

Análise do comportamento de contas no Ethereum durante um evento de impacto na economia

Pedro Henrique F. S. Oliveira¹, Daniel Muller Rezende¹, Heder S. Bernardino¹, Saulo Moraes Villela¹, Alex B. Vieira¹, Glauber Dias Gonçalves²

¹Universidade Federal de Juiz de Fora (UFJF) – DCC

²Universidade Federal do Piauí (UFPI) – CSHNB

{phfsoliveira,daniel.muller,heder}@ice.ufjf.br,

{saulo.moraes,alex.borges}@ufjf.edu.br, ggoncalves@ufpi.edu.br

Abstract. *One of the main events that involve the world economy in 2022 is the conflict between Russia and Ukraine. This event offers a rare opportunity to analyze how events of this magnitude can reflect the use of cryptocurrencies. This work aims to investigate the behavior of accounts and their transactions on the Ethereum cryptocurrency during this event. To this end, we collected all transactions that occurred two weeks before and two weeks after the beginning of the conflict, organized into two groups: the collection of the accounts involved in these transactions and the subset of these ones that interacted with a service in Ethereum, called Flashbots Auction. We modeled temporal graphs where each node represents an account, and each edge represents a transaction between two accounts. Then, we analyzed the behavior of these accounts with graph metrics for both groups during each observed week. The results showed changes in the behavior and activity of users and their accounts, as well as variations in the daily volume of transactions.*

Resumo. *Um dos principais eventos que envolve a economia mundial em 2022 é o conflito entre Rússia e Ucrânia. Esse evento oferece uma oportunidade ímpar para analisar como acontecimentos dessa magnitude podem refletir no uso de criptomoedas. Este trabalho busca investigar o comportamento de contas e suas transações na rede de criptoativos Ethereum durante esse evento. Para tal fim, coletamos todas as transações realizadas duas semanas antes e duas semanas após o início do conflito, organizadas em dois grupos: o conjunto das contas envolvidas nessas transações e o subconjunto dessas contas que interagiram com um serviço dentro do Ethereum, chamado Flashbots Auction. Então, modelamos grafos temporais em que cada vértice representa uma conta e cada aresta representa uma transação realizada entre duas contas. Analisamos o comportamento dessas contas via métricas de grafos para ambos os grupos durante cada semana observada. Os resultados mostram mudanças no comportamento e atividade de contas, bem como variações no volume diário de transações.*

1. Introdução

Em abril de 2021, forças armadas russas realizavam uma mobilização militar na fronteira com a Ucrânia, comparada com a mobilização para anexação da República da Crimeia à

federação russa, ocorrida em 2014¹. Quase um ano depois, em 24 de fevereiro de 2022, a Rússia realizou uma nova mobilização militar no território da Ucrânia, iniciando um conflito entre esses dois países². A fim de evitar uma maior escalada de tensão mundial, a forma que outros países ao redor do mundo têm buscado para interferir é por meio de sanções à Rússia e suporte econômico para a Ucrânia³. Eventos de grande magnitude como esse tendem a envolver movimentações financeiras, podendo refletir no uso e popularização de criptomoedas, baseadas na tecnologia blockchain, para transferências e aquisição de ativos digitais de forma descentralizada.

Entre as várias criptomoedas existentes, o *Ethereum* se destaca como uma das principais plataformas para negociação de criptoativos, possuindo atualmente o segundo maior valor de mercado com mais de 363 bilhões de dólares⁴. Adicionalmente, o *Ethereum* é a principal criptomoeda que contempla a funcionalidade de armazenar e processar códigos de programas – denominados contratos inteligentes – dentro de sua blockchain.

Em frente à essa situação, ainda há muitas incertezas sobre a forma que tal conflito armado com impactos na economia e no mercado financeiro mundial pode refletir nos criptoativos. Uma importante questão surge nesse contexto: Como monitorar grandes plataformas de criptoativos como o *Ethereum* para observar o possível impacto de eventos externos a essas plataformas no comportamento de seus usuários no menor período de tempo possível?

Para iniciar a elucidar essa questão, neste trabalho propomos uma caracterização do comportamento das contas no *Ethereum* dentro de um período de tempo curto, especificamente, menos de um mês. Nesse sentido, coletamos todas as transações no *Ethereum* entre duas semanas antes e duas semanas após o início do conflito. A seguir, nós contrastamos duas visões diferentes acerca do comportamento das contas envolvidas nessas transações nesse período. A primeira visão representa um contexto geral que contempla todas as contas que realizaram transações nas quatro semanas coletadas. A segunda visão representa um contexto mais específico, contemplando apenas as contas com transações no *Ethereum* via o serviço *Flashbots Auction*, que é um novo mecanismo de comunicação entre os mantenedores da plataforma (mineradores) e usuários⁵.

A escolha do serviço *Flashbots* se deve à sua relevância como mecanismo mediador de transações voltadas para a extração de receitas MEV, ou seja, os lucros máximos obtidos por negociações de criptoativos. Um exemplo relevante, é o cenário de compra e venda de tokens não fungíveis (NFTs). Nele, os usuários utilizam técnicas para monitorar a rede e lucrar com as diferenças de preço desses ativos entre as instituições de câmbio ou *exchanges*. A análise dos *Flashbots* nos permite obter uma aproximação das características comportamentais dessa vertente da plataforma que tem crescido consideravelmente nos últimos anos.

