Protegendo Redes de Canais de Pagamento Sem Fio com Janelas de Tempo de Bloqueio Mínimas

Gabriel Antonio Fontes Rebello, Maria Potop-Butucaru, Marcelo Dias de Amorim, Otto Carlos Muniz Bandeira Duarte

Protegendo Redes de Canais de Pagamento Sem Fio com Janelas de Tempo de Bloqueio Mínimas

Gabriel Antonio F. Rebello[1,2], **Maria Potop-Butucaru**[2], **Marcelo Dias de Amorim**[2], **Otto Carlos M. B. Duarte**[1]

[1]GTA/COPPE - Universidade Federal do Rio de Janeiro, Brasil
[2]LIP6/CNRS - Sorbonne Université, França

Resumo. *Redes de canais de pagamento (Payment Channel Networks - PCN) aumentam o impacto das criptomoedas, fornecendo uma solução rápida e independente de consenso para mitigar os problemas de escalabilidade dos protocolos tradicionais de correntes de blocos (blockchain). No entanto, as PCNs atuais são baseadas em nós robustos com alta disponibilidade e capacidade computacional, dificultando sua adoção em ambientes móveis e sem fio. Este artigo propõe uma arquitetura PCN híbrida que estende as funcionalidades das PCNs tradicionais para cenários de dispositivos sem fio com recursos limitados. O artigo analisa a vulnerabilidade de roubo de tokens e propõe uma contramedida com base em janelas de tempo de bloqueio. O artigo avalia a proposta com dados reais da Lightning Network e de redes de banda larga móvel. Os resultados mostram que a janela de tempo mínimo de bloqueio depende do tempo de inatividade dos dispositivos e que selecionar uma janela padrão é mais eficaz quando os dispositivos apresentam alta disponibilidade.*

1. Introdução

Os protocolos de consenso de correntes de blocos (*blockchain*) mais utilizados atualmente apresentam problemas significativos de latência e gasto de energia que impedem a adoção de criptomoedas na vida cotidiana [Rebello et al. 2020, Erdin et al. 2021]. Publicar uma transação no Bitcoin leva aproximadamente uma hora, incorre em mais de 100 reais de taxas e gasta uma quantidade de energia suficiente para manter uma residência brasileira média por três meses [Blockchain.com 2021, MME 2017]. As redes de canais de pagamento (*Payment Channel Networks - PCN*) oferecem uma solução fora da corrente (*off-chain*) de blocos escalável e eficiente para melhorar esse desempenho, permitindo que as transações ocorram sem a necessidade de consenso. No entanto, apesar de fornecerem uma solução eficiente em comparação com a transação diretamente na corrente de blocos, as redes de canais de pagamento ainda contam com poder de processamento, capacidade de armazenamento e alta disponibilidade de seus participantes. Os nós na rede de canais de pagamento Lightning Network, da criptomoeda Bitcoin, usam o roteamento tipo casca de cebola (*Onion*) [Poon and Osuntokun 2021, Poon and Dryja 2016], que é altamente custoso, enquanto o roteamento da Raiden Network, da criptomoeda Ethereum, se baseia em roteamento pela origem que possui uma visão de topologia global sincronizada para definir caminhos [brainbot labs Est. 2020]. Outras PCNs também contam com verificações constantes e armazenamento da corrente de blocos, o que sobrecarra usuários finais que desejam utilizar a rede [Roos et al. 2017, Erdin et al. 2021].

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ e FAPESP (18/23292-0, 15/24514-9, 15/24485-9 14/50937-1). Uma versão em inglês baseada neste artigo intitulada *Securing Wireless Payment Channel Networks with Minimum Lock Time Windows* deve ser submetida a congressos ou revistas internacionais.

As PCNs são difíceis de implementar em dispositivos sem fio com poucos recursos e padrões de conectividade intermitentes causados por conexões sem fio. Vários trabalhos na literatura oferecem adaptações da Lightning Network para dispositivos móveis [Kurt et al. 2021, Hannon and Jin 2019, Robert et al. 2020]. No entanto, no melhor do nosso conhecimento, nenhuma solução analisa o problema de conectividade em profundidade e de maneira independente da implementação da rede de canal de pagamento.

Este artigo propõe contribuições para a implementação de redes de canais de pagamento em ambientes com recursos limitados compostos por dispositivos sem fio. Primeiro, considera-se uma arquitetura de redes de canais de pagamento híbrida que permite que os dispositivos emitam pagamentos apesar de apresentarem conectividade intermitente e incapacidade de armazenar a corrente de blocos. Segundo, o artigo formula e analisa o problema do roubo de *tokens*[1], uma vulnerabilidade presente em todas as redes de canais de pagamento [Poon and Dryja 2016, brainbot labs Est. 2020, Erdin et al. 2021], mas que se torna crítica em ambientes sem fio devido à maior perda de pacotes e ao tempo de inatividade dos dispositivos. Terceiro, este trabalho propõe uma contramedida para o problema de roubo de *tokens* com base em janelas de tempo de bloqueio que as PCNs atuais já implementam. Por fim, o artigo analisa o desempenho da abordagem proposta usando dados reais da Lightning Network e conexões de banda larga móvel.

2. Redes de Canais de Pagamento Sem Fio

Esta seção apresenta os conceitos de redes de canais de pagamento tradicionais e, em seguida, a arquitetura de rede utilizada para ambientes sem fio.

2.1. Redes de Canais de Pagamento

Os canais de pagamento são conexões bidirecionais entre duas partes que desejam negociar entre si. A Figura 1 mostra um exemplo de canal de pagamento. Para abrir um canal de pagamento, dois usuários, Alice e Bob, assinam e publicam uma transação de financiamento que transfere uma quantidade fixa de *tokens* para um endereço comum controlado por ambos. Alice e Bob podem então reequilibrar continuamente os fundos do endereço, enviando transações de compromisso (*commitment transactions*) assinadas e privadas. Dessa forma, Alice e Bob transacionam entre si sem pagar taxas para os mineradores da corrente de blocos e sem esperar que o sistema aprove as transações através de consenso. Essa abordagem é especialmente adequada para micropagamentos do dia-a-dia, que exigem agilidade e possuem baixos valores. A transação de financiamento contém uma janela de tempo de bloqueio (*lock time window*)[2] W que define um atraso medido em blocos que a parte finalizadora deve esperar para recuperar seus *tokens* investidos. Para fechar o canal, Alice ou Bob publica a última transação de confirmação na corrente de blocos e aguarda a janela de tempo de bloqueio para recuperar seus *tokens*. A janela de tempo de bloqueio serve como um mecanismo de segurança para evitar que Alice e Bob publiquem um balanço anterior na corrente de blocos. Se qualquer uma das partes detectar esse comportamento durante a janela de tempo de bloqueio, ela pode punir a outra parte gastando todos os *tokens* no canal.

