Detecção de Mineração Egoista: Quando o poder varia

Willian Henrique Vilela Casa Grandi [1], **Ivan da Silva Sendin**[1]

Faculdade de Computação (FACOM) – Universidade Federal Uberlândia(UFU)

{williancasagrandi,sendin}@ufu.br

Resumo. *A mineração é um dos alicerces do funcionamento das criptomoedas. O correto funcionamento desse sistema depende da participação dos mineradores. No ambiente descentralizado, o comportamento honesto é incentivado pelos protocolos, assumindo-se que a obediência a eles maximiza os ganhos. Um desvio nesse comportamento, chamado de Mineração Egoísta, pode aumentar os lucros dos mineradores que o praticam e comprometer a segurança da criptomoeda. Atualmente, a identificação desse tipo de comportamento é complexa e realizada por meio de ferramentas estatísticas que assumem que os mineradores possuem poder computacional estável durante o período analisado. Neste trabalho, investigamos se os mineradores de fato apresentam poder computacional estável e avaliamos as consequências da variação desse poder nos métodos atuais.*

Abstract. *Mining is one of the foundations of cryptocurrency. The proper functioning of this system depends on the participation of miners. In a decentralized environment, honest behavior is encouraged by protocols, assuming that compliance maximizes profits. A deviation from this behavior, called Selfish Mining, can increase the profits of the miners who practice it and compromise the security of the cryptocurrency. Currently, identifying this type of behavior is complex and performed using statistical tools that assume that miners have stable computing power during the analyzed period. In this work, we investigate whether miners actually have stable computing power and assess the consequences of variations in this power under current methods.*

1. Introdução

O Bitcoin é uma criptomoeda descentralizada cujo correto funcionamento depende da aderência de seus participantes aos protocolos que a definem. As transações entre seus usuários são armazenadas na *blockchain*, que é mantida pelos mineradores: nós da rede que validam as transações e obtêm o direito de escrever na blockchain por meio do mecanismo chamado de Prova de Trabalho. Esse mecanismo, responsável por estabelecer um estado de consenso distribuído, pode ser entendido como uma loteria: um processo estocástico determina qual minerador terá a chance de escrever o próximo bloco, ao mesmo tempo em que remunera os participantes pelo trabalho executado. A honestidade dos mineradores nesse processo é fundamentada na Teoria dos Jogos, sob a suposição de que seguir estritamente os protocolos garantiria tanto a segurança do sistema quanto a maximização dos ganhos individuais [Nakamoto 2009].

Em [Eyal and Sirer 2014], foi descrito um comportamento — denominado Mineração Egoísta (ME), ou Selfish Mining em inglês — que pode ser adotado por mineradores com o objetivo de aumentar seus lucros, mesmo que isso comprometa a segurança

da criptomoeda. A detecção de mineradores egoístas por meio da análise da blockchain já foi abordada em diversos trabalhos [Schwarz-Schilling et al. 2022, Li et al. 2024, Silva and Sendin 2024], que geralmente se baseiam em métodos estatísticos voltados à identificação de anomalias. Um problema comum nessas abordagens é que elas exigem conhecimento prévio do poder computacional de cada minerador, assumindo que esse poder permaneça estável durante o período analisado — o que nem sempre é o caso.

A contribuição deste trabalho se dá em duas frentes: i) a análise do ecossistema de mineração de Bitcoin com o objetivo de estudar o poder computacional dos participantes; ii) a aplicação de métodos existentes para a detecção de ME, adaptando-os ao cenário em que o poder computacional dos mineradores varia ao longo do tempo.

2. Background

As tarefas dos mineradores no Bitcoin podem ser resumidas em: recolher as transações e validá-las verificando a existência de fundos e a corretude das assinaturas. Uma vez que um conjunto de transações válidas seja obtido, os mineradores as agrupam em um bloco. O protocolo do Bitcoin prevê que a primeira transação de cada bloco é uma transação diferente - chamada de `Coinbase` - nela o minerador coloca o próprio endereço como destino de criptomoedas que estão sendo criadas, desta forma ele obtém a remuneração pelo seu trabalho. De forma simplificada, podemos dizer que para que um bloco seja aceito pelos demais participantes ele deve ter a seguinte propriedade:

