# Investigando o Uso de Técnicas de Engenharia de Tráfego em Prefixos da Rede Bitcoin e suas Possíveis Implicações de Segurança

**Renan P. Barreto**[1], **Pedro Marcos**[1]

[1]Centro de Ciências Computacionais - Universidade Federal do Rio Grande (FURG)
Caixa Postal 474 – 96.201-900 – Rio Grande – RS – Brasil

renan.barreto@furg.br, pbmarcos@furg.br

***Abstract.*** *Bitcoin is one of the largest decentralized cryptocurrency networks, as such it is the target of studies and also of attacks. In this work we will investigate the use of traffic engineering techniques in order to observe possible vulnerabilities related to prefix hijack events.*
*We will demonstrate the use of traffic engineering methods, the length of advertised prefixes that contain Bitcoin nodes and the use of prepends in these prefixes. We will also estimate how many Bitcoin nodes are still under threat in the event of a prefix hijack. The results show that in 2022 only 2.72% of IPv4 and IPv6 nodes do not have the vulnerabilities addressed, increasing to 3.21% in 2023 .*

***Resumo.*** *O Bitcoin é uma das maiores criptomoedas, sendo assim ela é alvo de estudos e também de ataques. Neste trabalho iremos investigar o uso de técnicas de engenharia de tráfego, que a afetem, a fim de observar possíveis vulnerabilidades relacionadas a eventos de sequestro de prefixo.*
*Demonstraremos o uso de técnicas de engenharia de tráfego, a especificidade dos prefixos anunciados que contém nós Bitcoin e o uso de prepends nestes prefixos. Então iremos estimar quantos nós Bitcoin ainda estão sob ameaça de eventos de sequestro de prefixo. Os resultados encontrados mostram que somente 2,72% dos nós IPv4 e IPv6 não possuem as vulnerabilidades abordadas em 2022 e 3,21% em 2023.*

## 1. Introdução

Criptomoedas servem como uma rede descentralizada para transações monetárias eletrônicas *peer-to-peer*, permitindo o envio e recebimento de uma unidade monetária virtual. Isto ocorre sem a necessidade de uma instituição confiável como mediador e utilizando o mínimo de informação necessária entre as partes envolvidas, utilizando a infraestrutura da Internet, estrutura de *blockchain* e prova criptográfica para o armazenamento e verificação das transações.

Criado por Satoshi Nakamoto em 2008, o Bitcoin serve como uma criptomoeda com transações não-reversíveis [Nakamoto 2008]. Atualmente, de acordo com o site *CoinMarketCap*, a rede possui um valor de mercado de aproximadamente 560 bilhões de dólares americanos [CoinMarketCap 2022]. Por ser uma aplicação presente na Internet, o Bitcoin está suscetível a eventos que afetam a Internet como o sequestros de prefixos, onde um Sistema Autônomo, ou AS, anuncia um prefixo que não pertence a ele. Este evento pode levar ao atraso da rede e suas transações, desperdício energia e trabalho

dos computadores conectados a rede, o sequestro de nós ou de poder computacional na tentativa de manipular os dados de novos blocos na rede.

As vulnerabilidades da rede Bitcoin a ataques de roteamento, a efetividade dos mesmos e possíveis soluções para as vulnerabilidades são pontos já previamente abordados [Apostolaki et al. 2017]. Entre os pontos relevantes que não foram abordados estão o uso de *path prepending* e a conectividade dos ASes que possuem nós Bitcoin. Além dos pontos levantados, também houve mudanças na topologia dos sistemas autônomos (ASes) e da rede Bitcoin. Atualmente, de acordo com o site BitNodes, a estimativa é que existam 46 mil nós, sendo aproximadamente 16 mil destes considerados nós alcançáveis , sendo 52% destes na rede TOR, comparado com 5500 nós alcançáveis e 3,4% de nós na rede TOR em janeiro de 2017 [BitNodes 2022b].