Em nossa caracterização das contas do *Ethereum* com visões geral e específica exploramos propriedades de grafos, onde vértices representam contas e arestas caracterizam as transações entre duas contas. Essa abordagem nos permitiu analisar a dinâmica

¹<https://www.reuters.com/article/us-ukraine-crisis-usa-idUSKBN2BV2Z3>

²<https://www.cnbc.com/2022/02/24/russian-forces-invade-ukraine.html>

³<https://www.bbc.com/news/world-europe-60125659>

⁴<https://coinmarketcap.com/>

⁵<https://docs.flashbots.net/>

temporal do grau das contas, considerando valor e número de transações, bem como a identificação das contas centrais e com comportamento anômalo em um período que envolve um evento de impacto na economia. Em suma, esse trabalho tem duas contribuições principais: (i) uma estratégia para caracterizar o comportamento de usuários em plataformas de criptoativos como Ethereum, que permite o uso de vários serviços para negociar criptoativos dentro da plataforma, e (ii) a caracterização do comportamento das contas em função de um evento externo à plataforma de relevância para análise. Utilizamos como caso de estudo o serviço de Flashbots e o conflito atual entre a Rússia e Ucrânia.

As próximas seções desse artigo estão organizadas da seguinte maneira. Apresentamos trabalhos relacionados na Seção 2. Já na Seção 3, descrevemos a coleta dos dados utilizados, enquanto na Seção 4 descrevemos a metodologia para as análises desses dados. Os resultados obtidos são explorados na Seção 5 e, as conclusões finais e discussão sobre trabalhos futuros são apresentadas na Seção 6.

2. Trabalhos relacionados

Os grafos vêm se tornando uma forma importante para modelagem e caracterização de transações em plataformas de criptoativos. As primeiras análises baseadas em grafos foram conduzidas no Bitcoin, que foi a primeira plataforma de criptoativos concebida, baseada na tecnologia blockchain, sendo considerada ainda o maior criptoativo atualmente em termos de número de transações e valor de capital investido. Em [Miller et al. 2015, Sun et al. 2019] foram utilizados grafos para modelar a estrutura da rede Bitcoin com objetivo de identificar perfis de contas influentes ou suspeitas. Contudo, o Bitcoin é considerado um criptoativo de primeira geração que não suporta contratos inteligentes e os diversos serviços baseados em contratos para negociação de criptoativos.

O Ethereum, por sua vez, é uma plataforma de criptoativos de segunda geração, onde foi concebido primeiramente o uso de contratos inteligentes. Dado a variabilidade de serviços para criptoativos baseados em contratos, modelos de grafos vem sendo amplamente desenvolvidos para o Ethereum. O modelo proposto em [Chen et al. 2020] faz uso de grafos para representar criação de contratos inteligentes, invocação de contratos inteligentes e realização de transações externas. Por meio desses grafos, os autores conseguem fazer uso de métricas de centralidade em redes complexas, para detectar vértices importantes e vértices anômalos no Ethereum.

Técnicas que exploram grafos temporais também já foram propostas na literatura para análise da plataforma Ethereum. Em [Agarwal et al. 2021], por exemplo, características extraídas grafos temporais direcionados foram utilizados para desenvolver um modelo preditivo baseado em aprendizagem de máquina treinado para identificar perfis de contas maliciosas dentro dessa plataforma. Por sua vez, em [Zhao et al. 2021, Bai et al. 2020, Zanelatto Gavião Mascarenhas et al. 2020] modelos baseados em grafos foram utilizados para analisar o comportamento evolutivo do Ethereum ao longo do tempo desde sua origem em 2014.

Diferentemente dos trabalhos baseados em grafos acima mencionados, nesse trabalho, propomos modelos de grafos temporais para analisar a plataforma Ethereum em um curto período de tempo antes e após um evento de referência. Para o nosso conhecimento, nosso trabalho é o primeiro que explora métricas de grafos com essa abordagem.

Adicionalmente contrastamos métricas extraídas de um grafo temporal completo e seu subgrafo que representam respectivamente as contas gerais do Ethereum no período de interesse e as contas que interagiram com o serviço Flashbots.

Importante ainda mencionar que nosso trabalho utiliza Flashbots como uma aproximação para o comportamento de usuários no Ethereum que visam a exploração de lucros máximos provenientes da especulação de ativos digitais. Em [Daian et al. 2020, Capponi et al. 2022] são analisados os riscos que o uso de serviços para arbitragem de criptoativos como Flashbots oferecem para a segurança do Ethereum, podendo afetar negativamente o funcionamento da plataforma e a experiência dos usuários. Contudo, esses trabalhos não exploram métricas de grafos e análises temporais tendo como referência um evento de impacto na economia.

3. Descrição dos dados

3.1. Caracterização dos dados

As tropas russas invadiram o território leste da Ucrânia no dia 24/02. A partir disso, optamos por subdividir nosso conjunto de dados em quatro semanas. As semanas 1 e 2 são definidas pelos blocos inicial e final, respectivamente com os identificadores 14174989 e 14265470, caracterizam o período pré-invasão. Por sua vez, as semanas 3 e 4 compostas pelos blocos inicial e final, respectivamente com os identificadores 14265812 e 14355747, definem o período pós-invasão.