$$\mathcal{H}(bloco|r) < k,$$

onde $\mathcal{H}$ é uma função de hashing criptográfica; $bloco$ são as transações do período e o valor k é a dificuldade do trabalho. Uma vez que $bloco$ pode ser visto como uma sequência de bits fixa para um determinado conjunto de transações, o ponto central da mineração é a busca pelo valor de r que produza o *hash code* desejado. Essa busca exige força bruta, e as chances de um determinado minerador obter r são proporcionais ao poder computacional empregado. Uma vez que o r seja encontrado, o minerador propaga o bloco aos demais mineradores para obter a sua remuneração. Dado que o bloco é propagado entre os mineradores, o processo se reinicia com um conjunto novo de transações.

Em geral, cada bloco pode ter o seu minerador identificado pelos endereços contidos na transação `Coinbase`, desta forma, é possível inferir o poder computacional relativo de cada participante observando a sua produção de blocos em uma determinada janela de tempo [Schwarz-Schilling et al. 2022, Li et al. 2020a].

2.1. Mineração Egoista

Em [Eyal and Sirer 2014], foi observado que um desvio do protocolo original do Bitcoin poderia produzir maiores ganhos aos mineradores: uma vez que o bloco n seja encontrado, o minerador não propaga o bloco pela rede, mas fica trabalhando no bloco $n + 1$ sozinho, visando obter vantagem na busca por esse bloco. Devido a esta característica do minerador trabalhar sozinho, sem informar os concorrentes, este procedimento foi chamado de Mineração Egoísta (ME) ou, em Inglês, Selfish Mining (SE).

Esta prática é uma aposta, pois a não propagação de um bloco pode causar a perda da sua remuneração. No artigo [Eyal and Sirer 2014] os autores sugerem que o minerador deve ter 25% a 33% do poder computacional para esta prática ser lucrativa.

Importante observar que a prática ME deve deixar traços na Blockchain, pois deve produzir uma quantidade de blocos consecutivos desproporcional ao seu poder computacional e justamente essa característica é usada na sua detecção.

2.2. Mineração em Pool

A mineração de Bitcoin é uma atividade rentável e altamente competitiva. Um usuário sozinho pode levar centenas de anos para minerar um único bloco e obter lucro. Durante esse tempo, ele precisa arcar com os custos operacionais e ainda corre riscos, como a queda no valor do Bitcoin ou falhas no *hardware*. Por isso, o método usual de mineração é a organização em *pools* de mineração: uma entidade centraliza as operações, recebe e valida transações e monta um *template* de bloco a ser minerado. Nesse modelo, os mineradores executam a prova de trabalho sobre o *template* fornecido pelo *pool*, modificando apenas o campo da prova de trabalho. Todo o processo é controlado pelo protocolo *Stratum*, que não exige compromisso fixo dos mineradores com um único *pool*, permitindo a migração do poder computacional entre diferentes *pools*. Detalhes sobre o funcionamento e a segurança do protocolo podem ser encontrados em [Sannicolo 2023, Recabarren and Carbunar 2017].

Alguns *pools* ainda oferecem a possibilidade de mineração em nuvem: alguém interessado pode "alugar" um certo poder computacional com o *pool* e receber o lucro proporcional ao poder contratado. Outro serviço oferecido por alguns *pools* é o "Acelerador de Transações": o *pool*, em conjunto com seus parceiros, consegue acelerar a inclusão de uma determinada transação na blockchain. Essa prática evidencia que os *pools*, embora concorrentes, podem agir em conluio quando conveniente e se desviar do protocolo quando for de seu interesse. A prática de priorizar transações fora do protocolo é chamada de transações opacas e foi estudada em [Messias et al. 2021].

Na Tabela 1, são apresentados os principais *pools* do ano de 2024. Os dados foram obtidos em fevereiro de 2025 por meio de consultas aos respectivos sites. Nas Figuras 1 e 2, é mostrada a variação do *hashrate* dos *pools* de mineração durante o mês de fevereiro de 2025. O *hashrate* foi obtido de duas formas: na Figura 1, foram realizadas consultas aos *sites* de cada *pool* e o valor infomado pelo *pool* foi obtido; na Figura 2, foi observada a proporção de blocos minerados por cada *pool* no período estudado, desta forma, inferindo o seu poder comoputaciional relativo. Nota-se uma diferença entre os dados informados pelos *pools* e aqueles obtidos diretamente da *blockchain*. Essa diferença pode refletir alegações falsas feitas pelos *pools* ou estar relacionada a outros fatores, como, por exemplo, a conectividade. Além disso, observa-se que o poder computacional aferido variou consideravelmente ao longo do mês, independentemente da origem dos dados. Esse fato tem implicações imediatas nos métodos utilizados para a detecção de ME.

