Análise da Evolução Topológica da Rede Lightning de Canais de Pagamento

Gustavo Franco Camilo, Gabriel Antonio Fontes Rebello, Lucas Airam Castro de Souza, Maria Gradinariu Potop-Butucaru, Marcelo Dias de Amorim, Miguel Elias Mitre Campista, Luís Henrique Maciel Kosmalski Costa

Análise da Evolução Topológica da Rede Lightning de Canais de Pagamento

Gustavo F. Camilo[1], Gabriel Antonio F. Rebello[1,2], Lucas Airam C. de Souza[1], Maria Potop-Butucaru[2], Marcelo Dias Amorim[2], Miguel Elias M. Campista[1], Luís Henrique M. K. Costa[1]

[1]Grupo de Teleinformática e Automação
Universidade Federal do Rio de Janeiro (UFRJ)
[2]Sorbonne Université, CNRS, LIP6, F-75005 Paris, França

Resumo. *As redes de canais de pagamento (Payment Channel Networks - PCN) oferecem uma alternativa rápida, segura e distribuída para efetuar pagamentos, evitando os lentos mecanismos de consenso em correntes de blocos. Nessa nova tecnologia, a topologia da rede estabelecida entre canais de pagamentos influencia diretamente o desempenho, custo e o sucesso das transações dos participantes. Este artigo analisa a topologia da Rede Lightning, principal rede de canais de pagamentos da atualidade, avaliando e discutindo a evolução da rede. O artigo reconstrói o grafo da rede a partir de dados reais de um conjunto de mensagens de fofoca (gossip) de anúncios de canais e pagamentos coletadas entre janeiro de 2020 e agosto de 2021. Os resultados mostram uma forte tendência de centralização de renda e conectividade, em que 0,38% dos nós concentram 50% da capacidade da rede, expondo desta forma uma vulnerabilidade a ataques direcionados. Assim como na criptomoeda Bitcoin, a centralização encontrada na prática conflita diretamente com a proposta inicial de uma rede par-a-par, ou seja, descentralizada. Além disso, a baixa transitividade da rede compromete o uso de técnicas de rebalanceamento de canais, que contribuem para a estabilidade do sistema. Identifica-se assim a necessidade de novas políticas de conexão que priorizem maior descentralização e robustez da rede, além de priorizar a criação de ciclos para rebalanceamento efetivo de canais.*

1. Introdução

O rápido crescimento das criptomoedas como uma forma alternativa de meio de pagamento expõe o problema de escalabilidade das correntes de blocos públicas. Enquanto métodos tradicionais de pagamentos, como cartão de crédito, atingem taxas de 1.700 transações por segundo, as criptomoedas sofrem com baixa vazão, atingindo entre 7 e 15 transações por segundo em média nas redes Bitcoin e Ethereum, respectivamente [BitcoinWiki 2019]. Como consequência do baixo desempenho, usuários pagam altas taxas aos mineradores para priorização de transações. Em períodos de alta demanda de pagamentos na rede, o valor médio das taxas atinge altas quantias, chegando a mais de U$ 62 em abril de 2021 ($\approx$ R$ 321,74, utilizando a cotação do dia 20 de junho de 2022) [BitInfoCharts 2022]. Assim, o problema de escalabilidade das correntes de blocos torna desvantajosa e impraticável a utilização de criptomoedas para pagamentos rotineiros de baixo valor, em que é necessária rápida confirmação dos pagamentos.

As redes de canais de pagamento (*Payment Channel Networks* - PCN) apresentam uma solução para o problema de escalabilidade das criptomoedas [Poon e Dryja 2016]. Ao permitir que transações ocorram fora-da-corrente (*off-chain*) de maneira segura, descentralizada e com baixas tarifas, as PCNs evitam os lentos mecanismos de consenso e alcançam alta vazão de transações. As redes de canais de pagamento têm atraído a atenção tanto da academia [Sivaraman et al. 2020, Gudgeon et al. 2019, Rebello et al. 2021] quanto do público em

geral, tendo sido um dos motivos para o reconhecimento do Bitcoin como moeda corrente em El Salvador [CloudTweaks 2021]. Atualmente, a Rede Lightning, rede de canais de pagamentos do Bitcoin e principal PCN, possui mais de U$ $130.542.759$ ($\approx$ R$ $677.425.539,28$) alocados em mais de 86.000 canais públicos. Vale ressaltar que a Rede Lightning permite que canais existam sem serem divulgados por uma questão de privacidade. Assim, o número real de canais da rede pode ultrapassar o valor de 86.000.

O grande sucesso da Rede Lightning e sua consolidação como principal implementação de rede de canais de pagamento tornam fundamental analisar o seu crescimento, uma vez que o desempenho de propostas de roteamento e balanceamento de canais dependem das características topológicas da rede [Pickhardt e Nowostawski 2020, Khalil e Gervais 2017]. Apesar da topologia da Rede Lightning já ter sido explorada em outros trabalhos [Seres et al. 2020, Lin et al. 2020, Rohrer et al. 2019], poucos analisam o crescimento e evolução das métricas da rede. Ademais, devido ao rápido crescimento e alta dinamicidade da rede, que permite fácil abertura e fechamento de canais, algumas análises já se encontram defasadas em relação ao estado mais recente da rede [Seres et al. 2020, Lin et al. 2020]. Dessa maneira, a análise da evolução e das tendências da rede é essencial para avaliar a praticidade e viabilidade de propostas atuais e futuras em PCN. Com a avaliação do aspecto temporal através da evolução da rede, espera-se que a análise se torne mais atemporal.

Contribuições. Este trabalho avalia a evolução das métricas topológicas da Rede Lightning, analisando as tendências recentes e implicações no futuro da rede. O trabalho utiliza informações reais coletadas de mensagens de fofoca (*gossip*) da rede para reconstruir o grafo completo entre o período de janeiro de 2020 até agosto de 2021. A análise dos resultados é separada em duas etapas. Primeiro, o trabalho analisa o estado da rede em agosto de 2021, verificando a distribuição de renda e conectividade. Os resultados mostram que, apesar de propor o roteamento de transações de maneira totalmente distribuída, a Rede Lightning apresenta uma alta concentração tanto de renda quanto de conectividade em poucos nós, controlados por empresas. Segundo, o trabalho analisa a série temporal de métricas clássicas de teoria dos grafos e de redes complexas para avaliar a evolução e perspectiva da rede. A análise aponta que a Rede Lightning está se tornando ainda mais centralizada e que algumas técnicas propostas de rebalanceamento de canais são caras ou inviáveis para a maioria dos nós da rede. Os resultados também indicam a inviabilidade da utilização de técnicas atuais de rebalanceamento de canais para grande parte da rede. Além disso, o trabalho mostra a vulnerabilidade da rede simulando ataques direcionados e verifica que um ataque aos nós mais centrais da rede podem resultar em tarifas 30% mais caras ao usuário final. Por fim, o trabalho discute possíveis soluções para os desafios apresentados.