[1] *Tokens*, ou fichas de permissão, são qualquer ativo digital que seja comercializado na corrente de blocos. No caso de criptomoedas, o ativo é o dinheiro digital trocado pelos usuários.

[2] A janela de tempo de bloqueio é frequentemente referida como "atraso para si"("*to self delay*") ou "atraso para retorno"("*return delay*") na literatura [Poon and Osuntokun 2021, Erdin et al. 2021]. Este artigo considera os termos equivalentes.

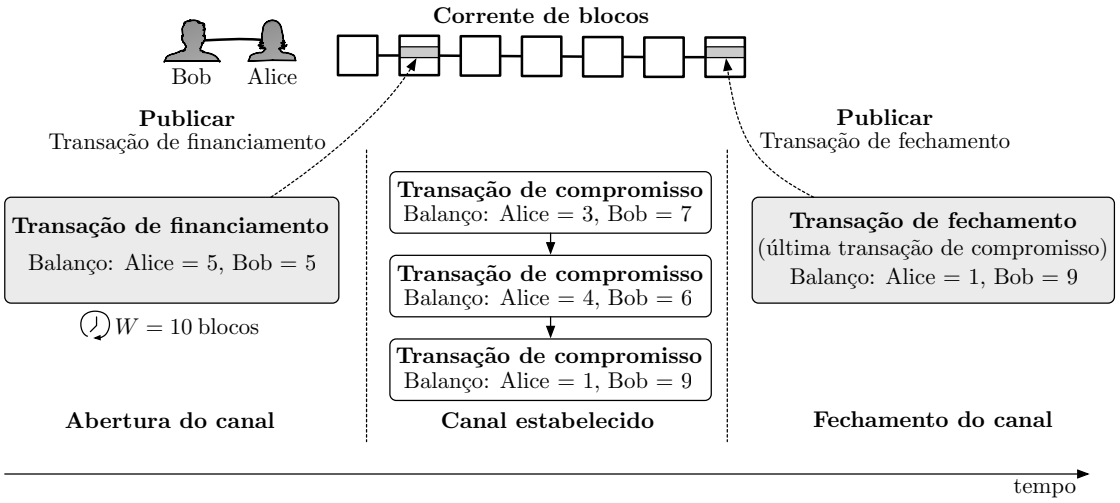

Figura 1. Um canal de pagamento entre os usuários Alice e Bob. Ambos os usuários emitem transações de compromisso privadas em tempo real após estabelecer o canal. A transação de financiamento contém uma janela de tempo *W* que bloqueia os *tokens* durante um número predefinido de blocos caso o canal seja fechado unilateralmente.

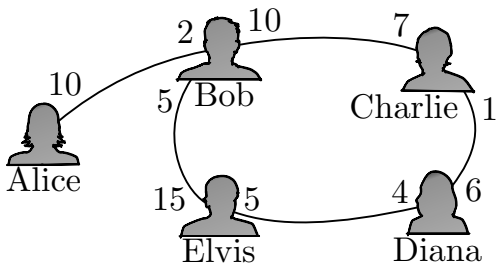

Figura 2. Um exemplo de rede de canais de pagamento composta por canais de pagamento bidirecionais com capacidade limitada. Os usuários que não compartilham enlaces diretos podem encaminhar os pagamentos por meio de intermediários.

Uma rede de canal de pagamento é uma rede par a par (*peer to peer - P2P*) composta de usuários e seus canais de pagamento. A Figura 2 mostra um exemplo de rede de canal de pagamento. Os nós podem emitir pagamentos para destinos mesmo que eles não compartilhem diretamente um canal de pagamento. Por exemplo, se Alice quiser enviar um *token* para Charlie, ela pode enviar o *token* para Bob, e Bob o retransmite para Charlie. Bob recebe o *token* de Alice assim que enviar um de sua autoria para Charlie por meio de contratos de bloqueio de tempo resumidos (*Hashed Timelock Contracts - HTLC*) [Lys et al. 2020], um tipo especial de *script* que pode ser escrito em criptomoedas. Consequentemente, o roteamento de pagamentos em redes de canais de pagamento é diferente das redes de dados clássicas porque o sistema deve garantir que cada intermediário tenha fundos suficientes para transferir *tokens*. O mecanismo de roteamento deve evitar o esgotamento dos enlaces no caminho de pagamento. Vários trabalhos na literatura exploram esse problema em redes de canais de pagamento tradicionais, como a Lightning Network, do Bitcoin, e a Raiden Network, do Ethereum [Sivaraman et al. 2020, Rohrer and Tschorsch 2020, brainbot labs Est. 2020].

2.2. Canais de Pagamento para Dispositivos Sem Fio com Restrições de Recursos

Este artigo considera o cenário de redes de canais de pagamento sem fio (*Wireless Payment Channel Networks - WPCN*), uma arquitetura de PCN híbrida composta de um núcleo estático e confiável, bem como de dispositivos móveis periféricos não confiáveis e com recursos limitados. Utilizar uma topologia híbrida é a mais impactante porque as principais plataformas Internet das Coisas e arquiteturas de dispositivos móveis hoje dependem de *gateways* e computação de borda para fornecer serviços. A Figura 3 descreve a topologia da arquitetura de rede considerada. Há dois tipos de nós na arquitetura:

- **Nós completos (NC)**, que compõem a rede central e atuam como roteadores. Os nós completos podem representar empresas de serviço, telecomunicações ou qualquer nó com capacidade de computação para armazenar uma cópia completa da corrente de blocos. Os nós completos permanecem online com alta probabilidade o tempo todo e se comunicam por meio de um protocolo de transporte confiável. Mesmo que falhas possam ocorrer na rede central, a probabilidade de que um nó completo saia da rede sem fechar seus canais de pagamento é insignificante em comparação com os nós móveis;
- **Nós leves (NL)**, que são dispositivos móveis que se conectam à rede por meio de conexões sem fio com perdas e possuem recursos limitados. Os nós leves podem representar telefones celulares, sensores, objetos inteligentes ou qualquer dispositivo de internet das coisas que apresente capacidade limitada de computação e armazenamento. Nós leves podem se desconectar a qualquer momento sem fechar o canal de pagamento devido ao mau funcionamento da bateria e do *hardware*, condições ambientais, problemas da operadora de celular e outras limitações dos dispositivos móveis. Os nós leves estabelecem conexões não confiáveis para enviar/receber transações e solicitar a verificação do estado do canal. Eles podem executar criptografia de chave pública para assinar transações, mas não são capazes de armazenar uma cópia da corrente de blocos.