3. Trabalhos Relacionados

A busca pela identificação de Mineração Egoísta (ME) usando dados da blockchain tem atraído atenção, e recentemente alguns trabalhos abordaram esse problema. Em comum, esses estudos utilizam a contagem de blocos minerados em sequência pelo mesmo minerador e comparam o valor observado na blockchain com o valor esperado para um determinado poder computacional. Quando o valor observado se desvia muito do valor esperado, conclui-se que a ME está sendo praticada e influenciando essas ocorrências.

Tabela 1. Principais *pools* de mineração de Bitcoin. Os dados foram obtidos por meio de consultas aos respectivos sites públicos. As colunas `Nuvem` e `Acelerador` indicam se o *pool* oferece esses serviços. EH/s (exahashes por segundo) é uma unidade que representa 10^{18} tentativas de cálculo de hash por segundo, usada para medir o poder computacional empregado na mineração de blocos.

Pool	Poder Computacional	Nuvem	Acelerador
Ant Pool	157 EH/s	Sim	Sim
F2Pool	90,10 EH/s	Sim	Sim
Binance Pool	58,30 EH/s	Sim	Sim
BTC.com	156 EH/s	Sim	Sim
Braiins Pool	13 EH/s	Sim	Sim
Poolin	3,69 EH/s	Sim	Sim
SBI Crypto	9 EH/s	Sim	Sim
Foundry USA Pool	–	–	–
ViaBTC	117,29 EH/s	–	Sim
MaraPool	–	Sim	–
SpiderPool	25,89 EH/s	–	–

Nos trabalhos [Li et al. 2020b, Li et al. 2020a], os autores introduzem uma metodologia estatística para identificar anomalias na mineração, baseada na criação de uma distribuição nula por meio de permutações. O método funciona mantendo fixa a quantidade total de blocos minerados por cada entidade em um determinado período, enquanto a ordem de descoberta desses blocos é embaralhada repetidamente. O desvio entre a contagem real de blocos consecutivos e a média das contagens obtidas nas permutações é, então, quantificado através do Teste Z. Essa abordagem parte de duas premissas fundamentais. Primeiramente, o uso do Teste Z requer que a distribuição da contagem de blocos consecutivos siga uma Distribuição Normal. Em segundo lugar, o modelo de permutação aleatória só é válido se o poder computacional dos mineradores for considerado estável durante o intervalo analisado, apenas sob essa condição se pode assumir que uma ordem de mineração aleatória representa um comportamento honesto.

De forma similar, em [Li et al. 2024], que propõe um teste sem o uso de permutações. Este método também foca na contagem de blocos sucessivos, mas modela a probabilidade dessa ocorrência sob a hipótese de mineração honesta utilizando uma distribuição binomial tipo II de ordem 2. Uma contribuição deste trabalho é a aplicação de heurísticas de agrupamento de endereços para aprimorar a estimativa do poder computacional real dos mineradores, corrigindo distorções causadas pelo uso de múltiplos endereços por uma mesma entidade.

Já em [Silva and Sendin 2024], foi proposta uma estratégia não paramétrica como um aprimoramento direto sobre os métodos baseados em Z-Score. O autor critica a dependência da suposição de normalidade e desenvolve um teste que, embora também utilize permutações, evita o cálculo do Z-Score. Em vez disso, a significância estatística é obtida através de um p-value empírico, que representa a frequência com que a contagem original de blocos consecutivos supera as contagens geradas nos embaralhamentos. A análise é segmentada em janelas mensais para capturar variações do hashrate, tornando