O trabalho é organizado da seguinte forma. A Seção 2 apresenta a tecnologia de canais de pagamento e a Rede Lightning, principal rede de canais de pagamento. A Seção 3 analisa o estado da Rede Lightning e as tendências da topologia da rede, discutindo as consequências e perspectivas da Rede Lightning. A Seção 4 discute os trabalhos relacionados. Por fim, a Seção 5 conclui o trabalho.

2. Redes de Canais de Pagamento e a Rede Lightning

Os canais de pagamento são uma tecnologia baseada em corrente de blocos que permite a dois usuários realizar pagamentos recorrentes entre si de forma privada e em tempo real. A premissa principal dessa tecnologia é que o protocolo de consenso, apesar de ser o principal mecanismo que garante a segurança da corrente de blocos, também é o principal causador de atrasos e tarifas excessivas no sistema. Assim, o sistema deve realizar o máximo possível de

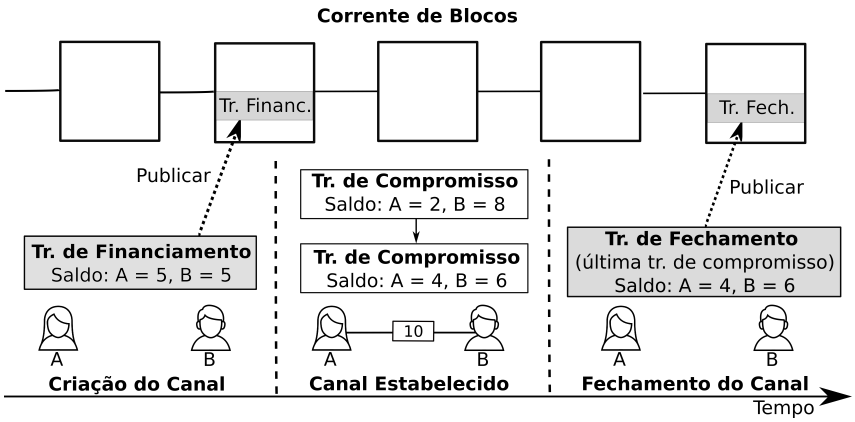


Figura 1: Estabelecimento de um canal de pagamento entre dois usuários. Após publicarem uma transação de financiamento que reserva uma quantia em *tokens*, os usuários podem emitir múltiplas transações de compromisso que realocam o saldo reservado. Ao final, uma das partes pode publicar a última transação de compromisso para encerrar o canal.

transações diretamente entre as partes envolvidas, sem a publicação em um bloco, e utilizar o protocolo de consenso apenas quando for necessário. As transações "fora-da-corrente" necessitam apenas de uma assinatura de cada parte envolvida.

A Figura 1 ilustra o processo de estabelecimento de um canal de pagamento em um sistema de corrente de blocos. No momento de abertura do canal de pagamento, dois usuários, A e B, devem assinar e publicar uma transação que reserva uma quantidade de *tokens* em um endereço de carteira compartilhado por ambos. Uma vez publicada a transação inicial de financiamento (*funding transaction*), A e B são capazes de rebalancear os fundos do endereço trocando transações de compromisso (*commitment transactions*) entre si de forma privada. Dessa forma, os dois usuários podem realizar pagamentos diretamente, dentro do limite reservado, de forma instantânea e sem pagar tarifas para os mineradores da corrente de blocos. Quando desejarem fechar o canal, A ou B podem publicar a transação de confirmação mais recente na corrente de blocos e aguardar o atraso do protocolo de consenso para recuperar seus *tokens* investidos no canal. Essa abordagem permite realizar pagamentos recorrentes do dia-a-dia, como compras semanais em mercados, pagamento de serviços mensais, entre outros, que exigem agilidade e possuem baixo valor.

Como a abertura de um canal de pagamento reserva *tokens* que não podem ser utilizados na corrente de blocos, torna-se inviável abrir canais de pagamentos com todos usuários da rede. Logo, usuários utilizam canais já estabelecidos para rotear pagamentos através de intermediários. O conjunto dos canais de pagamento estabelecidos entre usuários do sistema forma uma rede de canais de pagamento (*Payment Channel Network* - PCN), ilustrada na Figura 2. Cada enlace possui uma capacidade, ilustrada dentro do retângulo sobre a aresta na figura, que indica o total de *tokens* reservados pelas partes naquele canal. Essa informação é acessível e fica armazenada na transação de financiamento publicada na corrente de blocos. Os saldos de cada parte do canal, representados pelos números em cada extremo da aresta, indicam o estado atual do enlace. Os saldos são privados às partes envolvidas por motivos de segurança, uma vez que pagamentos poderiam ser rastreados se os saldos fossem públicos, e de escalabilidade, já que seria necessário inundar a rede com mensagens de atualização a cada pagamento.

A principal característica de uma rede de canais de pagamento é permitir através de roteamento que os usuários alcancem destinos que não constam na sua lista de canais de pa-

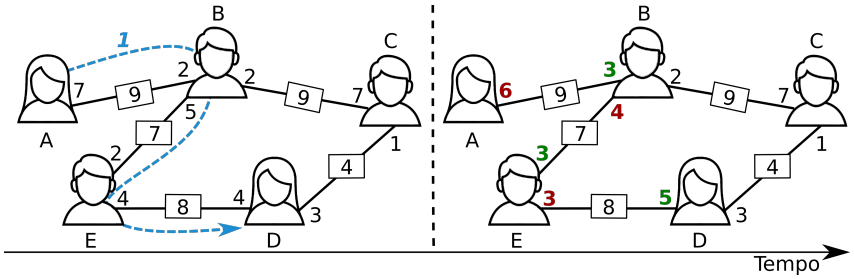


Figura 2: Um exemplo de pagamento de 1 *token* ocorrendo de um usuário A para um usuário D em uma rede de canais de pagamento. O pagamento percorre o trajeto indicado pelo remetente, modificando os saldos em cada canal no caminho. As capacidades dos canais, indicadas nos retângulos, representam o total reservado pelas duas partes e são constantes durante todo o tempo de vida do canal.

gamento estabelecidos. Isso permite que usuários realizem também transações não-recorrentes com agilidade e baixo custo. Se um usuário A deseja enviar um *token* para um destino D com o qual não compartilha um canal, ele pode encontrar um caminho na rede que leva até o destino e enviar o *token* através desse caminho. Os usuários intermediários agem como roteadores, encaminhando o pagamento até o próximo usuário no caminho. Cada intermediário cobra uma tarifa de roteamento pelo serviço de encaminhamento. Contratos bloqueados por tempo e *hash* (*Hashed Timelock Contracts - HTLC*), um tipo especial de contrato inteligente, impossibilitam o roubo de *tokens* ao garantir que os intermediários comprometam seus *tokens* com o próximo salto antes de receber os *tokens* do salto anterior. Assim, o roteamento em redes de canais de pagamento é diferente das redes de dados na Internet porque o pagamento só pode ser completado se todos os intermediários tiverem saldo suficiente para transferir os *tokens* necessários.