Para as análises, optamos por caracterizar o comportamento da rede sob dois pontos de vista. O primeiro, é referente ao contexto geral, em que é utilizado como base de dados todas as transações ocorridas na rede durante o período de coleta. O segundo aborda um contexto específico no qual focamos nas transações que interagem com o serviço Flashbots Auction.

Transações que interagem com esse mecanismo, após passarem por uma verificação de erros em um *gateway* denominado MEV-Relay, são enviadas diretamente para os mineradores, tornando-as invisíveis na rede até serem mineradas. Isso, além de prevenir a ocorrência de ataques que tentam roubar essas receitas, contribuem para a melhor experiência dos usuários em relação ao gasto de taxas para transações com falha, tornando Flashbots um mecanismo mediador de transações relevante para a nossa análise.

Dentre os dados coletados, definimos como volume de transações todas as negociações processadas com sucesso na rede Ethereum durante o período de coleta. Assim sendo, definimos as contas como todos os endereços individuais que participam de uma transação, sendo eles remetentes ou destinatários. O conjunto de contas que compõem nossa base de dados engloba tanto contratos inteligentes quanto endereços de carteiras de usuários, não sendo necessária sua diferenciação para a construção das análises de volume de contas. A distinção entre contrato e usuário foi realizada ao identificar endereços que não possuem tag pública no Etherscan na seção 5.3.

3.2. Forma de coleta

Para formar nossa base de dados, coletamos todas as transações realizadas na blockchain Ethereum entre os dias 10/02/2022 e 10/03/2022, sendo elas pertencentes ao intervalo

fechado definido entre os blocos 14174989 e 14355747. Esse intervalo de tempo foi escolhido de forma a obter informações comportamentais da rede antes e depois da invasão da Ucrânia pela Rússia. A coleta das transações foi feita através das APIs Etherscan.io⁶ e blocks.flashbots.net⁷. A primeira foi utilizada para a obtenção de todas as transações ocorridas na rede Ethereum durante o período de coleta, sendo a fonte para a obtenção das características principais de cada transação. Já a segunda foi usada para a identificação das transações do tipo Flashbots.

Ambas as APIs possuem propósitos distintos, enquanto o Etherscan.io fornece todos os dados públicos das transações do Ethereum, o blocks.flashbots.net fornece informações voltadas para a extração de receitas MEV, como por exemplo a quantidade de ether transferidas para a coinbase, taxas de transação e lucros totais do minerador. Tendo em vista o propósito deste trabalho, concentramos nossos esforços na obtenção dos dados gerais que possibilitem a caracterização da rede sem aprofundar no campo da arbitragem e extração das receitas MEV. Ambas as transações, gerais e transações do tipo Flashbots, possuem os mesmos atributos coletados. A Tabela 1 mostra os dados utilizados para as análises.

Tabela 1. Características extraídas de transações do Ethereum.

Atributo	Descrição
hash	Código hash que identifica cada transação
blockNumber	Número do bloco (necessário para ordenação)
timestamp	<i>Timestamp</i> definindo a data em que a transação foi processada
to	Conta destinatária da transação
from	Conta remetente da transação

4. Modelagem

Para realizar uma caracterização da rede, inicialmente nós modelamos o nosso problema utilizando grafos temporais direcionados para representar dois conjuntos dentro da rede principal do Ethereum: o conjunto C_1 , com todas as transações externas coletadas no período de 10/02 a 10/03; e o conjunto C_2 , com todas as transações que interagem com o Flashbots Auction dentro do mesmo intervalo de tempo.

Seja um grafo estático G definido como uma tupla (V, A) , com V como um conjunto de vértices e A um conjunto de arestas, sendo $A \subseteq \{(u, v) \mid u, v \in V\}$. Sendo (u, v) um par ordenado, G é também considerado um grafo direcionado. Diante disso, um grafo temporal direcionado é definido como uma sequência de grafos estáticos direcionados, em função de uma variável discreta t . A Figura 1 mostra um diagrama representando um grafo temporal direcionado. Os círculos representam os vértices do grafo, estando preenchidos conforme são adicionados ao grafo anterior.

No caso desse trabalho, grafos temporais serão usados em duas instâncias diferentes: Análise de principais contas e Análise de novas contas.

⁶<https://etherscan.io/>

⁷<https://blocks.flashbots.net/>

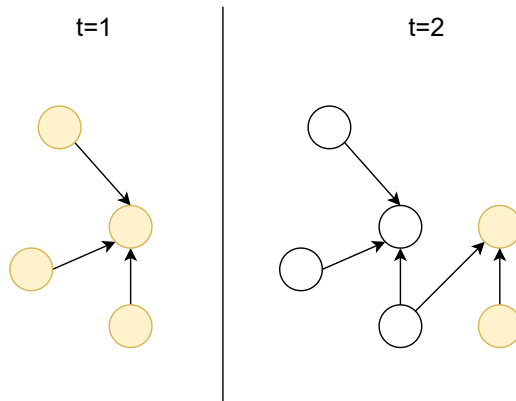


Figura 1. Exemplo de grafo temporal direcionado.

