univie.ac.at/philipp_zabka (P. Zabka), https://ktfoerster.github.io/ (K.-T. Förster), https://schmiste.github.io/ (S. Schmid).

https://doi.org/10.1016/j.telpol.2023.102696
Received 30 April 2023; Received in revised form 31 August 2023; Accepted 10 November 2023
0308-5961/

Please cite this article as: Philipp Zabka et al., *Telecommunications Policy*, https://doi.org/10.1016/j.telpol.2023.102696

their quickly growing popularity, blockchain networks face a scalability problem, and the requirement of performing repeated global consensus protocol is known to limit the achievable transactions rate.

Payment channel networks (PCNs) are a promising solution to mitigate the scalability issue, by allowing users to perform transactions *off-chain*. In particular, in a PCN, two users can establish so-called payment channels among each other, in a peer-to-peer fashion. The set of channels can then be seen as a graph, in which users are represented as nodes and channels are represented as edges. Payments can then also be routed in a multi-hop manner across these channels (typically using source routing), with forwarding users typically charging a small fee. Nodes can discover the cheapest routes using a gossip mechanism. The scalability benefit comes from the fact that it is only when a channel is opened or closed, that changes have to be made to the blockchain.

By the nature of the service they provide, PCNs need to meet stringent dependability requirements. Interestingly, while over the last years, several interesting approaches to design and operate payment channel networks in an efficient and reliable manner have been proposed in the literature, relatively little is known about the properties of the actually deployed networks today.

We in this paper are particularly interested in the level of decentralization provided by PCNs: decentralization is generally one of the key features of blockchain, and also naturally required from off-chain solutions.

The foundation of decentralized systems, like Bitcoin and the Lightning Network, is rooted in the desire to eliminate single points of failure and control. Centralization poses risks to privacy and the trustless and democratic ideology of decentralized systems. As the cryptocurrency domain matures, understanding the nuances of such systems becomes imperative, not just from a technical standpoint but also from a social and economic perspective. A centralized payment channel network, or any other system with similar intend for that matter, where transactions always flow through only few nodes, controlled by some kind of authority, would come close to show similar aspects to a bank. Centralization of such a network can lead to monopolistic control, reduced fairness in transaction fees, and potential censorship of transactions.

Indeed, it has recently been shown that skews in the routing system (e.g., due to exploits of the payment mechanism), can significantly harm the network performance, by depleting channels (Khalil & Gervais, 2017), or even lead to denial-of-service attacks (Tochner, Zohar, & Schmid, 2020) and privacy (Nisslmueller, Foerster, Schmid, & Decker, 2020; Tang, Wang, Fanti, & Oh, 2020) and other security issues (Malavolta, Moreno-Sanchez, Schneidewind, Kate, & Maffei, 2019a). While the primary function of the Lightning Network is to provide off-chain transaction capabilities, its centrality and structural dynamics remain largely unexplored. This paper delves deep into the complexity of the Lightning Network's topology, offering a comprehensive analysis of its centrality patterns. In order to gain a detailed understanding of Lightning, the most popular PCN, we monitored the network for several years, collecting millions of channel update and gossiping messages. To shed light on the network evolution, we further implemented tools which allow us to reconstruct the network at previous time stamps. In this paper, we present the main results of our study of the Lightning Network.

1.1. Our contributions

Motivated by the increasing popularity of payment channel networks and the resulting performance and dependability requirements, we report on an extensive empirical study of the most popular PCN, Lightning. In particular, we study to which extent Lightning fulfills the premise of decentralized transaction routing.

We find that there is a trend of increasing centralization and a high level of inequality, where a small portion of the nodes participate on most transaction routes. Well-connected nodes in the Lightning Network benefit as they can capitalize on their central position, handle increased traffic, and further strengthen their dominance in the network. This trend towards increased centralization and the benefits accrued by well-connected nodes can have implications for the network's resilience, economic fairness, and overall functionality.

We show that the level of centrality also depends on the transaction size, and we take a look at some of the highest ranked nodes according to centrality. We uncover that a fair share of nodes remained at the top over the examined period. To just give one example, our analysis shows that the top 5% of all nodes control a vast majority of all transaction routes, see Fig. 1, where previously, without channel capacities enabled, 10% of the nodes held the majority of the routes.

For our study, we collected significant data from the live Lightning Network, over a time span of almost two years. This data includes over 400 000 node announcement messages, over 1 000 000 channel announcement messages, and over 6 400 000 channel update messages. We further developed *TimeMachine*, a tool which allows us to reconstruct the network at desired moments in time. By introducing the TimeMachine, we provide a novel way to reconstruct and analyze the state of the Lightning Network at various historical points. This temporal analysis is pivotal in understanding the evolving patterns of centralization, a feat not achieved to this extent by previous studies.

Our empirical observations have implications for stakeholders, developers, users as well as for policy makers in general. By highlighting these patterns, we hope to instigate discussions on potential modifications to the network's protocols or the introduction of new mechanisms to ensure true decentralization.

As a contribution to the research community, in order to ensure reproducibility as well as to support future research in this area, we will make available all our code and experimental artifacts together with the accepted version of this paper.

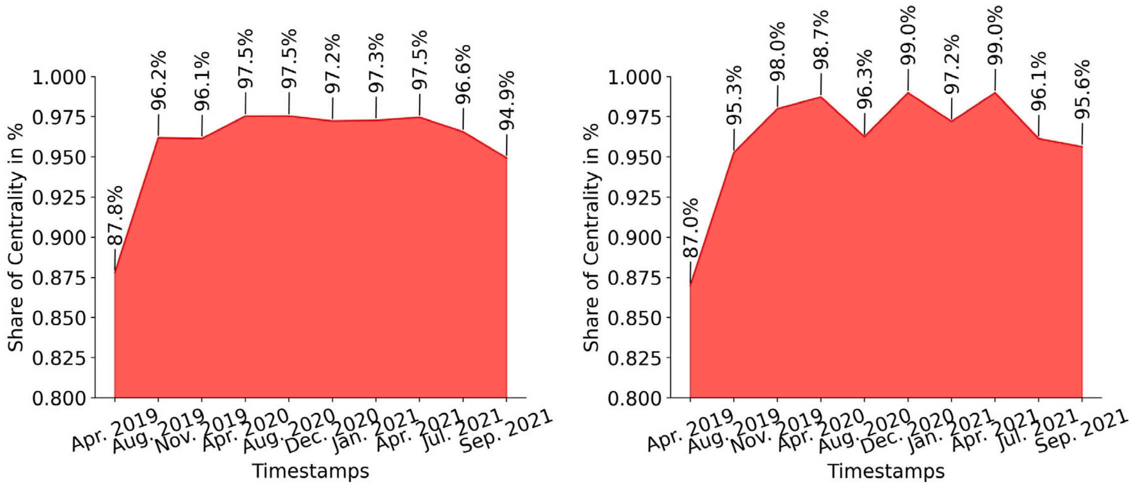

Fig. 1. Top 5% control over routes without (top) and with multi-path payments enabled (bottom).

1.2. Related work

Over the last years, many interesting approaches to design and operate payment channel networks have been proposed in the literature, and we refer the reader to Dotan, Pignolet, Schmid, Tochner, and Zohar (2021), Gudgeon, Moreno-Sanchez, Roos, McCorry, and Gervais (2020) and Neudecker and Hartenstein (2018) for an overview. In the remainder of this section, we first briefly give an overview on some dependability research, before focusing on our main topic of centralization. Here we first delve briefly into fiscal policies, before considering centralization in PCNs itself. Lastly, we give a short overview on further research of empirical properties of deployed PCNs.