2.1. A Rede Lightning

A criptomoeda Bitcoin, além de ter sido pioneira na implementação da tecnologia de correntes de blocos, também deu origem à primeira e maior implementação da tecnologia de redes de canais de pagamento. A Rede Lightning (*Lightning Network*) realizou sua primeira transação em 2017 e atingiu a marca de mais de 13.000 nós e 86.000 canais de pagamento distribuídos pelo mundo atualmente. O número de nós e canais triplicou entre janeiro de 2020 e agosto de 2021, como ilustrado na Figura 3. A Rede Lightning é hoje a principal implementação de canais de pagamento existente e, portanto, este trabalho a utiliza como referência para a análise de redes de canais de pagamento no geral.

A Rede Lightning padroniza os formatos de mensagens e protocolos utilizados na rede através das bases da tecnologia Lightning (*Basis of Lightning Technology* - BOLT), documentos inspirados nas RFCs da Internet que descrevem formalmente como a rede deve ser implementada. Em particular, o documento BOLT 2 prevê a divulgação de canais através de mensagens de anúncio de canal (*channel announcement*) que a rede difunde no modelo de fofoca (*gossip*) [Poon e Osuntokun 2021]. No protocolo de fofoca, um participante divulga uma mensagem a um número específico de vizinhos, que repetem a mensagem aos próprios vizinhos. O procedimento continua até a informação atingir toda a rede. Os nós da rede são capazes de construir, a partir das mensagens recebidas, uma topologia local contendo os canais ativos com seus respectivos participantes e capacidades. Este trabalho aproveita-se dessa característica para obter o conjunto de mensagens recebidas em um dos nós da rede e reconstruir a topologia em diversos momentos da história. Assim, é possível extrair conhecimento sobre o comportamento da rede ao analisar a evolução de métricas-chave de grafos ao longo do tempo.

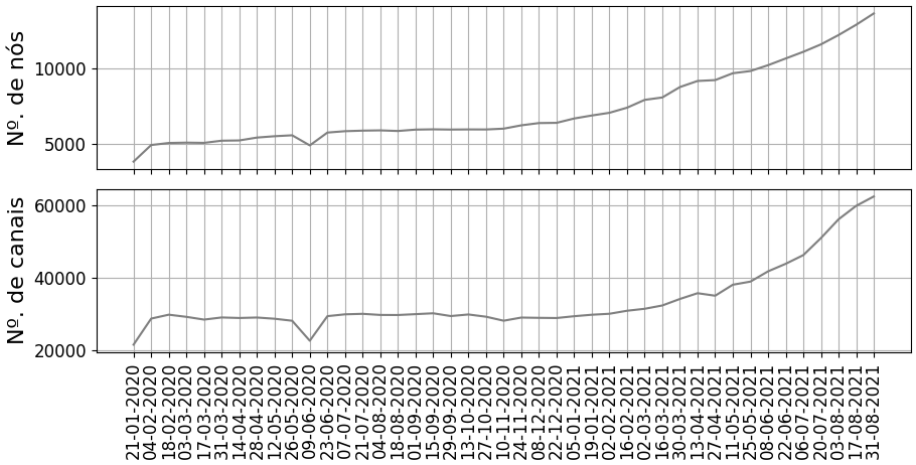


Figura 3: Crescimento da Rede Lightning entre os meses de janeiro de 2020 e agosto de 2021. O número de nós e de canais de pagamento triplicou.

3. Análise da Rede Lightning

O roteamento padrão da Rede Lightning é baseado na fonte (*source-based routing*). Assim, a rede requer que os nós conheçam a topologia completa da rede para efetuar pagamentos, o que é possível a partir das mensagens de anúncio. Este trabalho utiliza um conjunto de dados coletado por desenvolvedores da Rede Lightning de mensagens de anúncio transmitidas utilizando um protocolo de fofoca para sincronização dos nós da topologia da Rede Lightning [Decker 2021]. O conjunto de dados contém três tipos de mensagens coletadas por um nó através da implementação da Rede Lightning em linguagem C, `c-lightning`: (i) mensagens de anúncio de canal, que tornam um canal público na rede; (ii) mensagens de atualização de canal, utilizadas para informar e atualizar os parâmetros de um determinado canal e; (iii) mensagens de anúncios de nós, utilizadas para informar os metadados de um nó da rede. A implementação `c-lightning` automaticamente remove mensagens duplicadas. Assim, para a criação do conjunto de dados, as mensagens puras (*raw*) foram armazenadas em um arquivo. O arquivo contém mensagens da Rede Lightning de agosto de 2018 até agosto de 2021. Como o período de 2018 e 2019 já foi coberto por outros artigos [Seres et al. 2020, Lin et al. 2020], este trabalho considera o período entre janeiro de 2020 e agosto de 2021. Todas as mensagens possuem uma estampa de tempo que informa o momento em que foram criadas utilizando a base de tempo dos sistemas UNIX. Assim, utilizando uma janela de tempo, é possível reconstruir a topologia da Rede Lightning em qualquer instante de tempo. Este trabalho utiliza janelas saltitantes de duas semanas para análise da topologia, i.e., desconsidera mensagens anteriores a um período de duas semanas ao reconstruir a rede em um determinado instante.

Uma rede de canais de pagamento pode ser representada por um grafo não-direcionado $\mathbb{G} = (\mathbb{V}, \mathbb{E})$, em que $\mathbb{V}$ é o conjunto de nós da rede e $\mathbb{E}$ é o conjunto de canais de pagamento. Cada aresta $e_i \in \mathbb{E}$ possui um conjunto de atributos relacionado ao canal de pagamento, como capacidade de roteamento, tarifa cobrada para rotear pagamentos e os nós $v_1, v_2 \in \mathbb{V}$ que compõem o canal. Ao modelar a PCN como um grafo, é possível extrair informações úteis da rede, como a preferência de conexão de novos nós e o grau de centralização, a partir de métricas clássicas de teoria dos grafos e redes complexas [Li et al. 2005]. Este trabalho utiliza a biblioteca NetworkX v2.6.1 e Python 3.8 para processar as mensagens e reconstruir os grafos.

Estado da rede. O primeiro conjunto de experimentos verifica o estado mais atual do conjunto de dados de mensagens, de 17 a 31 de agosto de 2021, para estimar a concentração de renda e conectividade na Rede Lightning. A Figura 4 mostra a distribuição da capacidade de

roteamento dos canais na rede. A capacidade de roteamento do canal é o total de *tokens* alocados pelas duas partes durante sua criação. É possível perceber uma intensa concentração da capacidade na rede, em que poucos canais possuem alta capacidade e múltiplos canais possuem baixa capacidade. A capacidade dos canais é fator decisivo para o roteamento de transações. A baixa quantidade de canais de alto valor, p. ex., somente 13 canais ($0,02\%$ da rede) com capacidade acima de R\$ $200.000,00$ ($\approx$ 2 BTC), restringe a quantidade de caminhos que pagamentos de alto valor podem utilizar. Apesar do valor parecer alto, pagamentos de 2 BTC ou mais não são incomuns na Rede Bitcoin [Blockchain.com 2022]. Ao concentrar os canais de alta capacidade em poucos caminhos, a maior parte da rede deve recorrer à corrente de blocos para efetuar pagamentos de alto valor, passando por alto tempo de confirmação e altas tarifas.