4.1. Análise de principais contas

Nessa situação, a variável discreta t representa diferentes semanas em que focamos nossas análises. Portanto, G_1 representa um grafo na primeira semana dentro do intervalo de análise; isto é: a semana que contempla o primeiro bloco do dia 10/02 até o último bloco do dia 16/02. Da mesma forma, G_2 forma um intervalo do primeiro bloco do dia 17/02 até o último do dia 23/02 e assim por diante.

Para avaliar a relevância de uma determinada conta em um período nós nos focamos na métrica de grau. Um grau representa nesse problema o número de transações que uma conta recebe ou envia, ou seja, o número de arestas que se conectam com o vértice em questão. Separamos também a métrica de grau de entrada, que considera apenas transações com a conta em questão sendo o destino da transação e grau de saída, considerando apenas transações com a conta em questão sendo a origem da transação.

Entendemos que contas com alto grau ou contas que mostram um alto crescimento de grau de uma semana para a outra se mostram como contas relevantes a curto/médio prazo, e portanto, serão o objeto de maior interesse neste trabalho.

4.2. Análise de novas contas

Para esse cenário, a variável t passa a representar dias que se passaram a partir do primeiro. Assim, G_1 representa um grafo contendo todos os blocos e transações que entraram na blockchain no dia 10/02, G_2 todos os blocos e transações que entraram na blockchain no dia 11/02 e assim por diante.

O objetivo dessa abordagem é analisar o volume de contas envolvidas em transações de cada dia e de quantas dessas contas já haviam sido observadas com atividade recente na rede. Para definir um ponto inicial, realizamos uma coleta de todas as contas que haviam aparecido em transações na rede entre 10/01 e 10/02 e as inserimos como um ponto de partida em G_1 , adicionando ao grafo temporal contas que já haviam participado de transações recentes.

Seja N_t o número de vértices que o grafo temporal tem no dia t . Para cada dia t , temos que o volume diário de novas contas é definido por $N_t - N_{t-1}$. Para o dia 1, o número de novas contas é definido de maneira arbitrária como N_1 . Nesse contexto, o

volume de contas ativas em um dia t é definido pelo número de vértices de G_t que têm no mínimo uma transação com *timestamp* que corresponde ao dia t .

5. Caracterização

Nesta seção, apresentamos os resultados encontrados para as análises realizadas sobre a rede Ethereum de transações no período descrito na Seção 3. Utilizamos as técnicas de modelagem apresentadas anteriormente para analisar o volume de transações, a atividade das contas e posteriormente elaborar o ranqueamento dos nós com base na mudança de grau entre as semanas. Como este é um trabalho de caracterização, focamos em apresentar os resultados sem a preocupação de entender as causas e motivações para eles.

5.1. Volume de Transações

Na Figura 2, apresentamos os resultados obtidos para o volume de transações da rede. Para isso, construímos gráficos temporais relacionando cada transação com a data em que ela ocorreu de forma a obter o total diário de negociações. Como descrito anteriormente, separamos as análises em dois pontos de vista, o primeiro como uma visão geral da rede e o segundo sob o contexto dos Flashbots. Tendo isso em vista, é válido destacar que os gráficos da Figura 2 estão em escalas diferentes, fazendo com que as curvas de cada um devam ser analisadas separadamente.

Primeiramente analisamos o conjunto C_1 , referente ao comportamento geral do sistema, representado pela Figura 2(a). Nela, podemos observar uma evidente diferença entre os períodos antes e depois da invasão, em que em meados de fevereiro, a rede apresentou a ocorrência de grandes picos de transações, sendo o mais significativo de aproximadamente 1.35 milhões próximo ao dia 20 de fevereiro. Em contrapartida, é possível destacar uma evidente queda nesse número após o dia 20, fazendo com que o total de transações em um dia chegasse a um valor inferior a 1.10 milhões no início de março.

Posteriormente, fizemos as mesmas análises para o conjunto C_2 , referente às transações Flashbots, as quais são representadas pela Figura 2(b). Diferentemente do contexto geral, o conjunto C_2 apresenta comportamento de crescimento ao longo de todo o período analisado, possuindo uma queda mais intensa apenas entre os dias 10 e 15 de fevereiro, fazendo o total de negociações atingir um valor inferior a 20 mil. É válido destacar também que após a invasão, apesar de o volume de transações continuar crescendo, as oscilações foram mais significativas que antes do dia 24 de fevereiro, com variações superiores a 6 mil transações.

5.2. Atividade das Contas

Neste tópico, apresentamos os resultados para a análise da atividade das contas. Como discutido na Seção 4, modelamos a rede como um grafo orientado em que cada conta corresponde a um nó. A partir disso, construímos gráficos de tempo para relacionar a atividade desses nós ao longo dos dias do período analisado, contrapondo o volume de contas ativas com a ocorrência de novas contas. Todos os resultados são mostrados na Figura 3.