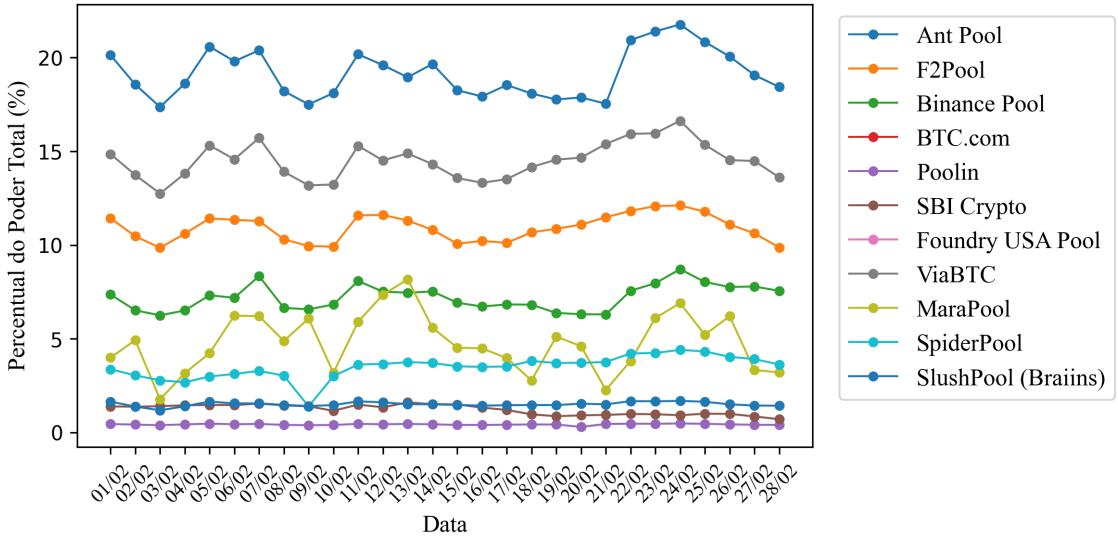

Figura 1. Gráfico do poder computacional alegado nos sites das pools em fevereiro de 2025. O poder computacional nesse grafico foi calculado usando o hashrate total da rede, fornecido nos proprios dominios, e o hash power próprio alegado pela mineradora.

o método mais adaptável à natureza volátil da mineração sem depender de suposições de distribuições estatísticas idealizadas, permitindo uma detecção mais precisa da ME.

4. Análises

4.1. Métodos atuais

Os métodos analisados neste trabalho são classificados em duas abordagens diferentes: testes paramétricos e não paramétricos.Os testes paramétricos, como mencionado anteriormente, consistem no uso de indicadores estatísticos para identificar possíveis mineradores praticantes de ME. Esse tipo de teste parte do pressuposto de que os dados seguem uma Distribuição Normal.

Em contrapartida, os testes não paramétricos adotam uma metodologia mais simples, composta pelas seguintes etapas:

1. Contagem de minerações consecutivas na amostra original;
2. Permutação da amostra;
3. Nova contagem nas amostras permutadas;
4. Comparação do número de ocorrências em que a contagem da amostra original é maior que a das permutadas;
5. Cálculo do `p-value`.

Para realizar as análises propostas, são apresentados primeiro os resultados obtidos com os métodos atuais de detecção de ME. Na Tabela 2, estão listados os resultados da aplicação dos métodos propostos em [Silva and Sendin 2024] (coluna `p-value`) e [Li et al. 2020a] (coluna `ZScore`). Os dados da Blockchain foram obtidos da plataforma Blockchair, assim como a identificação dos mineradores, feita com base no campo `guessed miner` fornecido pela plataforma.

