Simulação do Ataque 51% em Blockchains

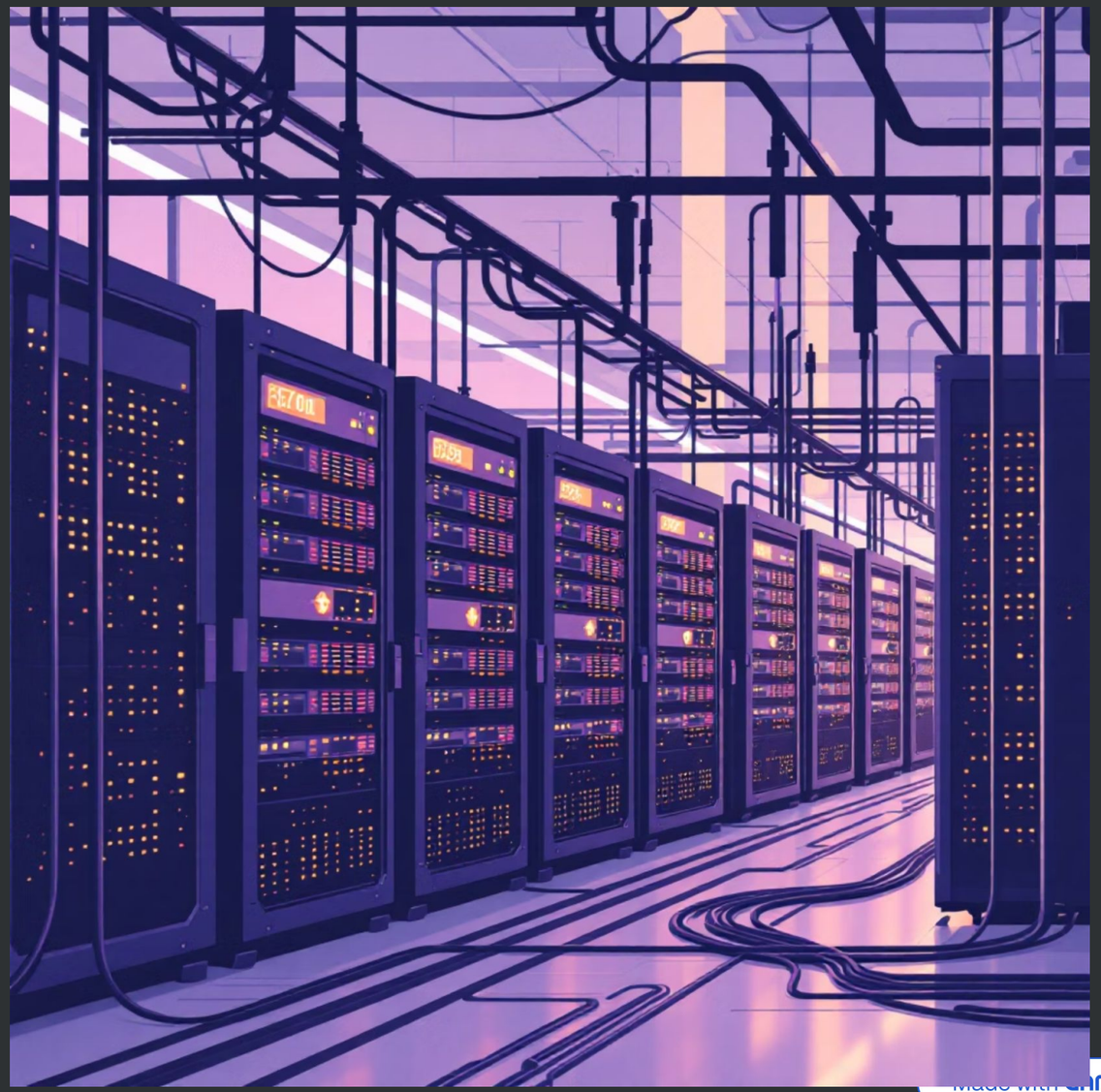
Uma análise prática da vulnerabilidade do consenso descentralizado através de simulação probabilística em Python

Bruno Kazuya Yamato Sakaji, nº14562466

Por que estudar o Ataque 51%?

O Problema

A segurança de blockchains como Bitcoin depende fundamentalmente da **honestidade da maioria** dos mineradores. Mas o que acontece quando um agente malicioso controla mais da metade do poder computacional da rede? Este projeto explora essa vulnerabilidade crítica através de uma **simulação off-chain** que torna o conceito tangível e mensurável.