Com os dados de roteamento disponibilizados pelo projeto Route Views [University of Oregon 2022a] e Bitnodes [BitNodes 2022a], foram feitas análises quanto a conectividade dos ASes que possuem nós Bitcoin. Também foram analisadas a especificidade dos prefixos anunciados e o uso de *prepending*. Com o objetivo de avaliar quantos nós possuem fatores de risco e quais fatores dentre os analisados neste trabalho.

## 2. Metodologia

O protocolo BGP, *Border Gateway Protocol*, é o protocolo de roteamento que ASes utilizam para trocar informação de roteamento entre si [Rekhter et al. 2006]. Um prefixo é inicialmente anunciada pelo AS que possui aquele prefixo para os ASes vizinhos, os quais podem então anunciar para seus respectivos vizinhos, disseminando a informações sobre os possíveis caminhos até aquele prefixo. Um AS que deseja chegar a um determinado prefixo irá escolher, entre seus vizinhos que conhecem um caminho até o prefixo, qual será o próximo pulo, este vizinho então escolhe o próximo e assim sucessivamente. A escolha da rota até um prefixo depende dos critérios definidos no protocolo, por exemplo o tamanho do caminho ou a especificidade de um prefixo. Estes podem ser utilizadas pela engenharia de tráfego para tentar influenciar a escolha das rotas [Feamster et al. 2003], entretanto, também podem criar vulnerabilidades [Marcos et al. 2020]. O roubo de prefixos acontece pelo fato destas rotas ofertadas não serem verificadas, logo um AS malicioso pode anunciar um prefixo que ele não é dono.

O sequestro de um prefixo acontece quando um AS anuncia, intencionalmente ou não, um conjunto de endereços que não pertencem a ele. Desviando conexões que deveriam ir para o destino correto para este AS, dado que este seja considerada a rota a ser seguida. Isto pode ser utilizado para descartar as requisições que deveriam ir ao AS correto ou para interceptar estes dados, para monitoramento ou alteração, e então enviar para o destino correto [Ballani et al. 2007].

Para o mapeamento das conexões entre ASes, utilizamos de dados de conexões BGP disponíveis de forma pública através do serviço RouteViews [University of Oregon 2022a]. Utilizando os arquivos disponibilizados pelos coletores podemos extrair os dados utilizando a ferramenta BGP Scanner [Gregori et al. 2018]. Assim, temos acesso aos dados sobre quais ASes possuem conexões entre si e quais são os possíveis caminhos entre eles. Os dados atuais e históricos de BGP irão permitir comparar o uso de técnicas de engenharia de tráfego e a conectividade entre ASes.

Para a rede Bitcoin, foram utilizados os dados do *crawler* disponibilizado pelo

BitNodes e sua API [BitNodes 2022a]. Esta disponibiliza os dados dos nós publicamente acessíveis da rede, o respectivo AS onde o nó se encontra, versão do nó, seu IP e localização aproximada. Os dados dos nós somente possuem histórico de 3 meses utilizando a API disponibilizada.

Com os dados da rede e do BGP definimos a especificidade dos anúncios, o uso de *prepending* e a conectividade do ASes. Assim é possível definir quais fatores relacionados a engenharia de tráfego podem facilitar ataques de sequestro de prefixo contra a rede Bitcoin, os quais poderiam particionar ou atrasar a rede e então gerar um evento de gasto duplo, onde uma mesma unidade monetária é utilizada mais de uma vez. Os dados de roteamento utilizados são do dia 31 de Agosto de 2022 às 22:00 horas e do dia 1 de Agosto às 4:00 horas, ambos do coletor de São Paulo [University of Oregon 2022b]. Os dados utilizados da API do BitNodes são os disponibilizados as 22:03 horas do dia 31 de Agosto de 2022 e do dia 1 de Agosto de 2023 às 3:01 horas, onde os campos extraídos foram o IP do nó e o AS ao qual ele pertence, o qual o último é identificado pela sigla AS seguida pelo número do mesmo [Barreto 2022].