Regarding *dependability* aspects, Kappos et al. (2021) showed the general susceptibility of privacy concerns, with Rohrer and Tschorsch (Rohrer & Tschorsch, 2020) focusing on timing attacks, and Romiti et al. (2021) using clustering techniques, whereas Moreno-Sanchez, Kate, Maffei, and Pecina (2015) and Malavolta, Moreno-Sanchez, Schneidewind, Kate, and Maffei (2019b) investigate how to preserve privacy and scalability. Harris and Zohar (2020) on the other hand consider how channel closures can be used to steal funds from channels.

However, we in this paper, we are particularly interested in issues related to *centralization*, a topic which has recently also received much attention in the context of Bitcoin in general (Beikverdi & Song, 2015; Coindesk, 2021; Forbes, 2019). Regarding the fiscal policy in political economy settings, Lockwood (Lockwood, 2002) discusses the efficiency gains from decentralization, concluding that the "*cost of centralization*" is inefficiency in project choice and slow responsiveness in legislation. The topic has been widely studied, we refer to Lockwood (Lockwood, 2002, §2) for an overview. For example, Azfar, Kahkonen, Lanyi, Meagher, and Rutherford (2018) state that decentralization can improve allocative and productive efficiency, that there is however also danger, e.g., referencing (Bardhan & Mookherjee, 1998), that elites may take over local governments—a danger also (omni-)present in cryptocurrencies, where attackers will try to attack the inherent consensus protocols (Bonneau, 2018).

In most research on cryptocurrencies and PCNs however, there is not much debate regarding policy choices on centralization versus decentralization, as a "*fully decentralized network*" (Dasaklis & Malamas, 2023) is a fundamental design goal itself. As such, in the context of PCNs, it has been shown that centralization of the routing system can harm performance (EmelyanenkoK, 2020; Tochner et al., 2020), liquidity (Khalil & Gervais, 2017; Khamis, Schmid, & Rottenstreich, 2021), security (Malavolta et al., 2019a), and privacy aspects (Malavolta, Moreno-Sanchez, Kate, Maffei, & Ravi, 2017; Nisslmueller et al., 2020; Tang et al., 2020; Tripathy & Mohanty, 2020), especially when considering on-path adversaries. Hence, from a network performance and vulnerability point of view, decentralization is inherently desirable. However from a state actor's point of view, the opinion may differ, and centralized regulations may be desired (Shulman, 2019), e.g., in order to control the outflow of money, or to better tackle terrorism funding and money laundering: "*There is, in many countries, continuing discussion over the desirable degree of fiscal decentralization.*" (Lockwood, 2002)

Interestingly, relatively little is known about the *empirical* properties of deployed payment channel networks such as the Lightning Network, in contrast to blockchains like Bitcoin, which have been extensively analyzed and measured over the past decade. Dotan, Pignolet, Schmid, Tochner, and Zohar (2022) conducted a survey in which, upon others, open research questions concerning payment channel networks are highlighted, especially related to their centrality and node connectivity over time. With this paper, we hope to shed a little bit of light onto these still unresolved research problems. Ben Mariem et at. measured the main properties and topology of Bitcoins P2P network (Vivisecting, 2019) and Dotani et al. presented a measurement tool for Bitcoins P2P network called BTCdoNEt (Donet, Pérez-Sola, & Herrera-Joancomartí, 2014).

The Lightning Network's topology has been analyzed by Seres, Gulyás, Nagy, and Burcsi (2020). Their work studies the robustness of the network against random failures of nodes as well as attacks targeting nodes. A similar, but more in detail work has been carried out by Rohrer, Malliaris, and Tschorsch (2019). Stefano Martinazzi (2020) analyzed the evolution of the Lightning Network over a period of one year, beginning on its launch on the Bitcoin mainnet in January 2018. Their work focuses on the topological robustness of the network, e.g., against attacks, where they also detect a high influence of a few nodes on the network. Next, a large scale empirical analysis on the client and geographical classification of nodes is performed by Zabka, Foerster, Schmid, and Decker (2022), Zabka, Förster, Schmid, and Decker (2021), see also Mizrahi and Zohar (2021). Related to this, Scellato, Mascolo, Musolesi, and Latora (2010) study how geographic distance affects social ties in a social network and Mislove, Lehmann, Ahn, Onnela, and Rosenquist (2011) examine geographical, gender and racial aspects of Twitter users to the U.S. population.

1.3. Organization

Organization. The remainder of this paper is organized as follows. Section 2 introduces some preliminaries and Section 3 describes our methodology, followed by the centrality analysis in Section 4 and centrality analysis considering multi-path payments in Section 5. We subsequently conclude in Section 6.

2. Preliminaries

We now introduce some of the necessary basics of the Lightning Networks and some specific preliminaries for the remainder of the paper.

The Lightning Network. The Lightning Network is an off-chain solution to improve the scalability of cryptocurrencies such as Bitcoin. The network can be accessed via three clients, namely LND (LND, 2023) implemented in Go, C-Lightning (CLN, 2023) implemented in C and Eclair (Eclair, 2023) implemented in Scala. However, with an usage of more than 85%, LND is currently by far the most popular client (Zabka et al., 2021). The Lightning Network users are able to create bidirectional connections to other users, called channels. These channels can be used to send instant payments between two users, which do not need to be necessarily directly connected. If a payment is routed across multiple users, the users in between the route may demand fees for the routing process. The Lightning Network does not operate on the blockchain itself, however the first transaction called the funding transaction to create a channel needs to be propagated onto the blockchain. The same goes for the last transaction or closing transaction to end the connection between two users. All intermediary transactions are not propagated onto the blockchain and therefore can be processed in a much faster fashion.

Gossip Messages. As the name implies, gossip messages are propagated through the whole network to either announce a node or channel creation or an update. Therefore, all participants have an contemporary view of the network. This mechanism is especially important in the case that a node wants to route a payment to a node it is not directly connected with. In the following we will take a more in detail look at the three most important gossip messages, which are specified in the Basics of the Lightning Technology (BOLT) (Lightning Network, 2023):

- **node_announcement_message**: This message allows nodes to inform other participants about extra data associated with it, besides the node ID. It contains data such as the IP address, color, alias and timestamp as well as information for opting into higher level protocols.
- **channel_announcement_message**: If a channel is created between two nodes this message is propagated through the network. It contains information such as an short channel ID, which is an unique identifier for the channel, as well as both node IDs.
- **channel_update_message**: A channel is practically not usable until both sides announce their channel parameters. These parameters are announced in this message. As the Lightning Network is directed, both channel participants have to send a message. The parameters included in this message are among other things used to calculate the routing fees. Every time one side updates its channel parameters, this message is broadcast in the network.

Routing Fees. In the Lightning Network nodes along a routed path take a small fee for forwarding transactions. The parameters necessary for the calculation are *fee_base_msat* and *fee_proportional_millionths* which can be found in the *channel_update_message*. Hereby *fee_base_msat* denotes the constant fee a node will charge for a transfer and *fee_proportional_millionths* is the amount a node will charge for each transferred satoshi over their channel. Fees are calculated as follows, where transferred_amount denotes the transaction in millisatoshi:

$\text{fee\_base\_msat} + (\text{transferred\_amount} * \text{fee\_proportional\_millionths}/1\,000\,000)$

Betweenness Centrality. The betweenness centrality represents a measure in a network based on shortest paths, a node's centrality is based on how many such paths traverse it. Formally, the betweenness centrality c_B of the nodes $v \in V$ is $c_B(v) = \sum_{s,t \in V} \sigma(s,t|v)/\sigma(s,t)$, with $\sigma(s,t)$ $[\sigma(s,t|v)]$ as # shortest st-paths [through v, $v \neq s,t$]. If $s = t$, $\sigma(s,t) = 1$, and if $v \in s,t$, $\sigma(s,t|v) = 0$ (Brandes, 2008; Hagberg, Schult, & Swart, 2008). For every node pair in a connected unweighted graph, there exists at least one shortest path between these nodes such that the number of edges is minimized. For weighted graphs such as the Lightning Network, where channel routing fees represent edge weights, the sum of the edge weights is minimized.