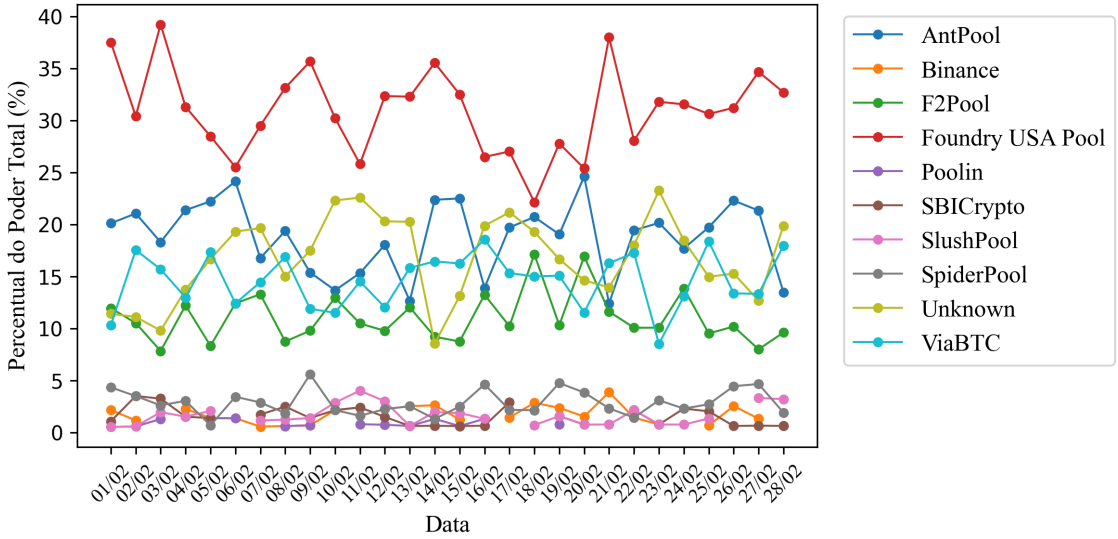

Figura 2. Gráfico do poder computacional real das pools baseado no registro da blockchain em fevereiro de 2025.

O poder computacional foi calculado com base na proporção de blocos minerados em relação ao total de blocos. Na Tabela 3, os valores de poder mínimo e máximo foram estimados considerando uma janela diária de mineração — aproximadamente 144 blocos . As colunas de média e desvio padrão referem-se ao número de minerações em sequência, calculado a partir de 20.000 permutações aleatórias dos dados. As colunas `p-value` e `ZScore` foram calculadas conforme descrito em [Silva and Sendin 2024] e [Li et al. 2020a], respectivamente, e servem como indicadores da ocorrência de ME.

Como critério de inclusão na tabela, considerou-se suficiente a indicação positiva por pelo menos um dos métodos utilizados. Contudo, é importante ressaltar que o poder computacional não está dentro dos intervalos mencionados anteriormente, uma vez que não foi identificado nenhum suspeito dentro desse parâmetro no período analisado. Assim, foram considerados válidos suspeitos com poder computacional superior a 10% e que atendessem a pelo menos um dos outros parâmetros mencionados. No período observado, foram identificados dois cenários suspeitos de prática de ME. Uma análise mais detalhada, considerando a variação do poder computacional, será apresentada a seguir.

Tabela 2. Análise da busca por ME para o ano de 2023 usando os métodos propostos, porém, nos dados do ano de 2024 não foram encontrados suspeitos que atendensem os critérios utilizados [Silva and Sendin 2024] e [Li et al. 2020a]

Mês	Minerador	Blocos minerados	Poder (%)	Blocos minerados em sequência	p-value	Z Score
3	Binance	485	10.37	62	0.041	1.85
7	ViaBTC	492	11.08	66	0.045	1.79

4.2. Análise com Poder Computacional Variável

A motivação racional para a análise que será apresentada a seguir considera os seguintes fatos:

- A análise de mineração em sequência é sensível à variação do poder computacional;
- A análise do poder médio - que é o que ocorre nos métodos atuais - pode facilmente gerar falsos positivos.

Na Figura 3, é mostrado um caso hipotético em que um minerador com 30% de poder computacional estável deve produzir quase 400 minerações em sequência no período de um mês. Na mesma figura, a curva azul mostra que um minerador com a mesma média de poder, mas com variação ao longo do período analisado, tende a produzir muito mais minerações em sequência — indicando que os métodos atualmente disponíveis na literatura não são compatíveis com o cenário real da mineração.