Nós completos se conectam a outros nós completos por meio de canais de pagamento com grande capacidade para encaminhar pagamentos. Os nós leves conectam-se a um ou mais nós completos por meio de canais de pagamento menores e possivelmente unidirecionais. Doravante refere-se aos canais entre nós completos como *canais de pagamento de núcleo* e aos canais entre um nó leve e um nó completo como *canais de pagamento de borda*. A arquitetura não considera canais de pagamento entre nós leves, pois seria improvável que dois nós leves transacionassem continuamente um com o outro por um longo período. *Nós de entrada* são os nós que um nó leve seleciona como suas conexões na rede de canais de pagamento. Os nós leves também estabelecem conexões TCP/IP com outros nós completos para verificar continuamente os estados de seus canais de pagamento e evitar ataques de eclipse. Para nossa definição formal de Redes de Canais de Pagamento Sem Fio (WPCN), estende-se a definição de PCNs de Malavolta *et. al* [Malavolta et al. 2017]:

Definição 1 (Redes de Canais de Pagamento sem Fio (Wireless Payment Channel Networks - WPCN)). Uma rede de canais de pagamento sem fio é um grafo direcionado e dinâmico $\mathbb{G}(t) := (\mathbb{V}(t), \mathbb{E}(t))$, onde $\mathbb{V}(t)$ é o conjunto de dispositivos na rede no tempo t e $\mathbb{E}(t)$ é o conjunto de canais de pagamento abertos no tempo t. Qualquer dispositivo $u \in \mathbb{G}(t)$ pode alterar o conjunto $\mathbb{E}(t)$ de arestas através de três primitivas:

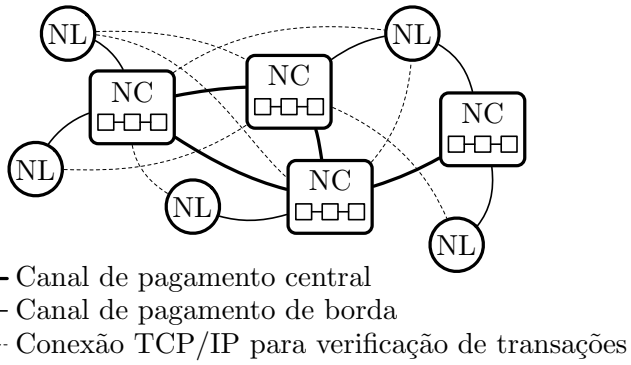

Figura 3. Um exemplo de topologia de redes de canais de pagamento sem fio. Os nós leves (NL) representam dispositivos sem fio e os nós completos (NC) representam nós que armazenam uma cópia da corrente de blocos. Os nós leves estabelecem conexões TCP/IP para verificar os estados de seus canais na corrente de blocos.

- `abrirCanal`$(\langle u, v\rangle, \langle \alpha, \beta\rangle, T, F, W)$ abre um canal de pagamento $u \leftrightarrow v$ com identificador c_{id}, capacidade (α, β), temporizador T, e taxa F. A janela de tempo de bloqueio W define a janela de tempo na qual nenhuma das partes pode recuperar os *tokens* se o canal for fechado de forma unilateral. A operação publica uma transação assinada por u e v na corrente de blocos;
- `fecharCanal`$(\langle u, v\rangle, Tx(t))$ encerra o canal de pagamento $u \leftrightarrow v$ com a transação $Tx(t)$, que contém o último balanço assinado no tempo t pelas duas partes, e a publica na corrente de blocos. Esta operação pode ocorrer com aprovação das duas partes ou de forma unilateral. Se o canal for encerrado de forma unilateral, a parte que fechou o canal só pode recuperar seus *tokens* após a janela de tempo de bloqueio W;
- `pagar`$(\langle u, v\rangle, p, V)$ transfere um valor de V *tokens* de u para v através do caminho $p = \langle u, r_1, r_2, ..., r_n, v\rangle$. Este artigo assume que o usuário u define o caminho p antes de utilizar a primitiva. Todos os saltos de u até v têm sua capacidade reduzida de V *tokens* na direção do destino v se todos os enlaces do caminho tiverem capacidade suficiente para a transferência. Do contrário, a operação falha e as capacidades dos canais permanecem inalteradas.

3. O Problema de Roubo de *Tokens*

PCNs como a Lightning Network [Poon and Dryja 2016] e a Raiden Network [brainbot labs Est. 2020] assumem que qualquer nó que transaciona na rede permanece em linha (*online*) enquanto o canal está aberto. Caso contrário, a contraparte do canal pode publicar uma transação antiga para recuperar os *tokens* que enviou para o nó desconectado. O sistema pune os nós maliciosos permitindo que a vítima gaste todos os *tokens* caso se recupere durante a janela de tempo de bloqueio predefinida. Portanto, só vale a pena tentar o ataque se o nó malicioso puder garantir que a outra parte não verificará a corrente de blocos até que a janela de tempo expire.

Um pequeno valor padrão para janelas de tempo de bloqueio funciona bem para redes com fio nas quais os nós têm uma cópia da corrente de blocos e todas as conexões são rápidas e confiáveis. Os usuários podem detectar comportamento malicioso instantaneamente, sem confiar em terceiros, simplesmente sincronizando suas correntes de blocos

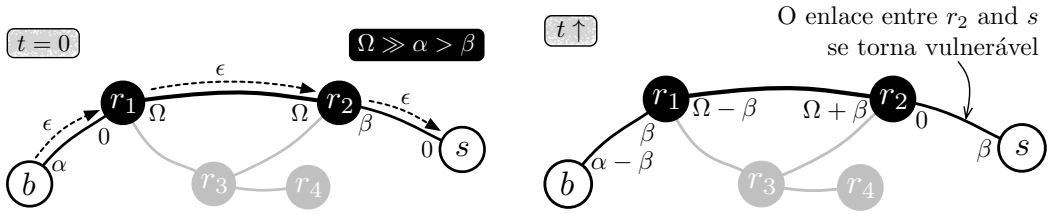

Figura 4. Um exemplo da vulnerabilidade de roubo de *tokens* em redes de canais de pagamento sem fio. À esquerda, uma quantidade contínua de ϵ *tokens* flui do comprador b para o vendedor s até que a capacidade do canal entre r_2 e s se esgote. Então, à direta, s se torna altamente vulnerável se perder a conexão antes de fechar o canal porque r_2 não tem nada a perder fechando o canal com um balanço anterior.

e verificando os blocos mais recentes. No entanto, os nós leves da arquitetura considerada podem se desconectar por longos períodos ou mesmo indefinidamente. O tempo de inatividade do dispositivo é especialmente desafiador para casos de uso em que a direção dos pagamentos é tendenciosa para um nó leve, como quando um vendedor usa seu dispositivo para receber transações de vários compradores. Nesse caso, espera-se que os canais de pagamento de borda sejam altamente desequilibrados em relação a uma das partes. A capacidade inicial do canal será desequilibrada em direção ao nó leve se o nó leve for um comprador, e em direção ao nó completo se o nó leve representar um vendedor.