A Figura 4 mostra a relação entre a centralidade de grau de nós da rede e a capacidade de roteamento do nó na rede. O grau de um nó indica a quantidade de canais de pagamento dos quais ele faz parte. A distribuição dos graus indica que a Rede Lightning se comporta como uma rede sem-escala (*scale-free*), em que poucos nós concentram grande parte das conexões da rede [Li et al. 2005, Seres et al. 2020]. É possível perceber que os nós de maior grau, em geral, apresentam maior capacidade de roteamento. Isso acontece porque novos nós tendem a se conectar a nós com alta capacidade de roteamento para efetuar pagamentos. Assim como no caso da capacidade da rede, os nós de maior grau são em sua maioria controlados por empresas ligadas ao Bitcoin e outras criptomoedas, como ACINQ, CoinGate e WalletOfSatoshi. Essas empresas operam nós na Rede Lightning, alocando alta quantia de dinheiro em seus canais, buscando coletar tarifas de roteamento de transações. Entretanto, a centralização em poucos nós torna a rede altamente dependente desses nós e a expõe a diversas vulnerabilidades de segurança, como ataques direcionados de negação de serviço (*Denial of Service* - DoS) e ataques de particionamento da rede.

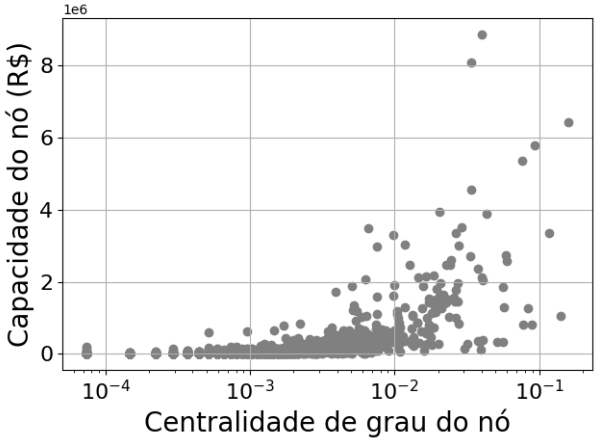


Figura 4: Relação entre o grau de um nó e a capacidade do nó na Rede Lightning.

A concentração do poder de roteamento fica ainda mais evidente ao remover os nós de maior grau. A Figura 5 simula um ataque direcionado aos nós de maior grau da rede, removendo-os e ilustrando as consequências deste ataque. Na Rede Lightning, essa remoção significa fechar todos os canais de um nó ou tornar o nó indisponível para roteamento durante um intervalo de tempo através de um ataque de DoS. A remoção de 49 nós, aproximadamente $0,38\%$ da rede, é o suficiente para reduzir a capacidade da rede pela metade. Um possível ataque desse tipo afeta toda a rede, aumentando a probabilidade de falhas por falta de caminhos disponíveis com capacidade suficiente. O experimento similar de Seres *et al.* na Rede Lightning mostra que, em 2019, bastava remover 37 nós para reduzir a capacidade da rede pela

metade [Seres et al. 2020]. Vale ressaltar, no entanto, que no período avaliado por Seres *et al.*, a rede possuía apenas 2.344 nós. Mesmo após o número de nós da rede mais que triplicar até agosto de 2021, a rede ainda é extremamente vulnerável a ataques direcionados aos nós mais centrais. Além disso, a remoção de 100 nós, aproximadamente $0,74\%$ da rede, aumenta em aproximadamente 32% a tarifa base paga pelo usuário final. O valor da tarifa base média paga pelo usuário é calculada a partir do aumento do número de saltos médio ao remover os nós. Como a tarifa base é fixa e paga a cada salto, é possível verificar o efeito financeiro deste tipo de ataque ao usuário final. É importante ressaltar que a possibilidade de ataques desse tipo não é somente teórica. A Rede Lightning já sofreu um ataque de negação de serviço que afetou 20% dos nós da rede, tornando-os indisponíveis para roteamento [TrustNodes 2018]. Dessa maneira, um ataque direcionado aos nós de maior grau da rede afeta diretamente todos os participantes, que passam a pagar mais tarifas devido ao aumento médio do caminho, além de aumentar a probabilidade de falhas devido à falta de capacidade para rotear.

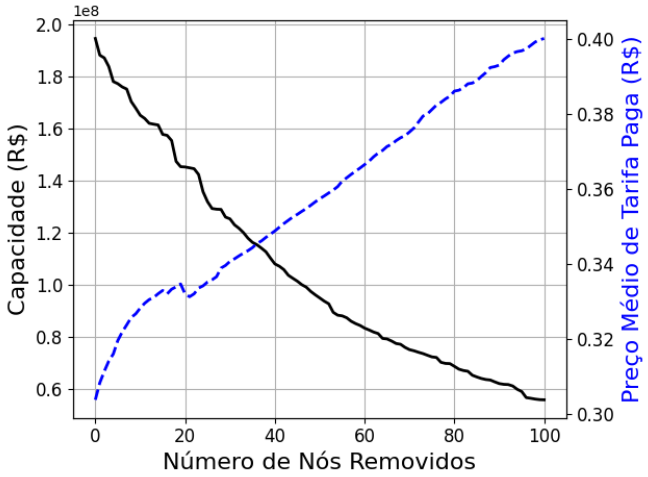


Figura 5: Capacidade e tarifa base média ao remover os nós de maior grau.

Evolução e Tendências da Rede. O segundo conjunto de experimentos verifica a evolução das métricas da rede para avaliar se o grau de concentração da rede vem aumentando. Os experimentos avaliam a rede no período entre 21 de janeiro de 2020 e 31 de agosto de 2021. A Figura 6 mostra a evolução das métricas da Rede Lightning. Todas as métricas consideram apenas o maior componente do grafo, exceto o resultado de número de componentes. Apesar do número de componentes na rede crescer de 6 para 53 durante o período avaliado, como mostra a Figura 6a, o número de nós dos menores componentes é insignificante se comparado ao número de nós do maior componente. Como exemplo, a imagem (*snapshot*) da rede com maior número de componentes possui 13.462 nós no maior componente, enquanto os menores componentes possuem no máximo 3 nós. Dessa maneira, utilizar somente o maior componente não afeta a confiabilidade dos resultados, uma vez que os menores componentes não efetuam pagamentos com mais de 1 salto e não conseguem atender as demandas da maior parte da rede. Vale ressaltar que o aumento do número de componentes é natural devido ao crescimento do número de nós da rede. Alguns nós estabelecem conexões entre si para efetuar pagamentos recorrentes e não buscam estabelecer conexões com outros participantes.