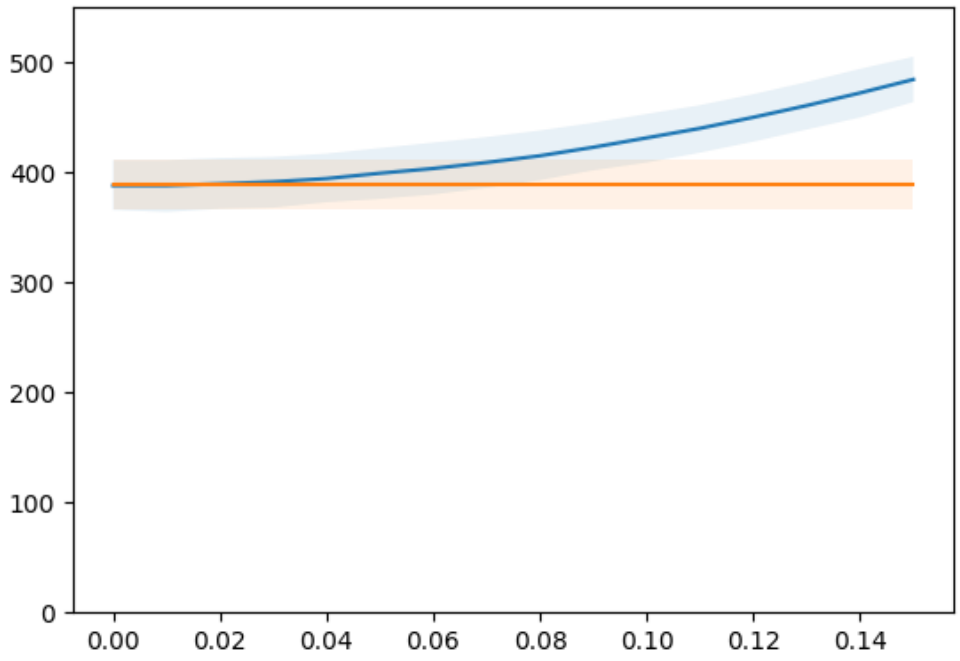

Figura 3. Minerações Consecutivas no período 1296 blocos, equivalente a um mês. Em laranja, a mineração obtida com um poder computacinal correspondente a 0.30 do poder computacional total, constante durante o período. Em azul, o a quantidade de minerações consecutivas com a variação do poder computacional - indicado no eixo x. A regiao sombreada indica o intervalo de 95% para os dois casos

Nas Figuras 4 e 5, são mostradas a variação do poder computacional nos dois eventos suspeitos de ME. Nelas, podemos observar aspectos interessantes, como os valores mínimo e máximo do poder computacional no período e o desvio padrão, o resumo dessas informações é mostrado na Tabela 3. Ao analisar esses dados, com o auxílio do gráfico do poder computacional diário, é evidente que o poder computacional de cada minerador é volátil, não segue um padrão cíclico e está longe de ser estável.

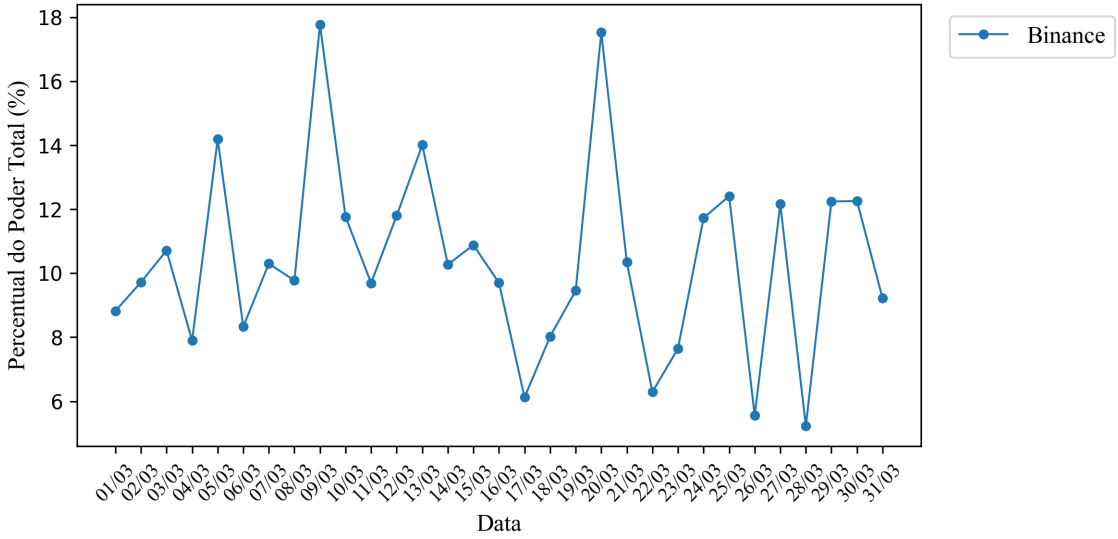

Figura 4. Gráfico da variação do poder computacionao da pool Binance no mês 3 de 2023.