Among several interesting alternatives (Das, Samanta, & Pal, 2018; Liu, Slotine, & Barabasi, 2011), we focus on betweenness centrality as our main centrality measurement. Nodes with high betweenness centrality have a considerable amount of influence on a network by means of information control, since most of the network traffic will pass though them—in contrast to other centrality measures which represent a more local view, e.g., degree centrality, which counts the numbers of edges incident to a node.

A high betweenness centrality is a particular concern as nodes choose routing paths with the overall cheapest fees, and a skewed centrality indicates that routing paths are concentrated to a small subset of nodes. A skewed centrality may not only quickly deplete

Table 1
Lightning network snapshots.

Abbr	Timestamp	Date	#Nodes
T1	1554112800	01 Apr. 2019	1362
T2	1564653600	01 Aug. 2019	4589
T3	1572606000	01 Nov. 2019	4699
T4	1585735200	01 Apr. 2020	5230
T5	1596276000	01 Aug. 2020	5905
T6	1606820400	01 Dec. 2020	6331
T7	1609498800	01 Jan. 2021	6629
T8	1617271200	01 Apr. 2021	8821
T9	1625133600	01 Jul. 2021	10 867
T10	1630490400	01 Sep. 2021	13 611

payment channels, but also makes the network vulnerable: many attacks recently reported in the literature are based on on-path adversaries (Mizrahi & Zohar, 2021; Rohrer et al., 2019). Getting a significant amount of traffic can also raise privacy concerns, e.g., during route discovery.

3. Methodology

We next introduce the methods to obtain and process our data set.

TimeMachine. The Lightning Network TimeMachine (Decker, 2023) is a tool written in Python, which reconstructs the state at a prior point in time by replaying gathered gossip messages up to that point in time. We have deployed a number of C-Lightning nodes that collect and archive these messages, which are then deduplicated and ordered by their timestamp, in order to allow the TimeMachine to replay them in the correct order, and terminate once the desired point in time has been reached, leaving the view of the network close to what the public network would have looked like at that time. We utilized the TimeMachine to rebuild the network at ten different points in time, covering a time span of two years ranging from 01 Apr. 2019 to 01 Sep. 2021. We then used the Python library NetworkX (Hagberg et al., 2008) to further analyze the networks in regard to the betweenness distribution in different timestamps. With the help of our TimeMachine we were able to reconstruct the network as it was at the timestamps mentioned in Table 1. From now on we will reference the timestamps as T1–T10.

Data Set. Our data was collected with help of C-Lightning nodes, which synchronize their view of the network topology by listening and exchanging gossip messages. Internally C-Lightning will deduplicate messages, discard outdated *node_announcements* and *channel- _updates*, and then apply them to the internal view. In order to persist the view across restarts, the node also writes the raw messages, along some internal messages, to a file called the *gossip_store*. The node compacts the *gossip_store* file from time to time in order to limit its growth. Compaction consists of rewriting the file, skipping messages that have been superceded in the meantime. Our data set is comprised of the three gossip messages discussed in the previous section. Our nodes have recorded more than 400 000 *node_announcement messages*, more than 1 000 000 *channel_announcement messages*, and over 6 400 000 million *channel_update messages*.

4. Centrality analysis

This section reports our main results from the centrality analysis. We performed a detailed analysis where we measured the betweenness centrality, a major centrality measure, of the Lightning Network at different points in time and observed how it has developed over almost two years. More precisely, we took seven snapshots of the network, dating from 01 Apr. 2019 to 01 Sep. 2021. Based on the formula for calculating routing fees introduced in we calculated the betweenness of each node based on three different realistic transaction sizes namely 10 000 000 Millisatoshi (0.0001 BTC), 100 000 000 Millisatoshi (0.001 BTC), 1 000 000 000 Millisatoshi (0.01 BTC), 10 000 000 000 Millisatoshi (0.1 BTC) and 100 000 000 000 Milisatoshi (1.0 BTC). The idea of calculating the betweenness with different transaction sizes was if we could detect significant changes.

4.1. Historic betweenness analysis of the lightning network

Evaluating the Lightning Network at different points in time in terms of the betweenness centrality can provide us with insights which allow us to better comprehend how it has developed until now e.g. has it become more centralized or the opposite and also make predictions in which direction it may develop in the future. We start by we examining our latest snapshot first.

Timestamp T10 We decided to use a logarithmic scale on the x-axis to better display the long range of centrality values (1 - 30 000 000). Further, we do not include nodes with a centrality value of 0, as they either represent leafs in the graph or nodes that cannot forward a payment and would distort the graph. Also the amount of such nodes is astonishing high, up to 11 397 nodes out of 13 611 in T10 for 0.0001 BTC.

In Fig. 2 (left) we can see that transaction size has indeed an influence on a node's centrality if the transaction amount is low or high enough. In the case of 0.0001 BTC respectively 0.01 BTC there is only a minimal change in the centrality distribution among the nodes, however, in the case of all other transaction sizes we can see a significant shift. A possible explanation for this

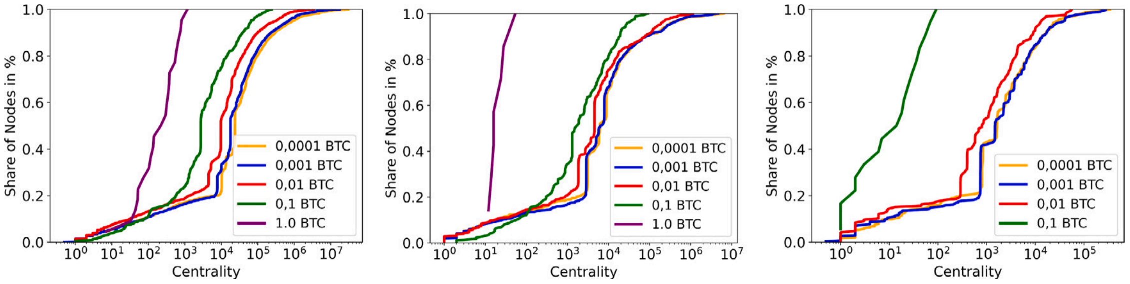

Fig. 2. Centrality distribution in timestamps T10 (left), T5 (middle) and T1 (right).

shift in distribution we are experiencing is that for smaller transactions, more routes are used, since more nodes can forward small transactions.

Another interesting observation is that the smaller a transactions is and therefore more nodes can be used to forward a payment, the more nodes stay under a specific centrality threshold before the centrality abruptly increases. Regarding 0.0001 BTC and 0.001 BTC the threshold for around 20% of the nodes lies at approximately 10 000 betweenness centrality. Looking at our highest transaction of 1.0 BTC, the threshold lies around 150 centrality and concerns around 10% of the nodes.

Timestamp T5 In T5 we can make out only a few detailed changes 11 months prior to our latest timestamp T10. Observing Fig. 2 (middle) shows the centrality distribution for 800 nodes out of 5905, so 5105 nodes remain leaf nodes or nodes having not enough liquidity with a centrality of 0 for our smallest transaction size of 0.0001 BTC. The most noticeable difference to timestamp T10 is that the distributions for both our smallest transaction sizes are even more identical and they are also getting closer to the distribution of our third largest transaction size of 0.01 BTC. However, this is most probably due to the overall lower amount of nodes in the network at that point in time and therefore limited amounts of paths that can be selected.