Dos dados dos coletores BGP, foram utilizados o prefixo anunciado e o caminho utilizado. Sendo possível inferir o número de *prepends* utilizados ao contar quantas vezes a mais o AS anunciante aparece no caminho. Sendo assim um AS que seja exibido 3 vezes em um caminho possui um *prepend* de valor 2. Em um trabalho anterior, [Marcos et al. 2020] propôs o estudo do uso de *prepending* pelos ASes e as possíveis vulnerabilidades relacionadas a utilização desta técnica de engenharia de tráfego, uma das conclusões é que o uso de 3, ou mais, *prepends* leva a maiores riscos no caso de eventos de sequestro de prefixo. No estudo mencionado um prefixo anunciado com 3 *prepends* teve 94% dos monitores que estavam conectados a ele sequestrados[Marcos et al. 2020].

Considerando que um nó esteja em um prefixo /24, ele seria menos suscetível a um evento de sequestro usando um prefixo mais específico já que prefixos /25 costumam ser filtrados pelos ASes, logo o sequestro tem sua eficácia diminuída dado que ele deverá sobrepor os outros critérios do BGP, como preferência local e caminho mais curto. No caso de um nó contido em um /23 o anúncio de um prefixo /24, ao qual contém o IP do nó, deverá ter mais sucesso no sequestro deste prefixo, já que o primeiro critério de escolha do BGP é a especificidade.

Para a conectividade de um AS foram utilizados os dados das relações entre ASes disponibilizadas pelo CAIDA, para dois ASes terem uma relação é necessário uma conexão. Logo foram contabilizadas as relações entre ASes independente de tipo, contando por par de AS impedindo que uma conexão seja contada duas vezes pela sua direção [Center for Applied Internet Data Analysis, UC San Diego 2013].

## 3. Resultados

Com os dados é possível demonstrar quantos nós possuem riscos quanto a especificidade do anúncio, conectividade do AS e uso de *prepends*. Na Tabela 1 vemos que somente 2,72% dos 7394 nós IPv4 e IPv6 estão em ASes com conectividade acima da média, em anúncios de especificidade /24, ou /48 para IPv6, e sem *prepends*, logo estes nós possuem maior segurança contra eventos de sequestro de prefixo. A porcentagem de nós que possuem fatores que facilitam eventos de sequestro de prefixo é de 97,28%. Entretanto é possível observar na Tabela 1 observar que não há nós que possuem todos os fatores,

sendo eles o uso de *prepends* longos, baixa conectividade e baixa especificidade.

**Tabela 1. Estado dos nó quanto a fatores que influenciam na segurança em casos de eventos de sequestro de prefixo segundo os dados de 2022.**

| **Conectividade e *Prepend*** | **Prefixo v4 /24** | **Prefixo v4 Menor que /24** | **Prefixo v6 /48 ou Maior** | **Prefixo v6 Menor que /48** |
|---|---|---|---|---|
| Sem *Prepend* Com Conectividade igual ou acima da mediana | 2,11% (156) | 58,17% (4301) | 0,61% (45) | 12,24% (905) |
| *Prepend* Menor que 3 Com Conectividade igual ou acima da mediana | 0,24% (18) | 8,16% (603) | 0,01% (1) | 0,15% (11) |
| *Prepend* Maior ou Igual a 3 Com Conectividade igual ou acima da mediana | 0,30% (22) | 1,08% (80) | 0,00% (0) | 0,42% (31) |
| Sem *Prepend* Com Conectividade abaixo da mediana | 2,56% (189) | 4,99% (369) | 0,20% (15) | 0,88% (65) |
| *Prepend* Menor que 3 Com Conectividade abaixo da mediana | 0,26% (19) | 0,53% (39) | 0,00% (0) | 0,01% (1) |
| *Prepend* Maior ou Igual a 3 Com Conectividade abaixo da mediana | 0,12% (9) | 0,32% (24) | 0,00% (0) | 0,05% (4) |
| Sem *Prepend* Com Conectividade igual a 1 | 0,78% (58) | 5,21% (385) | 0,07% (5) | 0,47% (35) |
| *Prepend* Menor que 3 Com Conectividade igual a 1 | 0,01% (1) | 0,04% (3) | 0,00% (0) | 0,00% (0) |
| *Prepend* Maior ou Igual a 3 Com Conectividade igual a 1 | 0,00% (0) | 0,00% (0) | 0,00% (0) | 0,00% (0) |