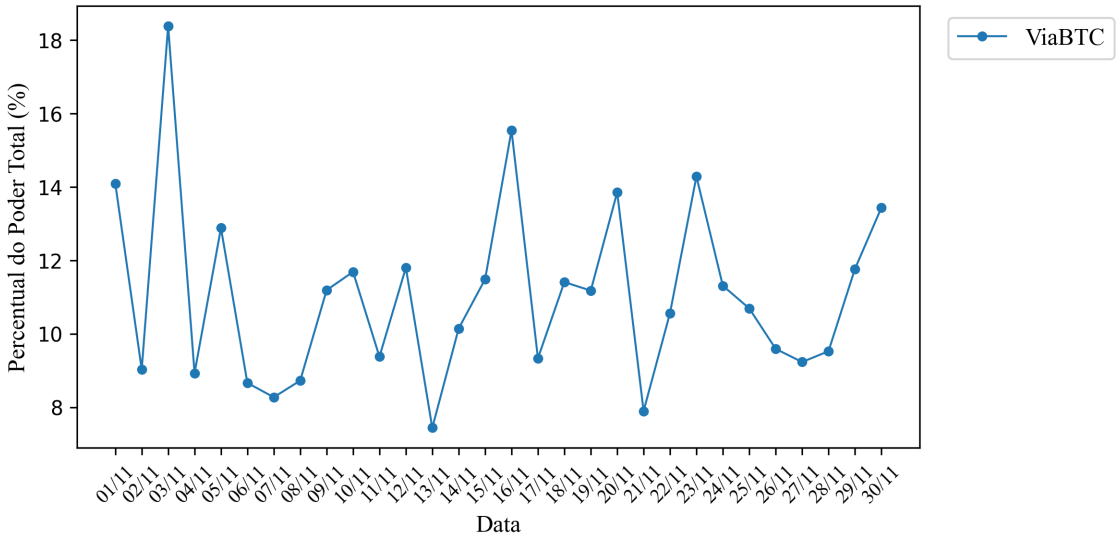

Figura 5. Gráfico da variação do poder computacionao da pool ViaBTC no mês 11 de 2023.

Tabela 3. estatísticas dos gráficos de mineradores suspeitos,

Minerador	Mínimo	Máximo	Desvio padrão
Binance	5.22	17.77	6.38
ViaBTC	7.4	18.38	6.58

Considerando os fatos apresentados, propomos uma adaptação do método descrito em [Silva and Sendin 2024] para lidar com poder computacional variável. O período de um mês é dividido em partes iguais, nas quais o poder computacional tende a ser mais

estável. As permutações características do método são realizadas em cada parte, e os resultados são agregados para calcular o `p-value`. O Algoritmo 1 descreve uma versão simplificada desse procedimento.

Algorithm 1 Análise de Selfish Mining por partes

```
Dividir o período total em n partes de mesmo tamanho
for cada pedaço do
    for cada minerador presente no pedaço do
        Filtrar os blocos minerados por este minerador na parte atual
        Calcular o número de blocos minerados
        Estimar o poder computacional do minerador na parte
        for cada uma das N permutações do vetor de blocos do
            Calcular a quantidade de blocos esperada via sorteio aleatório
        end for
        Calcular o p-value como a proporção de permutações com blocos ≥ observados
        Armazenar os resultados
    end for
end for
Calcular a média dos p-valores por minerador ao longo das partes
Identificar comportamentos suspeitos (p-valor médio baixo)
```

Na Tabela 4 é mostrado que, após a execução do algoritmo, com diferentes particionamentos dos períodos, observou-se que o `p-value` aumenta à medida que o número de partes cresce. Isso demonstra que o cálculo do `p-value` é sensível à variação de poder computacional.