The next noticeable observation is the high jump around the 5000 betweenness centrality mark for the transaction sizes of 0.0001, 0.001 BTC and also 0.01 BTC. For 0.0001 BTC roughly 100 nodes are affected and for 0.01 BTC or respectively 0.1 BTC roughly 130 nodes are concerned. Since the Lightning Network is still new and relatively small, it is possible that these nodes are all positioned on specific shortest paths and therefore share the same centrality. As the number of nodes increases it is likely that the distribution of betweenness centrality becomes more varied over time as nodes increase their interconnection creating new paths to route through.

Timestamp T1 Fig. 2 (right) depicts the centrality distribution for T1, which is 29 months prior to T10. At first glance we can immediately detect the missing line for 1.0 BTC, which means none of the nodes present at T1 was able to route this amount as it was too high. We can see that 0.1 BTC now has a similar distribution to 1.0 BTC in T5 and T10.

Furthermore jumps still occur. Betweenness values calculated with the transaction size of 0.001 BTC experience the highest jumps. The first one starts at around 1000 centrality and affects 0.3% of the nodes. At last, compared to the most central node in T10, the most central node in T1 only reaches an centrality of 340 000 for 0.0001 BTC. Even though the lower value is the result of fewer nodes in the network, one cannot deny the rapid centralization of the network within the period of two years. We next further substantiate our observation of growing centrality.

4.2. Inequality in the lightning network

The Gini coefficient is an economic measure for the inequality within a nation or a social group. Similarly, we use this index in the context of payment channel networks to shed light on the inequality and skew there exists in the network topology. In particular, an "unfair" distribution concentrates much control to a small set of nodes, which is problematic not only for the efficiency of the network but also raises security concerns. Many attacks in the literature are based on on-path adversaries (Mizrahi & Zohar, 2021; Rohrer et al., 2019), which hence have significant control. This also generally goes against the idea of decentralization of finance.

Fig. 3 (left and middle) depicts the Lorenz curves for T10 and T1. The Gini coefficient is equal to the area below the line of perfect equality minus the area below the Lorenz curve, divided by the area below the line of perfect equality. Looking at Fig. 3 (left) showing the latest snapshot of the network, we can see an excellent example of a perfectly unequal distribution, where 90% of the nodes correspond to only 2% of the cumulative betweenness of all nodes. Consequently, this indicates an extraordinarily high network centralization, where 90% of the shortest paths in the network lead through only a few highly centralized nodes. Next, looking at Fig. 3 (middle) we can observe that 90% of the nodes make up for slightly more than 5% of the betweenness, which is still not an ideal scenario. Subsequently, we can conclude from our observations that within 21 months the centralization has risen by 3%. Fig. 3 (right) depicts the Gini coefficients for all ten timestamps. Here we observe an upward trend in the direction of inequality or centralization. The coefficient is slightly rising almost each timestamp, reaching a peak centralization in timestamp T9 with 76.5%. The most significant icreases of the gini coefficient happened between timestamps T1–T2 (6.1%), T3–T4 (5.5%) and T7–T8 (6.5%). Overall, we can deduce that the Lightning Network is highly centralized. Having only few, very influential nodes through which most paths are routed, is not beneficial for the robustness of the network. These nodes pose as significant targets for attacks and could disrupt the network in the case of failure. However not only attackers could exploit this situation, but also the nodes or rather the individuals controlling these nodes.

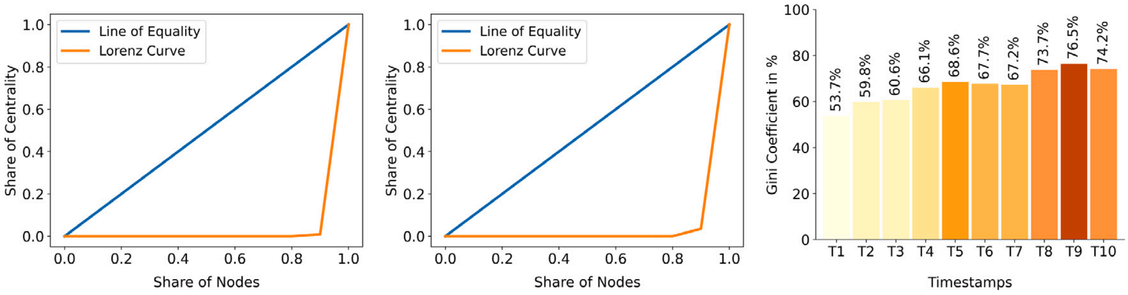

Fig. 3. Lorenz curves for the timestamps T10 (left) and T1 (middle). Gini Coefficients ranked according to all ten timestamps (right).

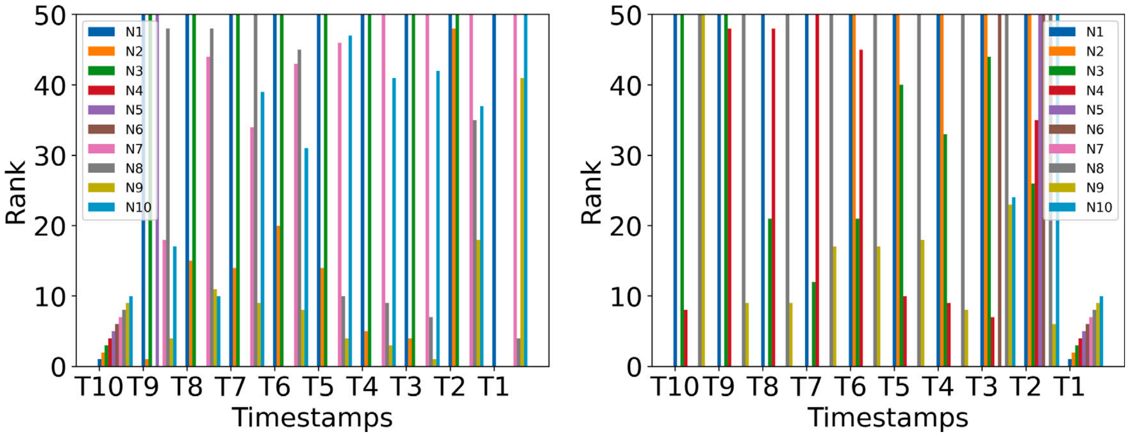

Fig. 4. Top ten influential node timelines, with latest left and oldest right.

4.3. Analysis of the top 10 nodes

We lastly trace the performance of the most influential nodes, based on their centrality, in our latest and oldest timestamp, and briefly discuss our findings.

Fig. 4 (left) depicts the top 10 nodes with the highest centrality in the latest timestamp T10 and their ranks in the earlier timestamps. We can see that most top nodes were also highly ranked in the past, e.g., N2 has always been in the Top 20, beginning from timestamp T2. Also node N9 (ACINQ (ACINQ, 2023), developer of Eclair) has been ranked below the top 50 throughout all our timestamps. Interestingly, a fair share of the top 10 nodes in T10, have not been around for long as they do not appear in the older timestamps at all, such as nodes N4, N5 and N6. These nodes have not been in the network two months prior in timestamp T9, but already count among the top 10 nodes in T10, displaying a high centrality.