A assortatividade r de um grafo indica a preferência de conexão dos nós na rede. Um grafo dissortativo apresenta $r < 0$, indicando que os nós de baixo grau da rede preferem conectar-se a nós de alto grau, enquanto um grafo assortativo possui $r > 0$, indicando que nós de alto grau preferem conectar-se a nós de alto grau. O coeficiente de assortatividade da

rede, na Figura 6b, mostra que a Rede Lightning é disassortativa, indicando que nós de baixo grau tendem a se conectar a nós de alto grau. Isso acontece porque algumas implementações da Rede Lightning, como o LND, apresentam políticas de preferência de conexão de novos nós a nós mais centrais da rede [Seres et al. 2020]. Esta preferência faz sentido, pois nós que pretendem efetuar pagamentos a mais de uma entidade podem priorizar a conexão a nós mais centrais, buscando menores caminhos e tarifas. Apesar da disassortatividade da rede, é possível perceber o crescimento dessa métrica, apontando para uma rede assortativa no futuro. Isso pode ser explicado pelo estabelecimento de conexão entre os *hubs* centrais após se consolidarem, aumentando a assortatividade. A tendência de subida na assortatividade pode ser explicada pelo surgimento de novos *hubs* em consequência do rápido crescimento da rede.

A transitividade de um grafo mede a fração de *loops* existentes na rede em relação às tríades, número de *loops* que poderiam existir na rede. As tríades são medidas pela contagem do número de duas arestas $(e_1, e_2) \in \mathbb{E}$ que compartilham o mesmo vértice $v_1 \in \mathbb{V}$. Dessa maneira, a medida de transitividade considera somente *loops* de três nós e varia entre zero e um. Um grafo de transitividade zero não apresenta caminhos fechados com 2 saltos, como grafos em topologia estrela e grafos acíclicos direcionados, enquanto grafos de transitividade um apresentam perfeita transitividade. A transitividade T de um grafo pode ser medido por

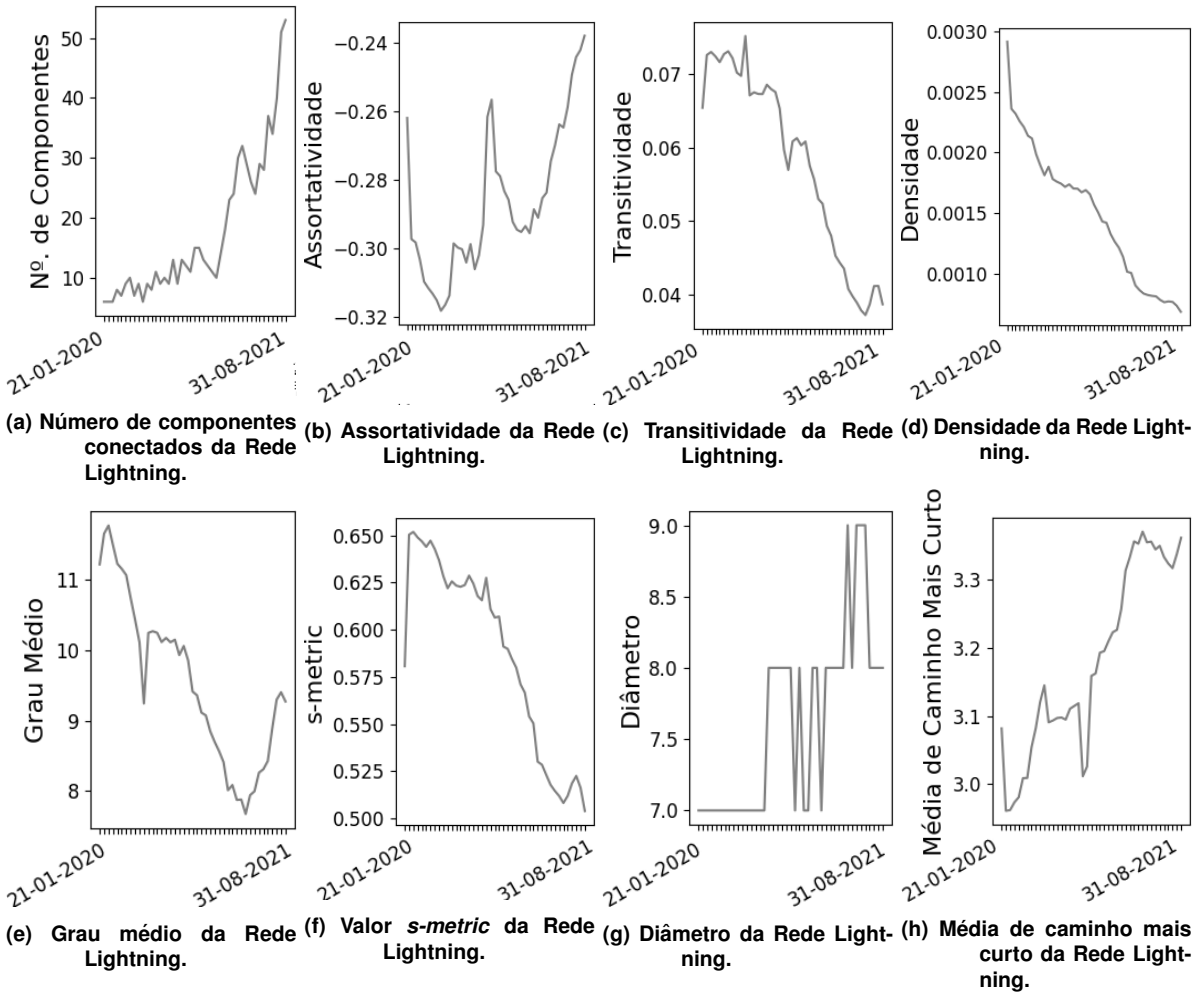
$$T = 3\frac{l_3}{t}, \tag{1}$$

em que l_3 é o número de *loops* entre 3 nós na rede e t é o número de tríades na rede. Nas redes de canais de pagamento, o estabelecimento de ciclos de poucos saltos é crucial para o barateamento de algumas propostas de rebalanceamento de canais [Pickhardt e Nowostawski 2020, Khalil e Gervais 2017]. Essas propostas se aproveitam de ciclos para que um nó possa efetuar pagamentos a si mesmo, rebalanceando os caminhos e movimentando dinheiro entre canais. Ademais, manter canais balanceados é de extrema importância para aumentar a probabilidade de sucesso de uma transação [Sivaraman et al. 2020]. Entretanto, a baixa transitividade , apresentada na Figura 6c e sua tendência de queda na rede apontam a existência de poucos ciclos de 3 nós, o que torna as propostas caras e possivelmente inviáveis para a maioria dos participantes que possuem baixo poder financeiro. Essa baixa transitividade é consequência natural do estabelecimento de conexões entre nós de baixo grau a nós de alto grau, gerando diversas possibilidades de ciclos que não são formados. A topologia centralizada tende a uma estrutura núcleo-periferia, na qual a maioria dos nós está nas extremidades, i.e., na periferia. Dessa forma, esses nós possuem somente um vizinho, o que não contribui com a formação de triângulos na rede, abaixando a transitividade. Assim, apenas os *hubs* centrais podem se aproveitar da sua própria alta conectividade para utilização de técnicas de rebalanceamento.