Canais desequilibrados em ambientes com recursos limitados aumentam o problema de roubo de *tokens*. Sejam dois dispositivos com recursos limitados b e s, que representam dispositivos de um comprador e um vendedor, respectivamente, e estão conectados aos nós de entrada r_1 e r_2 por meio de canais de pagamento unidirecionais conforme mostrado na Figura 4. Cada canal de pagamento $u \leftrightarrow v$ tem um balanço $bal_{u \leftrightarrow v}(t) = (bal_u(t), bal_v(t))$, onde $bal_u(t)$ e $bal_v(t)$ são os balanços dos nós u e v no tempo t, respectivamente. Observe que $bal_u(t) + bal_v(t)$ é constante. Para canais de pagamento de borda entre compradores e nós de entrada, por exemplo $b \leftrightarrow r_1$, a arquitetura assume um balanço inicial de $bal_{b \leftrightarrow r_1}(0) = (\alpha, 0)$, onde α é uma quantidade de *tokens* para os quais o comprador b reserva pagamentos no canal. Da mesma forma, o balanço inicial dos canais de pagamento de borda entre vendedores e nós de entrada, por exemplo $r_2 \leftrightarrow s$ é $bal_{r_2 \leftrightarrow s}(0) = (\beta, 0)$ onde β é a quantidade de *tokens* que o nó de entrada r_2 reserva para encaminhar pagamentos ao vendedor s. A formulação assume por simplicidade e sem perda de generalidade que s e b só participam de um canal de pagamento.

Uma vez que um pagamento `pagar` $(\langle b, s\rangle, \{r_1, r_2\}, \epsilon)$ de ϵ *tokens* ocorre de b para s nesta configuração, r_2 e s assinam uma transação de compromisso $Tx(1)$ contendo o novo balanço do canal $bal_{r_2 \leftrightarrow s}(1) = (\beta - \epsilon, \epsilon)$. Se s se desconectar indefinidamente neste momento, r_2 pode fechar o canal com a operação `fecharCanal` $(\langle r_2, s\rangle, Tx(0))$ e recuperar ϵ *tokens*. Fazer isso é arriscado porque r_2 perderia todos os seus *tokens* se s se recuperar e detectar o comportamento malicioso antes da janela de tempo de bloqueio. No entanto, à medida que s recebe mais pagamentos, o balanço em $r_2 \leftrightarrow s$ convergirá para $bal_{r_2 \leftrightarrow s}(t) = (0, \beta)$. Uma vez que isso aconteça, r_2 não tem nada a perder fechando o canal com uma transação anterior, mesmo que s recupere a tempo. Esta é a estratégia ótima para qualquer nó de entrada racional r quando seu canal de pagamento de borda para um vendedor se esgotar. Os nós maliciosos também podem decidir atacar em casos

intermediários dependendo da relação risco-benefício. Portanto, é necessário modificar os mecanismos tradicionais de segurança das redes de canais de pagamento para evitar que nós completos adotem essa estratégia. Caso contrário, o vendedor s está sujeito a roubo de *tokens* mesmo na ausência de comportamento malicioso.

Embora esteja formulado para um caso extremo de compradores e vendedores, o problema se aplica a qualquer situação em que um nó leve recebe pagamentos e se desconecta sem fechar o canal corretamente. O problema não se aplica aos compradores porque a outra parte só pode perder *tokens* publicando uma transação anterior. Para uma situação genérica em que os nós leves atuam como compradores e vendedores, por exemplo em uma feira de comércio, cada nó leve se torna vulnerável assim que recebe um pagamento.

4. Definindo uma Janela de Bloqueio Tempo Mínima

Uma solução simples para o problema de roubo de *tokens* é contratar nós "vigilantes" que constantemente verificam a corrente de blocos para detectar canais que foram fechados indevidamente [Poon and Dryja 2016, brainbot labs Est. 2020, Erdin et al. 2021]. A solução, no entanto, implica que o nó leve divulgue todas as transações de compromisso para o nó vigilante e confie que ele não agirá de forma maliciosa. Uma segunda contramedida seria criar um sistema de reputação para nós completos no qual os nós leves puniriam o comportamento malicioso emitindo opiniões. No entanto, os sistemas de reputação levam à centralização e introduzem novos vetores de ataque que seriam difíceis de tratar em ambientes descentralizados [Camilo et al. 2020]. Em vez das duas medidas anteriores, este artigo propõe uma abordagem estatística simples: descobrir uma janela de tempo de bloqueio W que minimiza a chance de ataques. Esta solução é a mais fácil de implementar e a mais impactante, pois a maioria das redes de canais de pagamento já adotam janelas de tempo de bloqueio como medida de segurança [Poon and Dryja 2016, brainbot labs Est. 2020, Roos et al. 2017]. A contribuição deste artigo também serve às redes de canais de pagamento tradicionais como uma referência para que os usuários selecionem a melhor janela para seu padrão de conectividade.

A janela de tempo de bloqueio W, definida em número de blocos em cada operação de criação de canal, representa a quantidade de tempo que os *tokens* devem permanecer bloqueados até que uma parte possa reivindicá-los. A janela de tempo de bloqueio serve como uma contramedida contra ataques baseados no fechamento unilateral de canais. Por exemplo, suponha que um nó em um canal se desconecte e ocorra um ataque de roubo de *tokens*. Nesse caso, a parte atacada tem W blocos para se recuperar, verificar a corrente de blocos e punir o atacante antes que ele reivindique os *tokens*. Consequentemente, quanto maior for W, mais seguro o canal se torna contra o roubo de *tokens*. Por outro lado, definir um W grande demais pode criar gargalos no roteamento e punir os nós honestos que desejam fechar o canal corretamente após a outra parte se desconectar. Nesses casos, W deve ser o menor possível para não bloquear as capacidades do canal por longos períodos e para melhorar a eficiência geral da rede. Portanto, o valor ideal de W representa uma compromisso entre segurança e eficiência, e o objetivo deste artigo é minimizar W sem comprometer a segurança.