Para o conjunto C_1 , Figura 3(a), observamos que a atividade das contas permanece estável, apesar de observarmos uma diminuição de endereços ativos entre os dias 10 e 20 de fevereiro, mantendo o volume de nós ativos entre 450 mil e 550 mil. Após isso, a curva

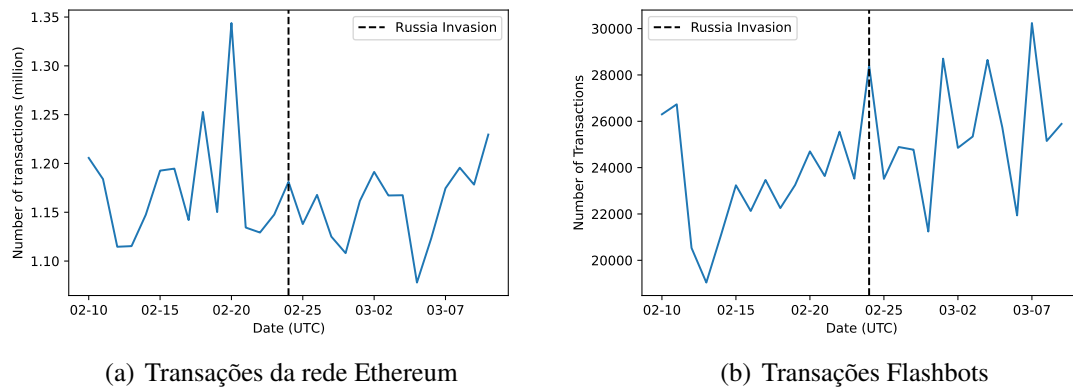


Figura 2. Volume diário de transações.

passa a possuir uma tendência de crescimento iniciada próximo à invasão que se estende até o início de março. Analogamente, o volume de novas contas segue o mesmo padrão, variando entre 200 mil e 300 mil novas contas em meados de fevereiro e posteriormente sendo caracterizado por um crescimento até o final do período de análise, tendo uma variação mais acentuada próximo ao dia 10 de março em que o volume de novos nós se aproxima de 350 mil.

Em relação ao conjunto C_2 , Figura 3(b), nota-se que apesar da ocorrência de uma queda de cerca de 5 mil contas em relação à quantidade de nós ativos entre os dias 10 e 15 de fevereiro, o gráfico mantém a tendência de crescimento ao longo do tempo, possuindo variações mais intensas a partir do dia da invasão. Nesse âmbito, nota-se que, assim como para o conjunto C_1 , a curva de novas contas segue um padrão semelhante à curva de endereços ativos, com a primeira apresentando um crescimento significativamente mais suave que a segunda, mantendo a variação em aproximadamente mil endereços.

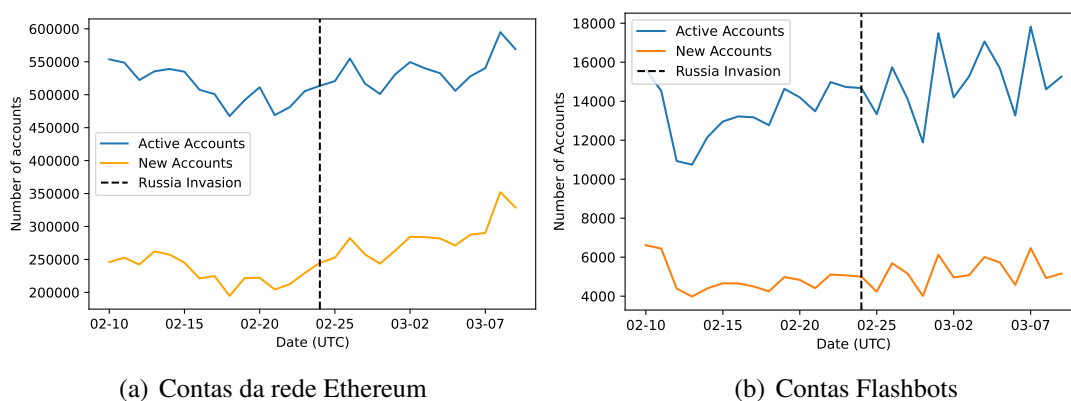


Figura 3. Contas ativas e contas novas.

5.3. Principais Contas

Como discutido na Seção 4.1, modelamos a rede por meio de grafos direcionados. As Figuras 4 e 5 mostram a distribuição de valores de diferentes graus de entrada e de saída

entre as contas durante cada semana. O maior volume de transações na base de dados da rede principal diminui a incerteza dentro dessa distribuição.

Nota-se que o comportamento das curvas em azul e laranja nos gráficos da Figura 4 mostram que algumas contas, em quantidade pequena, possuem grau de saída maiores, enquanto a curva de grau de entrada não atinge de forma contundente valores tão altos. Dessa forma, o perfil dessa base de dados nesse período indica a presença de contas distribuindo muitas transações para diferentes contas e muitas contas recebendo poucas transações. Esse comportamento não se altera de maneira significativa com o passar das semanas.