A densidade de um grafo é medida pela fração das arestas existentes no grafo e as arestas de uma grafo completo com o mesmo número de nós. Assim, a densidade de um grafo não-direcionado pode ser calculada por

$$d = \frac{m}{n(n-1)}, \tag{2}$$

em que m é o número de arestas na rede e n é o número de nós. A baixa densidade observada na Figura 6d mostra que a Rede Lightning é uma rede extremamente esparsa. A tendência de queda da densidade também pode ser explicada pela conexão de novos nós a nós mais centrais. Esse tipo de comportamento é comum em redes sem-escala (*scale-free*), em que uma pequena parte dos nós concentra grande parte das conexões [Li et al. 2005]. O comportamento da Rede Lightning como rede sem-escala também pode ser observado na queda do grau médio da rede



(a) Número de componentes conectados da Rede Lightning.
(b) Assortatividade da Rede Lightning.
(c) Transitividade da Rede Lightning.
(d) Densidade da Rede Lightning.
(e) Grau médio da Rede Lightning.
(f) Valor *s-metric* da Rede Lightning.
(g) Diâmetro da Rede Lightning.
(h) Média de caminho mais curto da Rede Lightning.

Figura 6: Evolução das métricas de grafos da Rede Lightning. Os resultados compreendem o período desde 21 de janeiro de 2020 até 31 de agosto de 2021.

e pelo resultado da s-metric, como mostram as Figuras 6e e 6f. A entrada de nós com somente uma conexão contribui para a queda do grau médio da rede mesmo com o aumento do grau dos nós mais centrais. A s-metric varia de zero a um e mede o quanto um grafo possui um núcleo de nós que aumenta a conectividade da rede, se assemelhando a um *hub* [Li et al. 2005]. É possível perceber que, apesar da queda na s-metric, a Rede Lightning ainda apresenta uma concentração de conectividade em poucos nós, como mostra a Figura 6e.

As Figuras 6g e 6h expõem o baixo diâmetro e média de caminho mais curto na Rede Lightning. O diâmetro de um grafo é definido pelo maior caminho mais curto entre qualquer par de nós. Já o caminho médio mais curto é obtido através do somatório da distância mínima para cada par de vértices do grafo dividido pela quantidade total de vértices. É possível perceber que, apesar do número de nós da rede triplicar no período, as duas métricas apresentam baixa variação se comparadas às outras métricas, variando em 28% no caso do diâmetro e aproximadamente 15% no caso do caminho mais curto.

A tendência de centralização fica ainda mais clara ao analisar a Figura 7, que mostra a concentração de renda dos nós ao longo do tempo. É possível perceber que, enquanto em janeiro de 2020 aproximadamente $2,0\%$ e $0,9\%$ dos nós concentravam 80% e 50% da capacidade total da rede, respectivamente, os números caíram para $1,1\%$ e $0,3\%$ em agosto de 2021. A tendência de queda, ainda que lenta, mostra que cada vez menos nós concentram grande parte da renda

alocada e expõe futuras vulnerabilidades e desafios de segurança na rede.

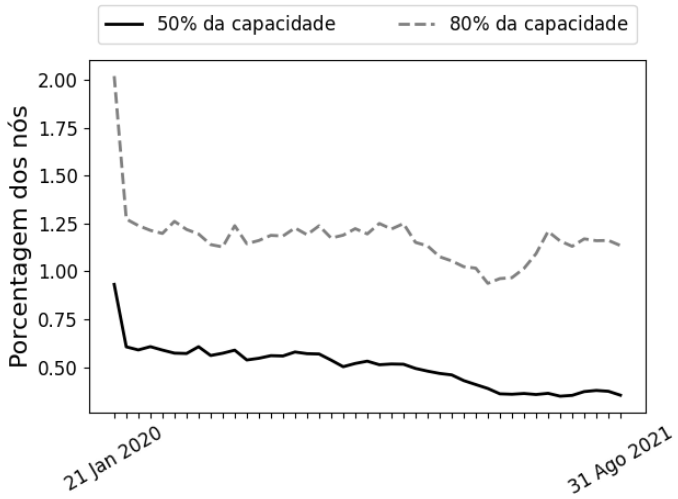


Figura 7: Concentração de renda na Rede Lightning de janeiro de 2020 a agosto de 2021. Os traços indicam a porcentagem dos nós que concentram 50% e 80% da capacidade total da rede em cada período de duas semanas.

Por fim, o último conjunto de experimentos verifica a evolução das características dos canais da rede. A Figura 8 ilustra a variação da capacidade e das tarifas cobradas pelos nós. A Rede Lightning apresenta dois tipos de tarifa: tarifa base e tarifa proporcional. Nós intermediários coletam a tarifa base de cada pagamento roteado independentemente do valor do pagamento. Por outro lado, a tarifa proporcional depende do valor do pagamento e é cobrada a cada 1 milhão de satoshis ($\approx$ R$\$$ $1.000{,}00$) roteado. As políticas de tarifa dos nós podem ser modificadas utilizando mensagens de atualização de canal, como definido pelo BOLT 2 [Poon e Osuntokun 2021], o que explica a variação da média das tarifas, chegando a mais de R$\$1{,}40$ em períodos de alta demanda. Apesar da variação, as tarifas da Rede Lightning são, em geral, muito menores que a média das tarifas da Rede Bitcoin, que alcançou mais de U$\$$ $60{,}00$ (R$\$$ $311{,}36$, utilizando a cotação em 20 de junho de 2022) em abril de 2021 [BitInfoCharts 2022]. Dessa maneira, a Rede Lightning cumpre a promessa de ser uma alternativa mais barata e vantajosa para transferências de baixo valor em criptomoedas.

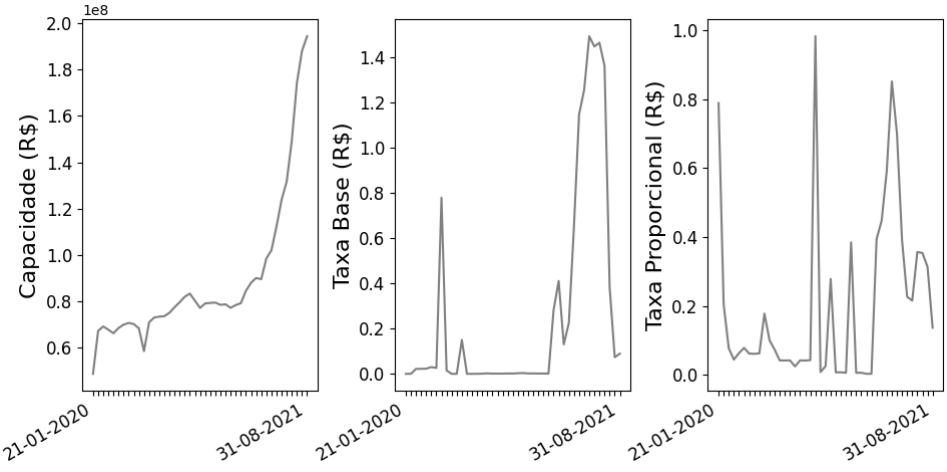


Figura 8: Evolução da média das características dos canais ao longo do tempo. Os resultados apresentados compreendem o período de 21 de janeiro de 2020 até 31 de agosto de 2021 com intervalo de duas semanas entre as medidas.