Seja s um dispositivo com recursos limitados. Este artigo propõe uma metodologia que usa quatro parâmetros para estimar W:

(i) T_{off}, uma variável aleatória que modela o tempo que s permanece desconectado do sistema, o que pode ocorrer devido a falha do dispositivo ou perda de pacotes.

T_{off} pode ser modelado por meio de uma distribuição aleatória contínua ou pode ser estimado com dados empíricos de um conjunto de dados;

(ii) D_{det}, uma variável aleatória que modela o atraso de s para detectar o ataque. D_{det} segue uma distribuição de Poisson com valor esperado limitado pela equação

$$E[D_{\text{det}}] = n\frac{E[T_{\text{off}}]}{b_t}\left(\frac{b_s}{d} + v\right), \tag{1}$$

onde n é o número de nós completos dos quais s solicita blocos, $E[T_{\text{off}}]$ é o tempo médio de recuperação de s, b_t é o tempo de bloco[3], b_s é o tamanho médio do bloco, d é a taxa média de download de s, v é o tempo médio para s verificar todas as transações em um bloco. $\frac{E[T_{\text{off}}]}{b_t}$ representa o número de blocos perdidos;

(iii) D_{pun}, uma variável aleatória que modela o atraso de s para punir o comportamento malicioso após a detecção. Como a punição incorre na publicação de uma transação na corrente de blocos, a distribuição de D_{pun} segue a distribuição Poisson definida por Nakamoto [Nakamoto 2008] com valor esperado

$$E[D_{\text{pun}}] = n_c b_t, \tag{2}$$

onde n_c é o número de confirmações necessárias para uma transação ser válida e b_t é o tempo de bloco. Observe que D_{pun} é diretamente proporcional às condições da corrente de blocos subjacente. Os valores padrão seriam aproximadamente $n_c = 6$ e $b_t = 600s$ para o Bitcoin, $n_c = 20$ e $b_t = 15s$ para o Ethereum, etc.;

(iv) Δ, uma variável aleatória que estima o desequilíbrio relativo de cada canal de pagamento aberto na rede. Para dados empíricos, calcula-se a razão de desequilíbrio de cada canal no conjunto de dados usando a equação

$$\Delta_i = \left|\frac{bal_u - bal_v}{bal_u + bal_v}\right| \forall \langle u, v\rangle \in \mathbb{E}(t), \tag{3}$$

onde i é o índice do canal e bal_u e bal_v são os balanços das partes do canal. O balanço Δ_i serve como uma estimativa de quão vulnerável a roubo de *tokens* o canal é, pois espera-se que ocorra um fluxo maior de pagamentos em direção à parte que possui menor capacidade.

Assim, cada um dos parâmetros descritos compõem a equação final de W:

$$W = (T_{\text{off}} + D_{\text{det}} + D_{\text{pun}})(1 + \Delta). \tag{4}$$

O raciocínio por trás desta definição é que a janela de tempo de bloqueio W deve ser pelo menos $T_{\text{off}} + D_{\text{det}} + D_{\text{pun}}$; caso contrário, a vítima não é capaz de se recuperar e punir o atacante antes que ele gaste os *tokens* roubados. Além disso, a metodologia aumenta a janela de tempo mínimo de bloqueio por um fator de Δ para compensar a vulnerabilidade extra de canais desequilibrados. Quanto mais desequilibrado é um canal inicialmente, mais pagamentos devem ocorrer do nó com mais capacidade para o nó com menos capacidade. Portanto, usando Δ como parte da equação, é possível aumentar a segurança do canal proporcionalmente à tendência dos fluxos esperados. Se o canal estiver equilibrado, espera-se que ambas as partes realizem transações entre si de maneira

[3]O tempo de bloco (*block time*) é o tempo médio necessário ara minerar um bloco no sistema.

uniforme e, portanto, nenhuma das duas terá interesse em atacar o canal. Observe que porque T_{off}, D_{det}, D_{pun} e Δ são distribuições aleatórias conhecidas ou dados estatísticos reais, o valor de W também será uma distribuição aleatória. O valor real de W a ser selecionado por um usuário depende do nível de segurança que ele deseja adotar para seu caso de uso. Os usuários que investem pesadamente no canal devem selecionar limites de W mais altos, pois ser atacado incorre em grandes perdas. Os usuários que desejam arriscar perdas podem selecionar limites menores para fornecer liquidez aos *tokens*.

5. Análise do Protótipo e Resultados

O protótipo proposto considera dados reais da Lightning Network [Poon and Dryja 2016] como referência, pois é a rede de canais de pagamento mais adotada por usuários [Erdin et al. 2021]. O perfil de conectividade dos dispositivos sem fio é baseado em conexões de banda larga móvel (*Mobile Broadband - MBB*) devido à sua presença massiva em todo o planeta [OECD 2021]. No entanto, a metodologia proposta é agnóstica a correntes de blocos, perfis de conectividade e topologias de canais de pagamento. É suficiente estimar os quatro parâmetros descritos na Seção 4 para encontrar um valor mínimo seguro para a janela de tempo de bloqueio que trata de qualquer caso de uso específico. O código completo da implementação está disponível no GitHub[4].

5.1. Configuração do Protótipo

O protótipo implementado simula três cenários diferentes que correspondem a medições de disponibilidade real de dispositivos de banda larga móvel para estimar a distribuição de T_{off} [Elmokashfi et al. 2017, Baltrunas et al. 2014]. Para o caso de alta disponibilidade, utilizam-se os dados de tempo de inatividade e de perda de pacotes de conexões de banda larga móvel encontrados por por Elmokashfi *et al.* [Elmokashfi et al. 2017]. No trabalho citado, mais de 90% das conexões usam tecnologia 4G e o tempo médio de indisponibilidade de uma conexão após interrupção do serviço é de 86,4s. O trabalho de Baltrunas *et al.* serve de referência para o caso de disponibilidade, pois mede a disponibilidade de conexões de banda larga móvel que usam 3G como tecnologia padrão e mostram que o tempo de indisponibilidade pode durar algumas horas [Baltrunas et al. 2014]. Por último, o protótipo simula um cenário de baixa disponibilidade, que é obtido ao se deslocar a distribuição de média disponibilidade para a direita pela distância média entre as distribuições de alta e média disponibilidade. Isso resulta em um tempo médio de indisponibilidade de cerca de uma semana. A Figura 5 mostra todos os casos lado a lado. Simulando três cenários quase simétricos com base em dados reais, é possível prever como diferentes níveis de disponibilidade afetam a janela de tempo mínimo de bloqueio. Isso pode ser estendido para dados de dispositivos do mundo real de qualquer tipo.