We now look the other way around to observe if a node could hold its central position in the network. Fig. 4 (right) depicts the top 10 nodes in T1 our oldest snapshot and how the nodes performed from there on. For clarification the nodes depicted in this figure are partially not same as in Fig. 4 (left). Many nodes could not hold their position and even disappeared from the network. None of the nodes from T1 stayed in the top ten for the whole time of observation, however, node N4 stayed in the top 50 throughout the time. Other nodes that stayed in the network, although not being of relevance are nodes N1, N3, N8 and N9. So in total half of the nodes, which have been in the top ten in T1, survived, the other half disappeared.

Hence we can conclude, a strong position in the past is not a guarantee, and many past top 10 nodes lost influence.

5. Centrality analysis with multi-path payments

In Section 4 we have analyzed the centrality of nodes in the Lightning Network with the standard proceeding when routing transactions from sender to receiver. To be more specific, the sender calculates a single path (single-path payment) on which each channel has to have enough capacity to forward the payment to the next hop until the final destination is reached. For small to medium sized single-path payments this path finding process is easy and unproblematic since most of the channels in the network have enough capacity to route the transaction. However, the larger a transaction gets, the more difficult it gets to find a viable path from sender to receiver. In the worst case a payment cannot be routed at all, because there exists no path with enough channel capacities along the way to reach the final destination.

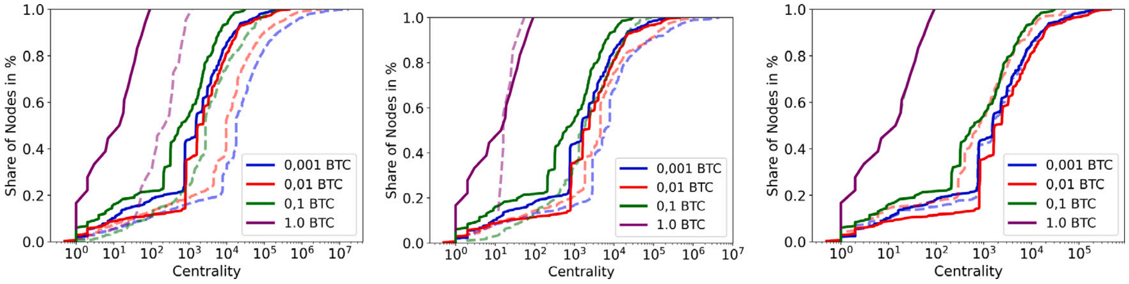

Fig. 5. Centrality distribution of Single Path and Multi Path in timestamps T10 (left), T5 (middle) and T1 (right).

Multi-path payments are Lightning Network's solution to overcome this critical problem and effectively enables the routing of large payments to the majority of participants in the network. Each Lightning Network client uses a bit different approach to this solution, however the core principle stays the same:

Large payments are split up into smaller chunks that should fit through most of the channels without a problem. Each chunk then may take a different path to the receiver. An important factor that needs to be considered when splitting up a transaction into smaller parts, is not to create too many of them, since they would easily consume all Hashed Time Lock Contracts (HTLCs) available. A HTLC ensures that in the case of payment failure, the transaction is rewinded and each node gets its money back.

5.1. Multi-path payments in core lightning (CLN)

Core Lightning, formerly known as C-Lightning, is one of the currently available clients to access the Lightning Network. LNC's multi-path payment process is comprised of two modifiers:

1. **Pre-Splitter**: This first modifier is applied to the original payment and splits the payment into parts that have a higher probability to succeed right away. However, splitting cannot be applied trivially or otherwise it could create more transactions than available HTLCs. CLN uses a threshold of maximal 16 splits (Core Lightning, 2023) for the pre-splitter and a multi-path payment target size of 10 000 000 msat (0,0001 BTC) for its splitting process. The initial root payment is divided by the target size and if the quotient is larger than the threshold, the target size is multiplied by the threshold and the process is repeated until the quotient equals less than the threshold.
2. **Adaptive-Splitter**: In the case that a part of a payment fails to be forwarded to the final receiver, the adaptive-splitter splits the failed payment in half. The goal of this modifier is to find two smaller routes through which the two halves can be routed to complete the full payment. The modifier also checks if there are still enough HTLCs available and aborts the process if that is not the case anymore.

While multi-path payments mitigate the issue of channels becoming bottlenecks for large transactions, they do not ensure the success of a payment even when it is divided into smaller transactions, due to potential liquidity constraints in the network. Consequently, there will always be a certain failure rate associated with the network's capacities. The only leeway available for a Lightning Network implementation is to optimize the search for a valid multi-path payment through channels for which the capacities are not known during the planning phase and are subject to a 60-second multi-path payment timeout. All implementations strive to align their payment success rate with this intrinsic network success rate. The pre-splitter and adaptive-splitter are optimizations designed to help achieve a success rate closer to that of the network. The increased traffic on the network results in additional difficulties that may need to be tackled. There are several hurdles that open up when splitting up a payment into smaller units such as a higher resource intensiveness on the channels and nodes, privacy concerns and an increased number failure points, since more nodes are involved in the routing process.

5.2. Historic betweenness analysis of the lightning network

We have evaluated the betweenness centrality of nodes regarding single-path payments in Section 4.1. Now we analyze what differences arise when we measure the betweenness centrality using multi-path payments.

Timestamp T10 By examining Fig. 5 (left) we can immediately detect the left shift regarding all multi-path payment distributions for all transaction sizes. This shift can be explained from the overall increased amount of nodes participating in the routing process. Many nodes which have had a betweenness centrality of 0 in single-path and therefore have not been included into the plots, now have centrality score greater zero and hence have shifted the distributions to the left, creating a deceptive impression that the overall centrality distribution is less skewed, which is not the case. What is more the centrality for the top nodes has increased significantly. The most central node for the transaction size of 0.001 BTC using single-path payments has a centrality of 17 530 847. In contrast the most central node when using multi-path payments shows a centrality of 53 763 369, which is 3 times higher than using former. To be clear, these top performing nodes are different, but the best performing node using multi-path payments is ranked 5th in single-path payments with a betweenness centrality of 8 444 838. Generally, speaking nodes that already showed a

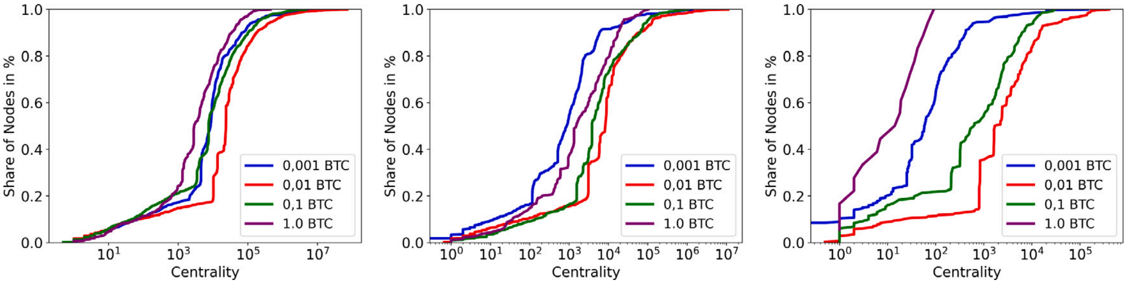

Fig. 6. Centrality distribution of differences of Multi Path and Single Path in timestamps T10 (left), T5 (middle) and T1 (right).

high centrality in single-path have an even higher centrality score when considering multi-path. Since these top nodes already are key hops, their traffic even increases when we split up the original transactions into smaller ones. When we split up a large payment into smaller sub payments, also more possibilities are created to route these payments since more channels have enough capacity to forward these smaller transactions, therefore more nodes are able to participate in the routing process. For the transaction size of 0.001 BTC, 2432 nodes have participated in the routing process, whereas for the same transaction size using single-path involves approximately 200 nodes less. However, multi-path payments performs the best when using large transactions, which otherwise could be routed only be a handful of nodes. The transaction of 0.1 BTC and 1.0 BTC could only be routed by 381 respectively 22 nodes using single-path payments. By using multi-path, 1458 nodes for 0.1 BTC have been involved or respectively 442 nodes for 1.0 BTC have been involved in the routing process.