Discussão. Apesar de se propor como uma alternativa descentralizada para pagamentos rápidos em correntes de blocos, os resultados mostram uma clara centralização de renda e conectividade da rede. A concentração de renda fica evidente ao analisar a distribuição da capacidade e dos graus dos canais na Figura 4. Nós de maior capacidade detêm o monopólio do roteamento de pagamentos de alto valor na rede, se tornando ainda mais ricos por coletar mais tarifas. Estes nós de maior capacidade atraem conexões de novos participantes, formando *hubs*, uma vez que novos participantes buscam abrir canais em um local que possam chegar a múltiplos destinos em poucos saltos. Dessa maneira, os participantes escolhem se conectar aos nós mais centrais buscando diminuir a tarifa de roteamento paga ao efetuar um pagamento.

A baixa conectividade de nós na periferia também inviabiliza ou encarece propostas que se aproveitam de ciclos para rebalancear canais na prática. Essas propostas ficam limitadas aos nós mais centrais, que possuem maior conectividade e probabilidade de encontrar caminhos com ciclos para rebalanceamento. Enquanto os nós de maior conectividade conseguem facilmente rebalancear os próprios canais utilizando a topologia da rede, grande parte dos participantes da rede deve utilizar a corrente de blocos. Este fenômeno acentua ainda mais a desigualdade na rede, uma vez que os nós centrais tem possibilidade reduzida de passar por períodos de indisponibilidade de roteamento ao aguardar confirmação de transação na corrente de blocos e tampouco pagam altas tarifas para rebalancear os próprios canais.

A evolução das métricas aponta para uma continuidade da centralização da Rede Lightning, com os nós centrais ganhando ainda mais influência. Possíveis ataques direcionados a esses *hubs*, como o ataque de particionamento (*split attack*) [Lin et al. 2020] e ataques de negação de serviço possuem consequências catastróficas para a rede [Rohrer et al. 2019, Tikhomirov et al. 2020]. Grande parte dos nós da rede teria que pagar mais tarifas, devido ao aumento do caminho mais curto, e sofrer com falhas de pagamento, devido à redução da capacidade de roteamento da rede.

Possíveis soluções para o problema de centralização incluem propostas de conexões que privilegiam a distribuição da conectividade na abertura de canais. Nesse caso, a criação de caminhos alternativos na rede garante uma menor dependência dos nós periféricos em relação aos nós centralizados e reduz os efeitos de um ataque de particionamento na rede. Ademais, a conexão de novos nós criando ciclos na topologia diminui o impacto de problemas relacionados à baixa transitividade, como o rebalanceamento de canais através da topologia da rede. Assim, gerar ciclos na abertura de canais garante que nós possam rebalancear seus canais sem necessidade de recorrer à corrente de blocos. Esta solução, no entanto, apresenta um compromisso (*trade-off*). Ao modificar a preferência da conexão dos nós a nós periféricos, a rede ganha em robustez a alguns ataques direcionados, mas também cresce em diâmetro, resultando em caminhos mais longos e mais tarifas pagas pelo usuário final. Por fim, forçar a criação de ciclos beneficia propostas de rebalanceamento de canais, que podem aumentar a probabilidade de sucesso de um pagamento. No entanto, o participante deve reservar quantias nos dois canais, o que pode sair caro para usuários do dia-a-dia. É importante que a criação de novas políticas de preferências de conexão considere este compromisso.

4. Trabalhos Relacionados

O rápido crescimento das redes de canais de pagamento tem motivado diversos trabalhos de pesquisa. A maioria dos trabalhos busca solucionar problemas relacionados ao roteamento eficiente de transações [Sivaraman et al. 2020, Prihodko et al. 2016], segurança e privacidade em PCNs [Malavolta et al. 2016, Roos et al. 2017, Rebello et al. 2021], além de rebalanceamento de canais [Pickhardt e Nowostawski 2020, Khalil e Gervais 2017]. Devido às

características do roteamento de pagamento de transações em uma PCN, a proposta de algoritmos eficientes e seguros de roteamento e balanceamento dependem fortemente da topologia da rede. Nesse cenário, o conhecimento das características topológicas de uma PCN, como a Rede Lightning, é imprescindível para avaliação da praticidade e da viabilidade de propostas.

Outros trabalhos exploram a topologia da Rede Lightning [Seres et al. 2020, Lin et al. 2020, Rohrer et al. 2019, Beres et al. 2019]. Seres *et al.* analisam a topologia da Rede Lightning utilizando métricas de grafos e uma imagem da rede de janeiro de 2019 [Seres et al. 2020]. Os autores avaliam a robustez da rede a ataques direcionados aos nós de maior grau e verificam uma forte centralização de conectividade. A partir da análise, os autores concluem que a Rede Lightning apresenta comportamento similar a redes sem-escala e redes de mundo pequeno, além de apresentar robustez contra ataque de falhas aleatórias e vulnerabilidades a atacantes racionais. Os autores avaliam somente o estado da rede em janeiro de 2019, sem considerar o crescimento histórico. Devido ao rápido crescimento e à alta dinamicidade da rede, os resultados são limitados à data avaliada e não consideram as perspectivas de crescimento da rede que estão em constante mudança, como demonstrado no presente trabalho. Além disso, a análise de Seres *et al.* não considera alguns parâmetros financeiros, como as tarifas pagas pelos usuários e o efeito direto de ataques direcionados ao usuário final.

Lin *et al.* avaliam o crescimento da Rede Lightning em relação à concentração de renda da rede [Lin et al. 2020]. Os autores avaliam índices como Gini, centralidade de proximidade e centralidade de intermediação da rede no período entre janeiro de 2018 e julho de 2019. Os resultados mostram que a rede apresenta estruturas do tipo núcleo-periferia em que o núcleo é formado por *hubs* e subestruturas do tipo estrela, verificando uma forte centralização na rede em torno dos nós de maior capacidade. Os autores expõem que a remoção de *hubs* levaria ao particionamento da rede em múltiplos componentes, deixando a rede mais vulnerável a ataques. Similar a Lin *et al.*, Beres *et al.* analisam métricas da Rede Lightning, como número de arestas, grau médio e transitividade, no período entre janeiro de 2018 e maio de 2019 [Beres et al. 2019] para a construção de um simulador de tráfego. Os artigos, no entanto, são limitados à análise de poucas métricas de centralização, desconsiderando os aspectos específicos, como evolução da densidade, componentes, s-metric e assortatividade, além da evolução e distribuição das características dos canais, como tarifas cobradas e capacidade. Essas métricas permitem uma maior compreensão do estado da rede e as suas perspectivas.Também utilizando uma análise temporal, Zabka *et al.* apresentam uma classificação para o tipo de nó da Rede Lightning e analisam a distribuição geográfica dos participantes da rede [Zabka et al. 2021]. A partir da análise da localização dos nós, os autores observam uma correlação entre conexões de canais e países que possuem a língua em comum. Rohrer *et al.* focam na análise de segurança, quantificando a resiliência da Rede Lightning a ataques baseados na topologia [Rohrer et al. 2019]. O resultado mostra que atacantes com recursos disponíveis devem seguir a estratégia de remoção de nós de maior centralidade para efetuar ataques efetivos, enquanto nós com baixo recurso devem focar em canais de baixa capacidade cuja remoção particiona o grafo. Em outro artigo, os autores utilizam conhecimentos de teoria dos grafos para analisar as estratégias de conexão de nós na rede [Lange et al. 2021]. Os autores avaliam múltiplas estratégias e suas consequências em curto e longo prazo e expõem um compromisso entre centralização e eficiência no roteamento de pagamentos pela rede.