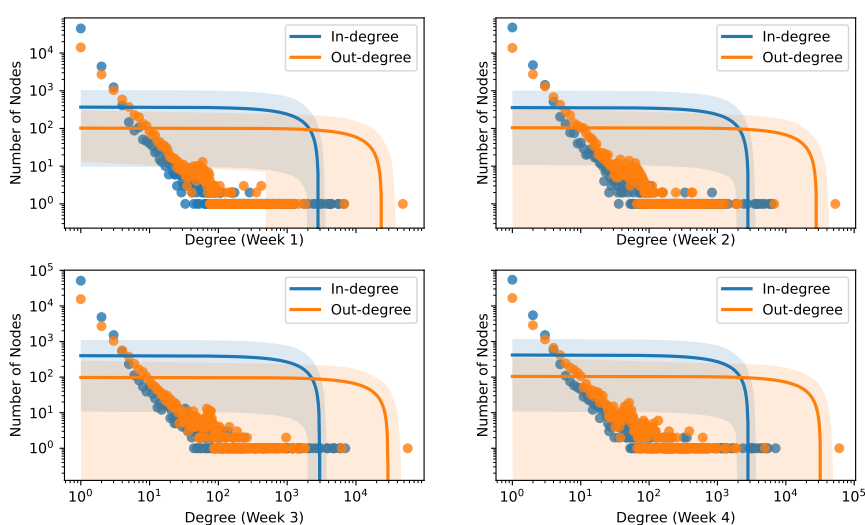


Figura 4. Relação de Grau Entre Semanas Flashbots

Observando a Figura 5, esse padrão entre as curvas se inverte. Nesse caso, parece haver um maior número de contas com alto grau de entrada, o que reflete um comportamento um pouco diferente, com mais contas recebendo transações de muitos usuários diferentes. É importante ressaltar que nesse caso as curvas se aproximam mais umas das outras, o que indica um comportamento mais equilibrado nesse sentido. Da mesma forma, o passar das semanas não alterou de maneira impactante o comportamento da rede.

Além de uma observação geral sobre os graus das contas, nós realizamos um ranqueamento a fim de encontrar contas consideradas relevantes para o período em questão. A relevância de uma conta, nesse trabalho, é definida pelo quanto o grau de uma conta aumenta de uma semana para outra, isto é, com quantas contas passou a enviar e receber transações.

Isso posto, realizamos uma análise comparativa das quatro semanas, comparando as contas que mais aumentavam seu grau entre uma semana e a semana seguinte. A fim de compactar os resultados, iremos mostrar apenas as 10 contas de maior relevância no período. Adicionalmente, endereços hash de cada conta serão encurtados aos últimos sete caracteres do endereço. Por exemplo, a conta *0xa090e606e30bd747d4e6245a1517ebe430f0057e* será mostrada apenas como *0f0057e*.

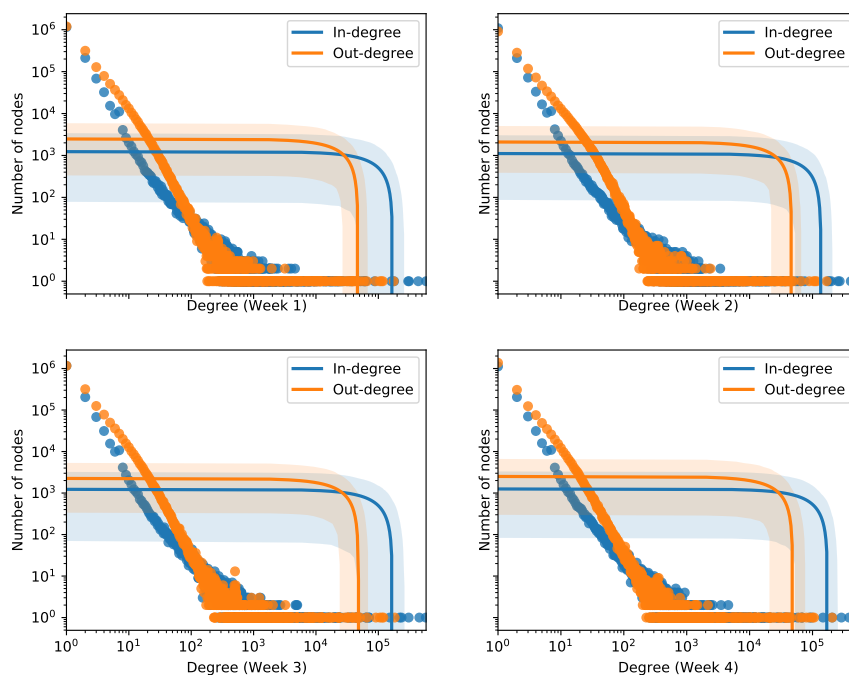


Figura 5. Relação de Grau Entre Semanas Rede Ethereum

Para facilitar a identificação das contas, rotulamos cada conta de acordo com tags disponíveis publicamente no Etherscan.

Dentro desse período de coleta, as duas primeiras semanas descrevem o período anterior à invasão russa. Possíveis efeitos de uma tensão pré-conflito podem ser refletidos dentro desse período. Já as semanas 3 e 4 descrevem o período após a invasão, que podem conter efeitos e consequências da nova situação.