Fig. 6 shows the betweenness centrality differences between multi-path and single-path payments. We see that the largest share of differences lies in the range within 1000 to 1 000 000, showing that using multi-path payments has a significant impact on a node's centrality, creating a less skewed distribution and hence, in almost all cases, performing better.

Timestamp T5 and T1 Looking at T5 in Fig. 5 (middle), we can see a similar picture in distribution as we already have observed in T10. However, the centrality distributions between single-path and multi-path now are more narrow. This is most due to the fact that there are fewer nodes in the network as they are in T10. The fewer nodes are in the network the fewer the options are regarding the transaction routing, which explains why the distributions for single-path and multi-path get more similar. Fig. 5 (right) depicting the distributions for our oldest timestamp T1, even more highlights this circumstance, since there are even fewer nodes in the network at that time. The only exception is the distribution for the largest transaction of 1.0 BTC. When using single-path, no node was able to route a transaction this high, whereas when using multi-path, we see that routing was possible.

Figs. 6 (middle and right) show us that the discrepancies between the centrality distributions of single-path and multi-path increase, when fewer nodes are involved. Because of the fact that there are not many nodes to choose from, the nodes with an already high centrality in single path profit the most when using multi-path, since we create more transactions by splitting them up and therefore allowing these nodes to forward them.

5.3. *Inequality in the lightning network*

We already have observed a high inequality in Section 4.2 using single-path payments. Even though the disparity gets a little bit more equal if we split the payment, however not significantly as we can see in Fig. 7 (left and middle) for timestamps T10 and T1. As we already have seen in the previous chapter, well connected nodes profit even more from multi-path payments, strengthening their central position in the network even further. Still, through multi-path payments more nodes can be utilized to partake in routing the split payments to their final destination, providing a bit more equality as single-path does. Lastly, let us take a look at Fig. 7 (right) depicting the gini coefficients for timestamps T1 to T10. Compared to Fig. 3 (right) depicting the gini coefficients using single-path payments, we can see that the coefficient has risen even higher when using multi-path payments, peaking in timestamp T3 and T4 with almost 90%. Surprisingly, although the numbers still remain relatively high, levels off to around 84% to 86% in the following timestamps. The main cause for such high gini coefficients in each timestamps using multi-path is the disproportionately high betweenness centrality score of the few top nodes compared to the majority of nodes in the network as we have already examined in the previous sections. The elevated centrality scores of certain nodes, which were already notable due to their strategic position and connectivity within the network, are influenced by a combination of factors. These include the reliability and efficiency of their connections, and their historical performance in handling transactions. It is not solely about the increased traffic they manage. Their essential role in the network is amplified by the dynamics of simultaneous transactions and their ability to maintain consistent performance under heavy load.

Generally speaking the goal of multi-path payments is not to lower the centrality in the network and providing more equality. It was mainly introduced to make high transactions viable. By splitting a transaction, more routes can be used and more users can forward and also receive such payments. Fig. 2 (right) in Section 4.1 and Fig. 5 (right) in Section 5.2 show that the mechanism succeeds in its purpose as we could route 1.0 BTC in timestamp T1 using single-path, however enabling multi-path payments have made it possible. Though there are currently no mechanisms in place to prevent a strong level of inequality, addressing this issue, especially concerning multi-path payments, is crucial for the health of the network. One potential approach to mitigate this

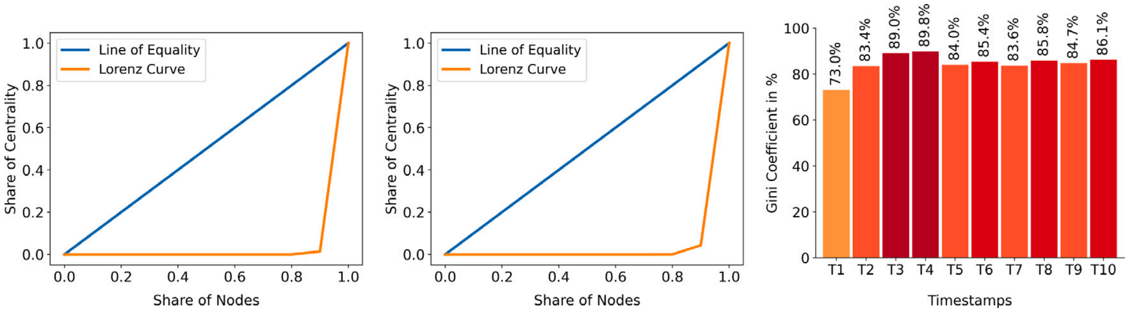

Fig. 7. Lorenz curves for the timestamps T10 (left) and T1 (middle). Gini Coefficients ranked according to all ten timestamps (right).

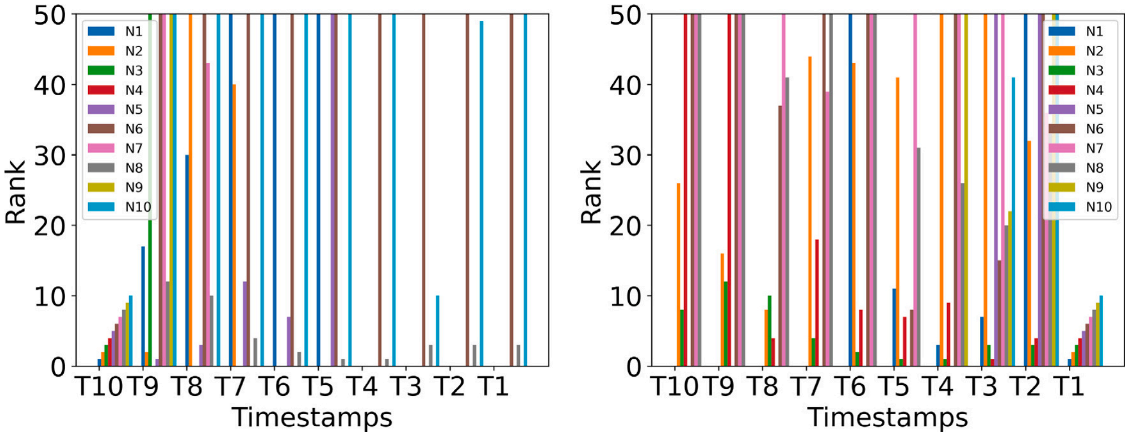

Fig. 8. Top ten influential node timelines, with latest left and oldest right.

centralization is to introduce incentives that promote a decentralized structure. By rewarding nodes that establish connections with less central nodes or offering benefits for diversifying channel connections, the network can encourage a more balanced distribution of transaction flow. Next, modifying or enhancing the current routing algorithms to prioritize more decentralized paths can also be a viable solution. Even if these paths might be slightly less efficient, directing transactions through a broader set of nodes can reduce the dominance of the central nodes. Additionally, adjusting the fee structures to make transactions that continually use the most central nodes more expensive could encourage users to seek alternative routes for their transactions, further promoting decentralization.