Diferentemente dos artigos citados, este trabalho avalia a evolução de centralização da Rede Lightning a partir de métricas de grafos e redes complexas, além de avaliar o resultado de ataques direcionados e seus efeitos aos usuários finais. A análise utiliza dados reais coletados de mensagens da Rede Lightning entre o período de janeiro de 2020 a agosto de 2021 e avalia a

tendência de centralização de conectividade e renda da rede, além de discutir as consequências e tendências do modelo de crescimento atual da rede para propostas futuras.

5. Conclusão

As redes de canais de pagamento apresentam um mecanismo fundamental para permitir pagamentos rápidos, seguros e descentralizados de criptomoedas no dia-a-dia. Devido à forma como o roteamento de pagamentos através de canais de pagamento é implementado, as PCNs são influenciadas pela sua topologia. Este trabalho analisa a evolução da topologia da Rede Lightning, principal rede de canais de pagamento, utilizando métricas de teoria dos grafos e mensagens reais coletadas da rede. Os resultados mostram que as conexões e capacidade alocada para a rede são extremamente concentradas em poucos nós, que em sua maioria são controlados por empresas ligadas ao desenvolvimento de corrente de blocos. Essa centralização é consequência natural de como se dá a entrada de novos participantes, que buscam menores caminhos para efetuar transações e, consequentemente, pagar menores tarifas. Entretanto, a concentração de muitos canais em poucos nós não é compatível com a proposta inicial das redes de canais de pagamento de uma rede totalmente distribuída e torna a rede suscetível a ataques. Além disso, o trabalho verifica que os resultados indicam uma evolução para uma rede pouco transitiva, o que inviabiliza técnicas de rebalanceamento de canais para grande parte dos nós. Em trabalhos futuros, pretende-se propor uma heurística para o estabelecimento de novas conexões, visando aumentar a distribuição da conectividade e a transitividade na rede.

Referências

Beres, F., Seres, I. A. e Benczur, A. A. (2019). A cryptoeconomic traffic analysis of Bitcoin's lightning network.

BitcoinWiki (2019). Bitcoin Scalability. `https://en.bitcoin.it/wiki/Scalability`. Acessado em 18 de janeiro de 2022.

BitInfoCharts (2022). Bitcoin Average Transaction Fee Chart. `https://bitinfocharts.com/comparison/bitcoin-transactionfees.html`. Acessado em 3 de fevereiro de 2022.

Blockchain.com (2022). Transações não confirmadas. `https://www.blockchain.com/btc/unconfirmed-transactions`. Acessado em 3 de fevereiro de 2022.

CloudTweaks (2021). How Bitcoin Brought The Lightning Network To El Salvador. `https://cloudtweaks.com/2021/07/how-bitcoin-brought-lightning-network-el-salvador/`. Acessado em 3 de fevereiro de 2022.

Decker, C. (2021). Lightning network research; topology datasets. `https://github.com/lnresearch/topology`. Acessado em 29 de dezembro de 2021.

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P. e Gervais, A. (2019). Sok: Off the chain transactions. *IACR Cryptol. ePrint Arch.*, 2019:360.

Khalil, R. e Gervais, A. (2017). Revive: Rebalancing off-blockchain payment networks. Em *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, página 439–453, New York, NY, USA. Association for Computing Machinery.

Lange, K., Rohrer, E. e Tschorsch, F. (2021). On the impact of attachment strategies for payment channel networks. Em *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, páginas 1–9. IEEE.

Li, L., Alderson, D., Doyle, J. C. e Willinger, W. (2005). Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4):431–523.

Lin, J.-H., Primicerio, K., Squartini, T., Decker, C. e Tessone, C. J. (2020). Lightning network: a second path towards centralisation of the bitcoin economy. *New Journal of Physics*, 22(8):083022.

Malavolta, G., Moreno-Sanchez, P., Kate, A. e Maffei, M. (2016). Silentwhispers: Enforcing security and privacy in decentralized credit networks. *Cryptology ePrint Archive*.

Pickhardt, R. e Nowostawski, M. (2020). Imbalance measure and proactive channel rebalancing algorithm for the lightning network. Em *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, páginas 1–5. IEEE.

Poon, J. e Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

Poon, J. e Osuntokun, O. (2021). BOLT #2: Peer protocol for channel management. `https://github.com/lightningnetwork/lightning-rfc/blob/master/02-peer-protocol.md`.

Prihodko, P., Zhigulin, S., Sahno, M., Ostrovskiy, A. e Osuntokun, O. (2016). Flare: An approach to routing in lightning network. *White Paper*, página 144.

Rebello, G. A., Potop-Butucaru, M., de Amorim, M. e Duarte, O. C. (2021). Protegendo redes de canais de pagamento sem fio com janelas de tempo de bloqueio mínimas. Em *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, páginas 295–308, Porto Alegre, RS, Brasil. SBC.

Rohrer, E., Malliaris, J. e Tschorsch, F. (2019). Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. Em *IEEE EEuroS&PW*.

Roos, S., Moreno-Sanchez, P., Kate, A. e Goldberg, I. (2017). Settling payments fast and private: Efficient decentralized routing for path-based transactions. *arXiv preprint arXiv:1709.05748*.

Seres, I. A., Gulyás, L., Nagy, D. A. e Burcsi, P. (2020). Topological analysis of bitcoin's lightning network. Em Pardalos, P., Kotsireas, I., Guo, Y. e Knottenbelt, W., editors, *Mathematical Research for Blockchain Economy*, páginas 1–12, Cham.

Sivaraman, V. et al. (2020). High throughput cryptocurrency routing in payment channel networks. Em *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*, páginas 777–796.

Tikhomirov, S., Moreno-Sanchez, P. e Maffei, M. (2020). A quantitative analysis of security, anonymity and scalability for the lightning network. Em *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, páginas 387–396. IEEE.

TrustNodes (2018). Lightning Network DDoS Sends 20% of Nodes Down. `https://www.trustnodes.com/2018/03/21/lightning-network-ddos-sends-20-nodes`. Acessado em 3 de fevereiro de 2022.

Zabka, P., Förster, K.-T., Schmid, S. e Decker, C. (2021). Node classification and geographical analysis of the lightning cryptocurrency network. Em *International Conference on Distributed Computing and Networking 2021*, páginas 126–135.