Objetivos do Projeto

Demonstrar Visualmente

Ilustrar de forma intuitiva como um atacante com poder majoritário pode reorganizar a cadeia de blocos e invalidar transações confirmadas

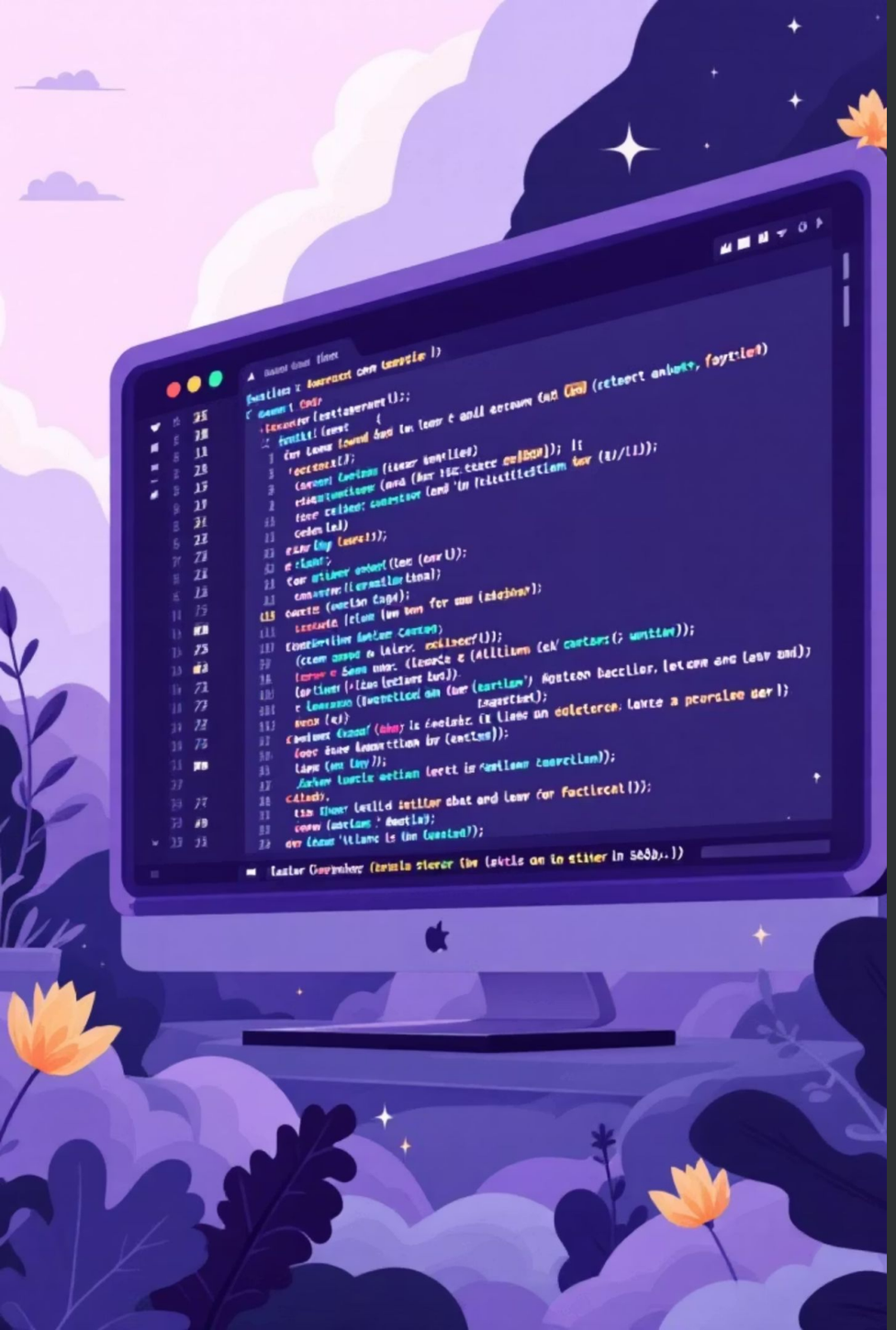
Quantificar o Risco

Calcular probabilisticamente as chances de sucesso do ataque em função do poder de mineração e número de confirmações

Abordagem Didática

Criar uma simulação leve e reproduzível em Python, ideal para fins educacionais sem necessidade de infraestrutura complexa

Escolha metodológica: A simulação probabilística permite experimentação controlada e análise estatística robusta do comportamento do ataque