O protótipo utiliza $n = 3$, $b_t = 600s$ e $b_s = 10Mb/s$ como parâmetros do atraso de detecção D_{det}. $n = 3$ representa o número mínimo necessário de nós para os quais s deve solicitar blocos em caso de falhas, e b_s e b_t seguem o tempo de bloco e tamanho médio de bloco do Bitcoin, respectivamente. $E[T_{\text{off}}]$ é a média do cenário correspondente e a taxa de download d segue dados encontrados em trabalhos que avaliam a eficiência de redes de banda larga móvel: $d = 30Mb/s$ para alta disponibilidade, $d = 2Mb/s$ para média disponibilidade e $d = 1Mb/s$ para baixa disponibilidade [Baltrunas et al. 2014].

[4]Em caso de aceitação, os autores fornecerão o código em: https://github.com/gfrebello/pcn-time-window

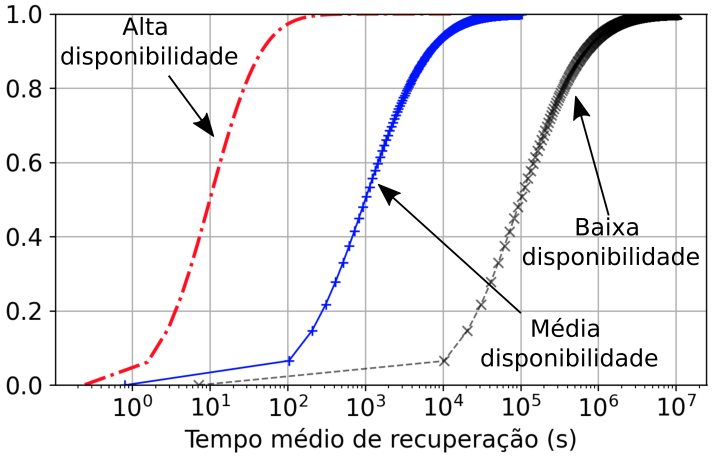

Figura 5. Funções de distribuição acumulada de T_{off}, o tempo de indisponibilidade de um nó vulnerável. As distribuições são baseadas em dados reais de estudos anteriores em redes de banda larga móvel 3G e 4G [Elmokashfi et al. 2017, Baltrunas et al. 2014].

Os parâmetros para o atraso de punição D_{pun} também seguem os padrões do Bitcoin. $b_t = 600s$ é o tempo de bloco e n_c, o número de confirmações, é definido de acordo com dois cenários diferentes. No cenário otimista, assume-se que uma transação é definitiva assim que aparece em um bloco; no cenário padrão, a avaliação utiliza a regra de seis confirmações proposta por Nakamoto no artigo original do Bitcoin [Nakamoto 2008].

5.2. Análise e Discussão

Os valores de Δ são obtidos através do LNChannels[5], uma plataforma de código aberto que oferece um conjunto de dados completo da Lightning Network. O protótipo utiliza os balanços de todos os canais fechados desde o início da rede e calcula o desequilíbrio normalizado Δ_i de cada canal de acordo com a Equação 3. A Figura 6 mostra a distribuição Δ. Os resultados mostram uma tendência forte de fluxos de pagamento em direção a uma das partes, mesmo que a distribuição seja composta por balanços de canal de uma rede de canais de pagamento tradicional. Isso confirma que o problema de roubo de *tokens* não é exclusivo das redes de canais de pagamento sem fio. Portanto, a adoção de janelas de tempo mínimo de bloqueio que dependem do desequilíbrio esperado do canal pode ser útil a diversas redes de canais de pagamento. O comportamento também é coerente com trabalhos anteriores que analisam a Lightning Network [Tikhomirov et al. 2020, Guo et al. 2019]. Há uma lacuna em torno do percentil 99% que se deve à implementação da Lightning Network. O BOLT #2 da documentação da Lightning Network [Poon and Osuntokun 2021] define um valor mínimo de pagamento chamado `dust_limit_satoshis` e escolhido pelo usuário que, se não for cumprido, invalida a transação e a transforma em taxas para o canal. O valor padrão de `dust_limit_satoshis` cria uma lacuna na distribuição Δ por não permitir que as partes paguem mais *tokens* quando o canal está quase esgotado.

Finalmente, o protótipo avalia a janela W através dos limites $W(p)$ que correspondem ao valor de W necessário para um dispositivo detectar e punir um invasor com

[5]Disponível em https://ln.fiatjaf.com/

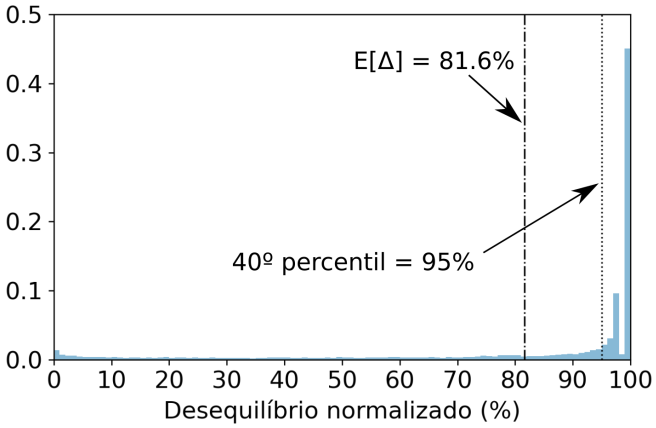

Figura 6. Desequilíbrio Δ dos canais de pagamento na Lightning Network. 60% dos canais apresentam desequilíbrio superior a 95%, e o desequilíbrio médio de 81% indica um comportamento fortemente assimétrico dos fluxos de pagamento.

probabilidade p. Portanto, um usuário que adota $W(p)$ obtém p probabilidade de estar seguro e assume $(1-p)$ de risco de ser atacado quando ocorre comportamento malicioso. O valor $W(50\%)$ serve como referência para um limite inseguro e o valor $W(95\%)$ serve para um limite seguro. A avaliação mede o compromisso entre janelas de tempo inseguras e seguras calculando a distância d entre os dois limites. Distâncias curtas significam nenhum ganho significativo com a adoção de uma janela menor, enquanto distâncias longas significam que o compromisso é significativo e, portanto, o usuário deve selecionar cuidadosamente o valor de W de acordo com suas necessidades. A Figura 7 descreve as funções de distribuição acumulada para os tamanhos mínimos de janela de todos os cenários considerados. Os limites $W(p)$ equivalem aos percentis da distribuição de W.