Ao observar os dados utilizados para o ano de 2023 demonstrados na Tabela 2, podemos notar proporções similares as vistas nos dados de 2022. Entretanto é possível observar que o houve um aumento no número de nós IPv6 que estão contido em anúncios com o uso de *prepend*, com isso diminuindo os nós que estão em ASes com conectividade acima da mediana, em anúncios de especificidade maior ou igual a /48 para IPv6 e sem *prepends* de 12,24% para 6,97%.

Houve aumento da proporção de nós em ASes que possuem um menor número de relações com outros ASes, independente da especificidade do anúncio, de 7,55% para 12,07%. Em ambos os anos não há nós nos piores casos, que seriam com *prepend* maior ou igual a 3, com especificidade menor que /24 e /48, para IPv4 e IPv6 respectivamente, e em ASes com somente 1 vizinho, independente do tipo de relação. Como uma observação, em 2022 só foram vistos anúncios com a especificidade até /48, entretanto em 2023 um único nó estava contido em um prefixo /52.

## 4. Considerações Finais

As medições realizadas permitem observar que a rede Bitcoin possui outras vulnerabilidades quanto ao roteamento de tráfego, além das levantadas por estudo anteriores

**Tabela 2. Estado dos nó quanto a fatores que influenciam na segurança em casos de eventos de sequestro de prefixo segundo os dados de 2023.**

| Conectividade e *Prepend* | Prefixo v4 /24 | Prefixo v4 Menor que /24 | Prefixo v6 /48 ou Maior | Prefixo v6 Menor que /48 |
|---|---|---|---|---|
| Sem *Prepend* Com Conectividade igual ou acima da mediana | 2,65% (179) | 47,78% (3222) | 0,56% (38) | 6,97% (470) |
| *Prepend* Menor que 3 Com Conectividade igual ou acima da mediana | 0,44% (30) | 10,32% (696) | 0,06% (4) | 4,33% (292) |
| *Prepend* Maior ou Igual a 3 Com Conectividade igual ou acima da mediana | 0,43% (29) | 4,17% (281) | 0,06% (4) | 2,43% (164) |
| Sem *Prepend* Com Conectividade abaixo da mediana | 1,94% (131) | 10,13% (683) | 0,19% (13) | 0,92% (62) |
| *Prepend* Menor que 3 Com Conectividade abaixo da mediana | 0,15% (10) | 0,65% (44) | 0,03% (2) | 0,06% (4) |
| *Prepend* Maior ou Igual a 3 Com Conectividade abaixo da mediana | 0,15% (10) | 0,34% (23) | 0,01% (1) | 0,03% (2) |
| Sem *Prepend* Com Conectividade igual a 1 | 1,23% (83) | 3,07% (207) | 0,53% (36) | 0,30% (20) |
| *Prepend* Menor que 3 Com Conectividade igual a 1 | 0,00% (0) | 0,03% (2) | 0,00% (0) | 0,00% (0) |
| *Prepend* Maior ou Igual a 3 Com Conectividade igual a 1 | 0,03% (2) | 0,00% (0) | 0,00% (0) | 0,00% (0) |