O primeiro intervalo analisado foi o intervalo das duas primeiras semanas. Observa-se que, conforme a Tabela 2 demonstra, uma grande quantidade de contas relacionadas à negociação de tokens se destaca. X2Y2⁸, por exemplo, trata de um *marketplace* para trocas e negociações de NFTs. Isso também ocorre no contexto dos Flashbots. Como mostrado na Tabela 3, a conta que obteve maior crescimento de grau foi o Open-Sea⁹, que também trata de um mercado focado na negociação de tokens. Além disso, nota-se a presença de um endereço de carteira sem tag pública no Etherscan que obteve um aumento de grau de 1200 unidades, assim como a ocorrência de outros ativos como USDT Stablecoin com Tether¹⁰ e agregador DEX com 1inch¹¹. É válido destacar também, o aparecimento de bots de extração de MEV como endereços relevantes, tendo em vista o objetivo dos Flashbots como ambiente seguro e transparente para a extração dessas

⁸<https://x2y2.io/>

⁹<https://opensea.io/>

¹⁰<https://tether.to/>

¹¹<https://app.1inch.io/>

receitas.

Tabela 2. Comparação de principais contas entre a primeira e a segunda semana na rede Ethereum.

Endereço	Tag	Crescimento de Grau
1abebc9	X2Y2: X2Y2 Token	44774
49a41fa	X2Y2: X2Y2 Drop	27772
a67eed3	X2Y2: Exchange	24353
b23c98a	Cat Blox: CATBLOXGEN Token	17192
c756cc2	Wrapped Ether	15267
76a1b85	X2Y2: Fee Sharing System	14792
147ea85	ENS: Base Registrar Implementation	12849
903a5d0	The Sandbox: SAND Token	12720
5fd74c0	<i>Contrato: Sem tag pública</i>	12403
def3c7a	<i>Contrato: Sem tag pública</i>	11541

Tabela 3. Comparação de principais contas entre a primeira e a segunda semana no âmbito dos Flashbots.

Endereço	Tag	Crescimento de Grau
bB538E5	OpenSea: Wyvern Exchange v2	3787
5843dE9	<i>Usuário: Sem tag pública</i>	1200
991e2D4	MEV Bot: 0x000...2D4	833
7455580	MEV Bot: 0x8aF...580	768
57Fb793	Wintermute 1	597
643097d	1inch v4: Router	335
140449c	<i>Contrato: Sem tag pública</i>	325
5206C3E	<i>Contrato: Sem tag pública</i>	287
3f7c613	<i>Contrato: Sem tag pública</i>	282
D831ec7	Tether: USDT Stablecoin	259

Em seguida, foi feita a comparação entre as semanas 2 e 3 do período de coleta. Essa análise permite observar transformações que a rede Ethereum teve no período da invasão russa, comparando a semana imediatamente anterior e a primeira semana posterior ao fato. Nota-se, comparando a Tabela 2 com a Tabela 4, que os tokens anteriormente em alta deram lugar a uma variedade maior de perfis de contas. A exchange Coinbase passa a se destacar um pouco mais. Nota-se também a maior presença de contratos relacionados a outros ativos, como USDT Stablecoin ou USD Coin. Por fim, a conta 7455580 mostra até mesmo um bot voltado à extração de MEV.

Em relação aos Flashbots, comparando-se as Tabelas 3 e 5, é possível destacar o aumento do número de MEV bots dentre os nós mais relevantes, assim como o aparecimento de endereços sem tags públicas na rede. Além disso, é válido salientar que Ethermine¹² aparece em primeira posição na Tabela 5 como o nó com maior crescimento

¹²<https://ethermine.org/>

de grau, sendo esse crescimento quase 55 mil unidades maior que a conta que ocupa a segunda posição da tabela.

Tabela 4. Comparação de principais contas entre a segunda e a terceira semana na rede Ethereum.

Endereço	Tag	Crescimento de Grau
0f0057e	Coinbase: Miscellaneous	106853
bb538e5	OpenSea: Wyvern Exchange v2	101837
d831ec7	Tether: USDT Stablecoin	48732
606eb48	Centre: USD Coin	35541
8d01279	Celsius Network: Wallet 5	23776
7975ef8	OogaVerse: MekaApes Game Contract	16276
b898ec8	Ethermine	15246
7455580	MEV Bot: 0x8aF...580	13650
dc49699	Coinbase 4	13600
bf77006	<i>Contrato: Sem tag pública</i>	12533

Tabela 5. Comparação de principais contas entre a segunda e a terceira semana no âmbito dos Flashbots.

Endereço	Tag	Crescimento de Grau
B898ec8	Ethermine	56624
991e2D4	MEV Bot: 0x000...2D4	1881
0a3f8e7	MEV Bot: 0x4Cb...8e7	1568
C378B9F	SushiSwap: Router	1324
5645718	<i>Usuário: Sem tag pública</i>	1195
e416B40	MEV Bot: 0x000...B40	1191
0fDd6CF	MEV Bot: 0xa57...6CF	1117
7455580	MEV Bot: 0x8aF...580	724
01Db497	<i>Usuário: Sem tag pública</i>	703
08850aF	<i>Usuário: Sem tag pública</i>	666

As duas últimas semanas formam a última janela de análise, comparando semanas posteriores à invasão. Observando a Tabela 6, algumas características se mantêm em relação à Tabela 4, como a presença de bots de extração de MEV e a ainda alta relevância de contas como Ethermine e Coinbase: Miscellaneous. Contas de token voltam a surgir com relevância, da mesma forma que nas duas primeiras semanas, o que pode ser visto, por exemplo, com o crescimento do protocolo Uniswap, que pode ser utilizado para troca e aquisição de tokens¹³. Outra nova observação nessa janela é a presença de contas com maior relevância que não possuem tags públicas de identificação no Etherscan. O mesmo comportamento é observado em relação aos Flashbots que, conforme mostra a Tabela 7, mantém MEV bots entre os nós com maior variação de grau, além da maior relevância de nós voltados para o comércio de tokens, como o Uniswap já mencionado.