No cenário de alta disponibilidade, a conectividade 4G permite que os dispositivos fiquem protegidos contra ataques mesmo com janelas de tempo de bloqueio curtas. A distância de menos de um bloco entre $W(50\%)$ e $W(95\%)$ demonstra que aumentar W para um nível seguro não gera atrasos significativos. Logo, dispositivos com boa conectividade devem adotar o valor de W mais seguro possível. O resultado também confirma a suposição de que bons perfis de conectividade presentes na maioria das redes de canais de pagamento tradicionais podem mitigar o roubo de *tokens*.

O compromisso entre segurança e eficiência torna-se significativo no cenário de disponibilidade média. A distância de 33 blocos entre $W(50\%)$ e $W(95\%)$ corresponde a um acréscimo de 5,5 horas na espera da parte que fecha o canal. À medida que o tempo de recuperação aumenta, as diferenças entre os valores de W para uma confirmação e seis confirmações diminuem. T_{off} torna-se o parâmetro dominante na Equação 4. Os resultados indicam que um usuário com conectividade 3G deve definir janelas de tempo mínimo de bloqueio de pelo menos algumas horas para reduzir a probabilidade de ataques; caso contrário, os invasores com melhor conectividade podem explorá-los facilmente.

O cenário de baixa disponibilidade demonstra que os usuários com baixa conectividade devem selecionar valores de W no intervalo de dias a semanas ou usar a corrente de blocos para realizar transações diretamente. Atrasos em tal ordem de magnitude podem ser economicamente vantajosos se as taxas para publicar transações forem muito

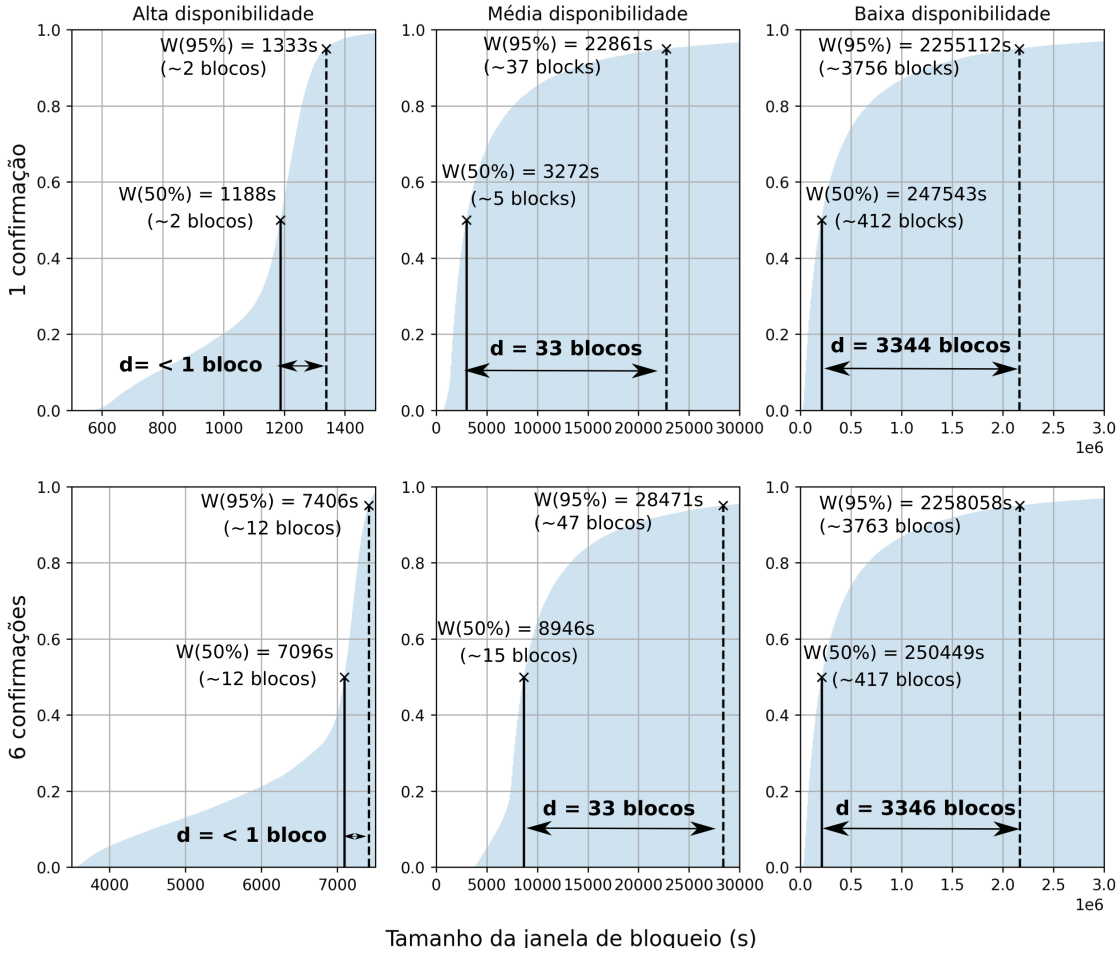

Figura 7. Tamanhos de janela de tempo de bloqueio para todos os níveis de disponibilidade com confirmação única e confirmação de seis blocos. Quando a disponibilidade é alta, a distância *d* entre os limites de 50% e 95% permanece abaixo de um bloco, o que indica que uma pequena janela é segura para a maioria dos usuários. Para disponibilidade média e baixa, a distância aumenta significativamente e obriga o usuário a selecionar uma janela de tempo que melhor se adapte às suas necessidades de segurança e atraso.

caras para o usuário. No entanto, assumindo um atraso de seis confirmações, mais de 550 transações poderiam ser publicadas em um intervalo de 3346 blocos. Assim, a janela de tempo W pode não ser a contramedida mais eficiente para dispositivos que permanecem offline por longos períodos. Em vez disso, deve-se adotar W com outros recursos de segurança, como punições mais pesadas para os invasores.