[Apostolaki et al. 2017]. Entre as vulnerabilidades encontradas estão nós em ASes com baixa conectividade, a especificidade dos anúncios em IPv6 e o uso demasiado de *prepending*. Considerando os resultados apresentados, há um indício de que somente 2,72% dos nós IPv4 e IPv6 visíveis não possuíam estas vulnerabilidades contra eventos de sequestro de prefixo em 2022 e 3,21% em 2023. Importante lembrar que o Bitcoin é uma aplicação que está na Internet, sendo assim as mesmas vulnerabilidades geradas pelo uso das técnicas da engenharia de tráfego podem estar presentes em outras aplicações que estejam contidas em prefixos os quais os ASes utilizem estas técnicas.

As possíveis soluções variam de acordo com as vulnerabilidades dos nós, mas podem ser consideradas a desagregação de prefixos em /24 e /48, o uso de *prepends* menores, aumento da conectividade dos ASes ou a realocação dos nós para ASes com maior conectividade mas evitando a concentração em poucos ASes. Importante levar em consideração que as soluções para estas vulnerabilidades podem apresentar problemas também, como o aumento das RIBs, *routing information base*, maiores custos para os ASes ou desafios de engenharia de tráfego.

Entre as possibilidades de trabalhos futuros há a expansão das análises para todos anúncios de todos os ASes presentes na Internet e o cálculo do risco de cada fator, assim como determinar um método para permitir que o operador tenha a informações

sobre os riscos associados com os métodos e parâmetros escolhidos para a engenharia de tráfego aplicada. Há também o desafio da criação de conjuntos de dados utilizando as RIBs dos coletores disponíveis para gerar um panorama mais completo dos anúncios das rotas, levando em considerações a visibilidade de cada coletor, problemas nas coleta, ASes irmãos, eventos de sequestro de prefixo e outros eventuais erros e problemas.

## Referências


Apostolaki, M., Zohar, A., and Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 375–392.

Ballani, H., Francis, P., and Zhang, X. (2007). A study of prefix hijacking and interception in the internet. In *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '07, page 265–276, New York, NY, USA. Association for Computing Machinery.

Barreto, R. (2022). BTCData. https://github.com/RPBarreto/BTCData/tree/main. [Online; accessed 14-October-2023].

BitNodes (2022a). Api. https://bitnodes.io/api/. [Online; accessed 11-June-2022].

BitNodes (2022b). Dashboard. https://bitnodes.io/dashboard/. [Online; accessed 06-June-2022].

Center for Applied Internet Data Analysis, UC San Diego (2013). As relationships. https://www.caida.org/catalog/datasets/as-relationships/. [Online; accessed 20-January-2023].

CoinMarketCap (2022). Bitcoin. https://coinmarketcap.com/currencies/bitcoin/. [Online; accessed 06-June-2022].

Feamster, N., Borkenhagen, J., and Rexford, J. (2003). Guidelines for interdomain traffic engineering. *SIGCOMM Comput. Commun. Rev.*, 33(5):19–30.

Gregori, E., Improta, A., and Sani, L. (2018). Bgpscanner. https://gitlab.com/Isolario/bgpscanner/-/tree/master/. [Online; accessed 11-June-2022].

Marcos, P., Prehn, L., Leal, L., Dainotti, A., Feldmann, A., and Barcellos, M. (2020). As-path prepending: There is no rose without a thorn. In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 506–520, New York, NY, USA. Association for Computing Machinery.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot.

Rekhter, Y., Li, T., and Hares, S. (2006). Rfc 4271: A border gateway protocol 4 (bgp-4).

University of Oregon (2022a). University of Oregon Route Views Archive Project. http://archive.routeviews.org/. [Online; accessed 12-June-2022].

University of Oregon (2022b). University of Oregon Route Views Archive Project: São Paulo Data Archive. https://archive.routeviews.org/route-views2.saopaulo/bgpdata/. [Online; accessed 13-September-2023].