¹³<https://uniswap.org/faq>

Tabela 6. Comparação de principais contas entre a terceira e a quarta semana na rede Ethereum.

Endereço	Tag	Crescimento de Grau
33ab239	Livepeer: LPT Token	95535
0f0057e	Coinbase: Miscellaneous	76216
97b3fca	<i>Contrato: Sem tag pública</i>	56225
665fc45	Uniswap V3: Router 2	52794
b898ec8	Ethermine	21609
9f2488d	Uniswap V2: Router 2	19930
500fb08	<i>Contrato: Sem tag pública</i>	17267
d831ec7	Tether: USDT Stablecoin	16330
0a3f8e7	MEV Bot: 0x4Cb...8e7	12988
6155ba9	KPOP CTzen: KCPT1 Token	11093

Tabela 7. Comparação de principais contas entre a terceira e a quarta semana no âmbito dos Flashbots.

Endereço	Tag	Crescimento de Grau
B898ec8	Ethermine	3950
0a3f8e7	MEV Bot: 0x4Cb...8e7	2986
40f594e	MEV Bot: 0x000...94e	1398
9F2488D	Uniswap V2: Router 2	1306
3923BcA	<i>Usuário: Sem tag pública</i>	922
9e5D3Fa	<i>Contrato: Sem tag pública</i>	636
80E83b6	Gelato Network: Gelato	444
665Fc45	Uniswap V3: Router 2	421
643097d	linch v4: Router	409
A7fAc82	<i>Usuário: Sem tag pública</i>	333

6. Conclusões

Neste trabalho, caracterizamos a rede do Ethereum de maneira geral e específica, construindo um modelo evolutivo da rede e realizando análises quantitativas e qualitativas sobre suas contas. Com isso, buscamos quantificar os nós ativos na rede e, por fim, isolamos e analisamos as contas com maior relevância durante aquele período.

Nossas investigações indicam um caminho inicial para monitoramento de possíveis efeitos de importantes eventos externos sobre uma grande plataforma de criptoativo. Foi possível observar mudanças de curto prazo em relação ao comportamento de contas e transações na rede, além do contraste entre o comportamento de transações na rede geral e de transações realizadas com o Flashbots Auction.

É importante ressaltar que esse trabalho busca fazer apenas uma caracterização concentrada em um período e que essas análises verificam um comportamento a curto prazo. Portanto, não é possível fazer inferências de causa e consequência em relação à invasão apenas observando esses detalhes específicos.

Para trabalhos futuros, pretendemos usar janelas temporais mais amplas e analisar de maneira mais detalhada os nós de maior influência a fim de possibilitar inferências causais de maneira mais assertiva. Outro ponto focal é expandir a investigação do impacto de eventos externos para outros acontecimentos passados que possuam relevância no âmbito econômico.

Agradecimentos

Os autores agradecem o apoio financeiro do CNPq, FAPEMIG, Capes e UFJF.

Referências

- Agarwal, R., Barve, S., and Shukla, S. K. (2021). Detecting malicious accounts in permissionless blockchains using temporal graph properties. *Applied Network Science*, 6(1):9.
- Bai, Q., Zhang, C., Xu, Y., Chen, X., and Wang, X. (2020). Poster: Evolution of ethereum: A temporal graph perspective. In *2020 IFIP Networking Conference (Networking)*, pages 652–654. IEEE.
- Capponi, A., Jia, R., and Wang, Y. (2022). The evolution of blockchain: from lit to dark. *arXiv preprint arXiv:2202.05779*.
- Chen, T., Li, Z., Zhu, Y., Chen, J., Luo, X., Lui, J. C.-S., Lin, X., and Zhang, X. (2020). Understanding ethereum via graph analysis. *ACM Trans. Internet Technol.*, 20(2).
- Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., and Juels, A. (2020). Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. IEEE.
- Miller, A., Litton, J., Pachulski, A., Gupta, N., Levin, D., Spring, N., and Bhattacharjee, B. (2015). Discovering bitcoin’s public topology and influential nodes. Technical report, University of Maryland, College Park.
- Sun, Y., Xiong, H., Yiu, S. M., and Lam, K. Y. (2019). Bitvis: An interactive visualization system for bitcoin accounts analysis. In *2019 Crypto Valley conference on blockchain technology (CVCBT)*, pages 21–25. IEEE.
- Zanelatto Gavião Mascarenhas, J., Ziviani, A., Wehmuth, K., and Vieira, A. B. (2020). On the transaction dynamics of the ethereum-based cryptocurrency. *Journal of Complex Networks*, 8(4):cnaa042.
- Zhao, L., Sen Gupta, S., Khan, A., and Luo, R. (2021). Temporal analysis of the entire ethereum blockchain network. In *Proceedings of the Web Conference 2021*, pages 2258–2269.