6. Trabalhos Relacionados

Diversos trabalhos propõem adaptações de redes de canais de pagamento tradicionais para dispositivos móveis. Kurt*et al.* propõem o LNGate, um protocolo leve para dispositivos IoT que permite usar a Lightning Network [Poon and Dryja 2016] via gateways não confiáveis [Kurt et al. 2021]. Hannon *et al.* propõem um protocolo semelhante para a Lightning Network e demonstram sua segurança e justiça usando teoria dos jogos [Hannon and Jin 2019]. Robert *et al.* propõem uma integração da Lightning Network com os ecossistemas IoT existentes em grande escala [Robert et al. 2020]. Mercan *et al.*

apresentam implementações leves de redes de canais de pagamento que se concentram na redução das necessidades computacionais para dispositivos móveis [Mercan et al. 2020]. Os trabalhos mencionados, no entanto, focam em adaptar a Lightning Network para cenários de IoT. Este trabalho propõe um novo modelo de redes de canais de pagamento e um recurso de segurança independente das implementações de PCNs.

Outros trabalhos analisam a segurança de redes de canais de pagamento tradicionais. Mizrahi *et al.* [Mizrahi and Zohar 2020] e Tochner *et al.* [Tochner et al. 2020] formulam ataques baseados em topologia que visam interromper o protocolo de roteamento de PCNs. Erdin *et al.* comparam a segurança e privacidade de várias implementações de PCN e identificam vetores de ataque emergentes [Erdin et al. 2021]. Os trabalhos não discutem ataques em redes de canais de pagamento com dispositivos com recursos limitados, nem apresentam contramedidas eficientes para ambientes sem fio. Este trabalho é o primeiro a propor uma arquitetura para PCNs sem fio, formular o ataque de roubo de *tokens* e propor uma análise de janela de tempo como uma contramedida eficiente.

7. Conclusão

Este artigo considerou uma arquitetura híbrida que permite que nós sem fio com recursos limitados emitam transações e analisou o impacto do problema de roubo de *tokens* em redes de canais de pagamento sem fio. As principais descobertas mostram que o problema não é exclusivo das redes de canais de pagamento sem fio e que a solução também pode funcionar com os redes de canais de pagamento tradicionais. Uma contramedida baseada em janelas de tempo mínimo de bloqueio é eficiente quando os dispositivos apresentam alta a média disponibilidade. Para dispositivos com baixa disponibilidade, a janela de tempo mínimo de bloqueio torna-se tão significativa que pode ser melhor publicar as transações diretamente na corrente de blocos. Assim, a principal contribuição deste artigo é prover uma referência precisa para assegurar trocas de ativos através de redes canais de pagamento. Em trabalhos futuros, pretende-se investigar outras contramedidas, como mecanismos de punição mais eficientes e janelas de tempo de bloqueio dinâmicas.

Referências

Baltrunas, D., Elmokashfi, A., and Kvalbein, A. (2014). Measuring the reliability of mobile broadband networks. In *14th ACM IMC*, pages 45–58.

Blockchain.com (2021). Blockchain charts. Disponível em: https://www.blockchain.com/charts. Acessado em 25/06/2021.

brainbot labs Est. (2020). The raiden network: Fast, cheap, scalable token transfers for ethereum. Disponível em: https://raiden.network/. Acessado em 25/06/2021.

Camilo, G. F., Rebello, G. A. F., de Souza, L. A. C., and Duarte, O. C. M. (2020). A secure personal-data trading system based on blockchain, trust, and reputation. In *3rd IEEE Blockchain*, pages 379–384. IEEE.

Elmokashfi, A., Zhou, D., and Baltrünas, D. (2017). Adding the next nine: An investigation of mobile broadband networks availability. In *23rd ACM MobiCom*, pages 88–100.

Erdin, E., Mercan, S., and Akkaya, K. (2021). An evaluation of cryptocurrency payment channel networks and their privacy implications. *arXiv preprint arXiv:2102.02659*.

Guo, Y., Tong, J., and Feng, C. (2019). A measurement study of bitcoin lightning network. In *2nd IEEE Blockchain*, pages 202–211. IEEE.

Hannon, C. and Jin, D. (2019). Bitcoin payment-channels for resource limited iot devices. In *IEEE COINS*, pages 50–57.

Kurt, A., Mercan, S., Shlomovits, O., Erdin, E., and Akkaya, K. (2021). Lngate: Powering iot with next generation lightning micro-payments using threshold cryptography. *arXiv preprint arXiv:2105.08902*.

Lys, L., Micoulet, A., and Potop-Butucaru, M. (2020). Atomic cross chain swaps via relays and adapters. In *3rd CryBlock*, pages 59–64.

Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M., and Ravi, S. (2017). Concurrency and privacy with payment-channel networks. In *2017 ACM SIGSAC CCS*, pages 455–471.

Mercan, S., Erdin, E., and Akkaya, K. (2020). Improving sustainability of cryptocurrency payment networks for iot applications. In *IEEE ICC Workshops*, pages 1–6. IEEE.

Mizrahi, A. and Zohar, A. (2020). Congestion attacks in payment channel networks. *arXiv preprint arXiv:2002.06564*.

MME (2017). Anuário estatístico de energia elétrica 2017. Technical report, Ministério de Minas e Energia do Brasil. Disponível em: http://epe.gov.br/sitespt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-160/topico-168/Anuario2017vf.pdf. Acessado em 25/06/2021.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Disponível em: https://bitcoin.org/bitcoin.pdf. Acessado em 25/06/2021.

OECD (2021). Mobile broadband subscriptions indicator. Disponível em: https://doi.org/10.1787/1277ddc6-en. Acessado em 25/06/2021.

Poon, J. and Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments. Disponível em: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf. Acessado em 25/06/2021.

Poon, J. and Osuntokun, O. (2021). BOLT #2: Peer protocol for channel management. Disponível em: https://doi.org/10.1787/1277ddc6-en. Acessado em 25/06/2021.

Rebello, G. A. F., Camilo, G. F., Guimarães, L. C., de Souza, L. A. C., and Duarte, O. C. M. (2020). On the security and performance of proof-based consensus protocols. In *4th CIoT*, pages 67–74. IEEE.

Robert, J., Kubler, S., and Ghatpande, S. (2020). Enhanced lightning network (off-chain)-based micropayment in iot ecosystems. *Future Generation Computer Systems*, 112:283–296.

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

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

Sivaraman, V., Venkatakrishnan, S. B., Ruan, K., Negi, P., Yang, L., Mittal, R., Fanti, G., and Alizadeh, M. (2020). High throughput cryptocurrency routing in payment channel networks. In *17th USENIX NSDI*, pages 777–796.

Tikhomirov, S., Pickhardt, R., Biryukov, A., and Nowostawski, M. (2020). Probing channel balances in the lightning network. *arXiv preprint arXiv:2004.00333*.

Tochner, S., Zohar, A., and Schmid, S. (2020). Route hijacking and dos in off-chain networks. In *2nd ACM AFT*, page 228–240. ACM.