5.4. Analysis of the top 10 nodes

In this section, we examine the ranking of the top ten nodes from timestamp T10 and vice versa when using multi-path payments. Fig. 8 shows us the top ten nodes in timestamp T10 and their ranks in the previous timestamps. The most notable difference compared to Fig. 4 (left) in Section 4.3 is how few nodes from the top ten are represented in the older timestamps, particularly in timestamps T1 to T4 we can observe always the three same nodes which are N6, N8 and N10. N6 and N10 are nodes which have not been represented in the top ten when using single-path. N6 ranks 28th and N10 ranks 101st in single-path, but N8 in multi-path is the same node as in single-path. Node N8 is also one of the few nodes remaining in relatively high ranked in every timestamp. However, otherwise no other nodes from the top ten in multi-path are represented in the top ten of single-path, though many of them remain in the top 100. Fig. 8 (right) visualizes the top ten nodes and their scores in timestamp T1 and their ranking in the other timestamps up to T10. Starting with node N1, we see that it could hold a high position until timestamp T5 ranking 11th. In T6 however N1 fell from the 11th place to the 1541st rank before completely disappearing from the network in T7. Node N1 can also be found in Fig. 4 (right) being represented as node N2. Examining the figure, we can observe a similar development until its disappearing in T7. Other nodes that are represented in both figures are node N3 in multi-path respectively N4 in single-path and node N10 in both plots. N10 shares a similar fate as node N1, but node N3 remains highly ranked throughout the time, which is no surprise, because it is the same node we have discussed in the paragraph above, namely N8. Using the website 1ML, a Lighting Network Explorer (Bitcoin Lightning, 2019), we take a more detailed look at node N8 (N3/N4). It is a well connected node with a total channel count of 234 active channels, a capacity of 4.67 BTC which are at the time of writing 88,646$ and called Rompert (2023). As it was already the case in Section 4.3, we can come to the end that a strong position at a timestamp in not an indicator for the performance in the past or future, since there can be several external factors that influence a nodes position in the network, such as maintenance of the nodes by their users.

Overall one of the primary benefits which well-connected nodes enjoy is the increased traffic they receive, even more with multi-path payments as they involve splitting a transaction into smaller parts to be routed through different paths. Given their central position, these nodes, are more likely to be chosen as intermediaries for a higher number of these split transactions. This not only boosts their transaction volume but also potentially increases the fees they collect for routing payments. Furthermore, the centrality of these nodes in the network's topology enhances their reliability as routing options. Transactions in the Lightning Network seek out the most efficient and reliable paths, and well-connected nodes, by virtue of their numerous channels. This means that they are more likely to be chosen as preferred routes, even when other, less central nodes might be available. Nodes that are not as well-connected do not enjoy these benefits to the same extent. Their peripheral position in the network means they handle fewer transactions and collect fewer fees. Moreover, they might not be privileged to the same volume of network information as their well-connected counterparts, potentially limiting their ability to optimize their operations. However, this centralization can introduce risks, such as single points of failure or increased potential for transaction censorship.

6. Conclusion

Motivated by the increasing decentralization requirements of emerging sectors in finance and telecommunications, we conducted a centrality analysis of one of the first and largest payment channel networks, Lightning. We uncovered a significant imbalance and skewed centrality in Lightning, and using our historical data, showed that there is a trend towards further centralization.

A direct implication for a more centralized network is the gradual loss of privacy of payments and the users performing these payments. In the most extreme case of a hub-and-spoke model, the hub can learn all payment pairs, create profiles, censor payments, and extort additional personally identifiable information (PII) in order to perform the payments of a user. While the decrease in privacy happens gradually, it is essential to keep the network as decentralized as possible. This ensures the network remains robust and reduces the risk of major privacy issues. These privacy concerns have both economic and social impacts, which can have negative economic and social implications. As such, our findings can also inform policy makers about potentially undesired effects which may require actions and regulations.

From the viewpoint of network performance and reduction of attack surfaces on privacy, the "right" answer for policy makers would as thus be to favor decentralization, e.g., to incentivize the better connectivity and availability of smaller nodes to reduce the impact of a centralized skew, first research on such incentives is proposed by Avarikioti, Lizurej, Michalak, and Yeo (2023). However, e.g., state actors might form different viewpoints depending on their ideologies (Shulman, 2019) and could even demand centralization and stronger regulation. Here the situation is more unclear, and "*much is still unknown as to effective regulation of the industry, and if there even is a 'right' answer* (Shulman, 2019), which would be interesting to investigate next.

We believe that our work also opens further several interesting directions for future research. In particular, it will be interesting to investigate other off-chain networks, further implications of centrality in cryptocurrency networks such as censorship concerns, and to develop mechanisms to foster more decentralization in payment channel networks. The latter includes the design of alternative, incentive-compatible routing mechanisms.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data is publicly available and referenced in out article.

Acknowledgments

We acknowledge the Austrian Science Fund (FWF) and netIDEE SCIENCE project P 33775-N (ReactNet) and supported by the German Federal Ministry of Education and Research (BMBF), project 6G-RIC, grant 16KISK020K (6G-RIC), 2021–2025.

References

ACINQ homepage. (2023). https://acinq.co. [Online; accessed 31-March-2023].

Avarikioti, Z., Lizurej, T., Michalak, T., & Yeo, M. (2023). Lightning creation games. http://dx.doi.org/10.48550/arXiv.2306.16006, CoRR abs/2306.16006 2306.16006.

Azfar, O., Kahkonen, S., Lanyi, A., Meagher, P., & Rutherford, D. (2018). Decentralization, governance and public services: The impact of institutional arrangements. In *Devolution and development* (pp. 45–88). Routledge.

Bardhan, P., & Mookherjee, D. (1998). *Expenditure decentralization and the delivery of public services in developing countries*: *Center for international and development economics research (CIDER) working papers 233623*, University of California-Berkeley, Department of Economics, http://dx.doi.org/10.22004/ag.econ.233623, https://ideas.repec.org/p/ags/ucbewp/233623.html.

Beikverdi, A., & Song, J. (2015). Trend of centralization in bitcoin's distributed network. In *2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)* (pp. 1–6). IEEE.

1ML - bitcoin lightning analysis engine. (2019). https://1ml.com/. [Online; accessed 10-November-2019].

Bonneau, J. (2018). Hostile blockchain takeovers (short paper). In A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, & M. Sala (Eds.), *Lecture notes in computer science*: *vol. 10958*, *Financial cryptography and data security - FC 2018 international workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, revised selected papers* (pp. 92–100). Springer, http://dx.doi.org/10.1007/978-3-662-58820-8_7.

Brandes, U. (2008). On variants of shortest-path betweenness centrality and their generic computation. *Social Networks*, *30*(2), 136–145.

Core-lightning (CLN) GitHub repository. (2023). https://github.com/ElementsProject/lightning. [Online; accessed 31-March-2023].

Coindesk (2021). Why China's crackdown may make bitcoin mining more centralized. Online.

Core lightning presplit. (2023). https://github.com/ElementsProject/lightning/blob/master/plugins/libplugin-pay.c#L3410-L3442. [Online; accessed 31-March-2023].

Das, K., Samanta, S., & Pal, M. (2018). Study on centrality measures in social networks: a survey. *Social Network Analysis and Mining*, *8*(1), 13.

Dasaklis, T. K., & Malamas, V. (2023). A review of the lightning network's evolution: Unraveling its present state and the emergence of disruptive digital business models. *Journal of Theoretical and Applied Electronic Commerce Research*, *18*(3), 1338–1364. http://dx.doi.org/10.3390/jtaer18030068.

Decker, C. (2023). Lightning network research; topology datasets. http://dx.doi.org/10.5281/zenodo.4088530, https://github.com/lnresearch/topology. Accessed: 31-March-2023.

Donet, J. A., Pérez-Sola, C., & Herrera-Joancomartí, J. (2014). The bitcoin P2P network. In *International conference on financial cryptography and data security* (pp. 87–102). Springer.