Tabela 4. Análise do período separado em partes

Qtd. partes	Minerador	p-value original	p-value partes
2	Binance	0.041	0.849
2	ViaBTC	0.048	0.658
4	Binance	0.041	0.860
4	ViaBTC	0.048	0.673

5. Discussão

Os métodos atuais de detecção de ME baseados na análise da blockchain partem de uma premissa forte: que a produção de blocos pelos mineradores se mantém estável durante o período analisado. Só com essa estabilidade os modelos estatísticos podem ser aplicados e a prática de ME identificada.

No entanto, a observação da blockchain mostra que a produção de blocos pelos mineradores varia bastante — e isso precisa ser levado em conta nas análises. O poder real dos mineradores é difícil de estimar. Os dados fornecidos pelas plataformas não correspondem aos observados na blockchain, o que levanta hipóteses como: possível

maquiagem dos dados; impacto da complexidade da rede P2P, tornando a produção de blocos menos dependente do poder computacional do que se assume na literatura; ou ainda, que o poder computacional dos mineradores é, de fato, variável.

A execução da ME também deixaria evidências durante o processo de mineração. Como os mineradores atuam organizados em *pools*, a troca do objetivo de trabalho — por exemplo, a mineração do bloco n+1 — poderia ser observada pelos participantes. Além disso, é possível imaginar um cenário em que parte do *pool* colabore secretamente com a prática. Embora esse tipo de ataque seja viável, sua detecção exigiria novas ferramentas, já que a busca pelo bloco egoísta poderia ocorrer com um poder computacional reduzido.

6. Conclusões

Neste trabalho, investigamos o estado da arte na detecção de estratégias de *selfish mining* (ME), com foco na avaliação da eficácia dos métodos baseados exclusivamente na análise de dados da blockchain. Para isso, testamos a robustez dessas abordagens em cenários mais realistas, nos quais o poder computacional dos mineradores varia ao longo do tempo.

Os resultados obtidos indicam a ausência de evidências consistentes que possam ser atribuídas de forma confiável à prática de ME. Observou-se que a produção instável de blocos pelos mineradores compromete os pressupostos fundamentais dos métodos existentes, que geralmente assumem um ambiente com distribuição de poder computacional estável. Tal limitação sugere que, na prática, esses métodos podem ser inviáveis para detectar ME em ambientes reais.

Diante desse cenário, concluímos que a detecção de *selfish mining* a partir de dados públicos da blockchain ainda carece de abordagens metodologicamente sólidas e confiáveis. Propomos que investigações futuras considerem a utilização de fontes complementares de informação, como participação ativa de investigadores em *pools* de mineração. Essa estratégia permitiria o acesso a dados operacionais internos que poderiam viabilizar análises mais precisas e fundamentadas sobre a ocorrência de ME.

Referências

Eyal, I. and Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8437:436–454.

Li, S. N., Campajola, C., and Tessone, C. J. (2024). Statistical detection of selfish mining in proof-of-work blockchain systems. *Scientific Reports*, 14.

Li, S.-N., Yang, Z., and Tessone, C. J. (2020a). Mining blocks in a row: A statistical study of fairness in bitcoin mining. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–4.

Li, S.-N., Yang, Z., and Tessone, C. J. (2020b). Proof-of-work cryptocurrency mining: a statistical approach to fairness. In *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 156–161.

Messias, J., Alzayat, M., Chandrasekaran, B., Gummadi, K. P., Loiseau, P., and Mislove, A. (2021). Selfish & opaque transaction ordering in the bitcoin blockchain: The case for chain neutrality. In *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pages 320–335. Association for Computing Machinery.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system.

Recabarren, R. and Carbunar, B. (2017). Hardening stratum, the bitcoin pool mining protocol. pages 1–18.

Sannicolo, S. J. A. D. S. C. G. V. C. S. A. B. F. (2023). Stratum v2: the next generation protocol for bitcoin pooled mining. Technical report.

Schwarz-Schilling, C., Li, S.-N., and Tessone, C. J. (2022). Stochastic modelling of selfish mining in proof-of-work protocols. *Journal of Cybersecurity and Privacy*, 2:292–310.

Silva, E. and Sendin, I. (2024). A non-parametric approach to identifying anomalies in bitcoin mining. In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 315–320, Porto Alegre, RS, Brasil. SBC.