Dotan, M., Pignolet, Y.-A., Schmid, S., Tochner, S., & Zohar, A. (2021). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Computing Surveys*, *54*(5), 1–34.

Dotan, M., Pignolet, Y., Schmid, S., Tochner, S., & Zohar, A. (2022). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Computing Surveys*, *54*(5), 107:1–107:34. http://dx.doi.org/10.1145/3453161.

Eclair GitHub repository. (2023). https://github.com/ACINQ/eclair. [Online; accessed 31-March-2023].

EmelyanenkoK (2020). Payment channel congestion via spam-attack. https://Github.Com/Lightningnetwork/Lightning-Rfc/Issues/182.

Forbes (2019). Bitcoin mining centralization is 'quite alarming', but a solution is in the works. Online.

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). Sok: Layer-two blockchain protocols. In *International conference on financial cryptography and data security* (pp. 201–226). Springer.

Hagberg, A. A., Schult, D. A., & Swart, P. J. (2008). Exploring network structure, dynamics, and function using networkx. In G. Varoquaux, T. Vaught, & J. Millman (Eds.), *Proceedings of the 7th python in science conference* (pp. 11–15). Pasadena, CA USA.

Harris, J., & Zohar, A. (2020). Flood & loot: A systemic attack on the lightning network. In *AFT* (pp. 202–213). New York, NY, USA: ACM.

Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., Miller, A., et al. (2021). An empirical analysis of privacy in the lightning network. arXiv:2003.12470 [cs].

Khalil, R., & Gervais, A. (2017). Revive: Rebalancing off-blockchain payment networks. In *Proc. ACM SIGSAC conference on computer and communications security (CCS)* (pp. 439–453).

Khamis, J., Schmid, S., & Rottenstreich, O. (2021). Demand matrix optimization for offchain payments in blockchain. In *2021 IEEE international conference on blockchain and cryptocurrency (ICBC)*. IEEE.

Lightning Network (2023). BOLT 7: P2P node and channel discovery. https://gitHub.com/lightningnetwork/lightning-rfc/blob/master/07-routing-gossip.md. [Online; accessed 31-March-2023].

Liu, Y.-Y., Slotine, J.-J., & Barabasi, A.-L. (2011). Controllability of complex networks. *Nature*, *473*, 167–173. http://dx.doi.org/10.1038/nature10011.

LND GitHub repository. (2023). https://github.com/lightningnetwork/lnd. [Online; accessed 31-March-2023].

Lockwood, B. (2002). Distributive politics and the costs of centralization. *Review of Economic Studies*, *69*(2), 313–337. http://dx.doi.org/10.1111/1467-937X.00207.

Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M., & Ravi, S. (2017). Concurrency and privacy with payment-channel networks. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 455–471).

Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., & Maffei, M. (2019a). Anonymous multi-hop locks for blockchain scalability and interoperability. In *26th annual network and distributed system security symposium (NDSS)*.

Malavolta, G., Moreno-Sanchez, P., Schneidewind, C., Kate, A., & Maffei, M. (2019b). Anonymous multi-hop locks for blockchain scalability and interoperability. In *26th annual network and distributed system security symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. Reston, Virgina, USA: The Internet Society.

Mislove, A., Lehmann, S., Ahn, Y., Onnela, J., & Rosenquist, J. N. (2011). Understanding the demographics of Twitter users. In *ICWSM*. Washington D.C, USA: The AAAI Press.

Mizrahi, A., & Zohar, A. (2021). Congestion attacks in payment channel networks. arXiv:2002.06564.v4 [cs].

Moreno-Sanchez, P., Kate, A., Maffei, M., & Pecina, K. (2015). Privacy preserving payments in credit networks: enabling trust with privacy in online marketplaces. In *22nd annual network and distributed system security symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*. Reston, Virgina, USA: The Internet Society.

Neudecker, T., & Hartenstein, H. (2018). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*, *21*(1), 838–857.

Nisslmueller, U., Foerster, K.-T., Schmid, S., & Decker, C. (2020). Toward active and passive confidentiality attacks on cryptocurrency off-chain networks. In *Proc. 6th international conference on information systems security and privacy (ICISSP)*.

Rohrer, E., Malliaris, J., & Tschorsch, F. (2019). Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. In *EuroS&P workshops* (pp. 347–356). Stockholm, Sweden: IEEE.

Rohrer, E., & Tschorsch, F. (2020). Counting down thunder: Timing attacks on privacy in payment channel networks. In *AFT* (pp. 214–227). Stockholm, Sweden: ACM.

Romiti, M., Victor, F., Moreno-Sanchez, P., Nordholt, P. S., Haslhofer, B., & Maffei, M. (2021). Cross-layer deanonymization methods in the lightning protocol. arXiv:2007.00764 [cs].

Rompert.com. (2023). https://rompert.com. [Online; accessed 31-March-2023].

Scellato, S., Mascolo, C., Musolesi, M., & Latora, V. (2010). Distance matters: Geo-social metrics for online social networks. In *WOSN*. Berkeley, USA: USENIX Association.

Seres, I. A., Gulyás, L., Nagy, D. A., & Burcsi, P. (2020). Topological analysis of bitcoin's lightning network. In *Mathematical research for blockchain economy* (pp. 1–12). Vilamoura, Portugal: Springer.

Shulman, R. (2019). Are centralized cryptocurrency regulations the answer? Three countries; three different directions. *Brooklyn Journal of International Law*, *45*, 835.

Stefano Martinazzi, A. F. (2020). The evolving topology of the lightning network: Centralization, efficiency, robustness, synchronization, and anonymity.

Tang, W., Wang, W., Fanti, G., & Oh, S. (2020). Privacy-utility tradeoffs in routing cryptocurrency over payment channel networks. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *4*(2), 1–39.

Tochner, S., Zohar, A., & Schmid, S. (2020). Route hijacking and DoS in off-chain networks. In *Proc. ACM conference on advances in financial technologies (AFT)*.

Tripathy, S., & Mohanty, S. K. (2020). Mappcn: Multi-hop anonymous and privacy-preserving payment channel network. In *International conference on financial cryptography and data security* (pp. 481–495). Springer.

(2019). Vivisecting blockchain P2P networks. https://api.semanticscholar.org/CorpusID:199597480.

Zabka, P., Foerster, K.-T., Schmid, S., & Decker, C. (2022). Empirical evaluation of nodes and channels of the lightning network. *Pervasive and Mobile Computing*, *83*, Article 101584.

Zabka, P., Förster, K., Schmid, S., & Decker, C. (2021). Node classification and geographical analysis of the lightning cryptocurrency network. In *ICDCN* (pp. 126–135). New York, NY, USA: ACM.

Philipp Zabka is a student at the University of Vienna, Austria, at the Faculty of Computer Science, currently finishing his master's degree. His research focuses on problems in networks and especially the Lightning Network.

Klaus-Tycho Foerster is a Professor for Networked and Distributed Systems at TU Dortmund, Germany, at the Faculty of Computer Science. His research focuses on fundamental problems of networked and distributed systems, especially software-defined networks, optical networks, resilience, consistency, and fault-tolerance.

Christian Decker is an early member of the Bitcoin community, and has written the first dissertation on the topic of blockchains with focus on Bitcoin. Part of his earlier work built the basis for the Lightning Network project, and he is still actively developing the Lightning Network protocol.

Stefan Schmid is a Professor for Internet Network Architectures at TU Berlin, Germany, in the Faculty of Electrical Engineering and Computer Science. His research focuses on the fundamental and algorithmic problems in networked and distributed systems.