Arquitetura da Simulação

01

Estrutura Modular

Bibliotecas: random, numpy e matplotlib para simulação e visualização

02

Modo Sample

Execução passo a passo mostrando evolução das cadeias pública e privada

03

Modo Batch

Milhares de simulações para cálculo estatístico da probabilidade de sucesso

Mecânica do Ataque: Competição Bloco a Bloco

Como Funciona

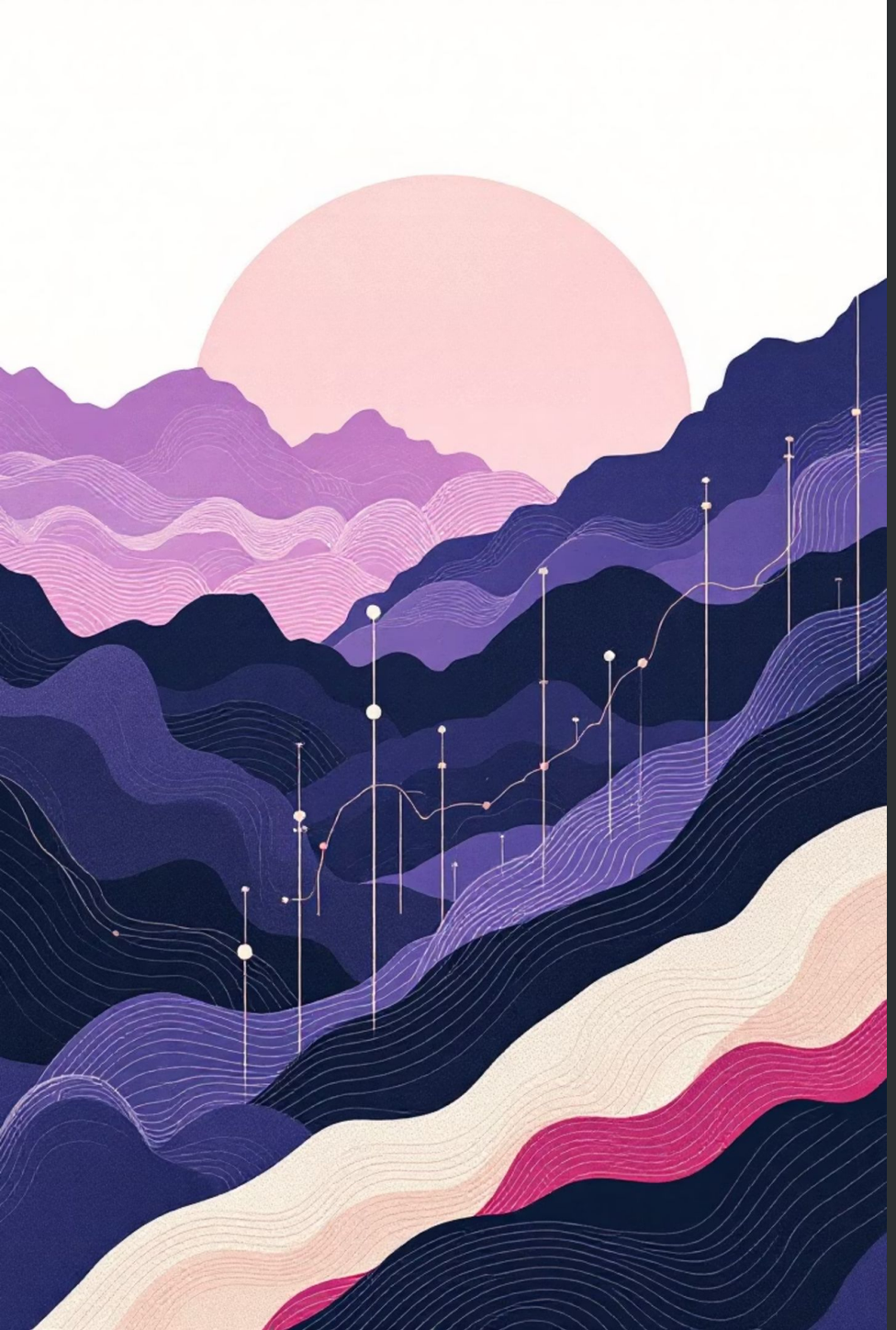
A cada rodada de mineração:

Com probabilidade **p**, o atacante minera um bloco

Com probabilidade **1-p**, os mineradores honestos mineram

O atacante mantém sua cadeia em segredo

Quando a cadeia privada supera a pública, ocorre o **reorg**



Visualização: Evolução das Cadeias

Linha Azul — Cadeia Pública

Representa os blocos minerados pelos participantes honestos da rede, visíveis para todos

Linha Laranja — Cadeia Privada

Mostra os blocos secretos do atacante, acumulados estrategicamente para superar a cadeia pública

Marcadores de Reorg

Linhas verticais indicam o momento crítico: quando o atacante revela sua cadeia e substitui a história oficial

```
python src/simulate_attack51.py --mode sample --p 0.55 --steps 400 --seed 42
```

Análise Estatística: Probabilidade de Sucesso

51%

Poder de Mineração

Limiar crítico para viabilizar o ataque

6

Confirmações

Blocos aguardados para aumentar segurança

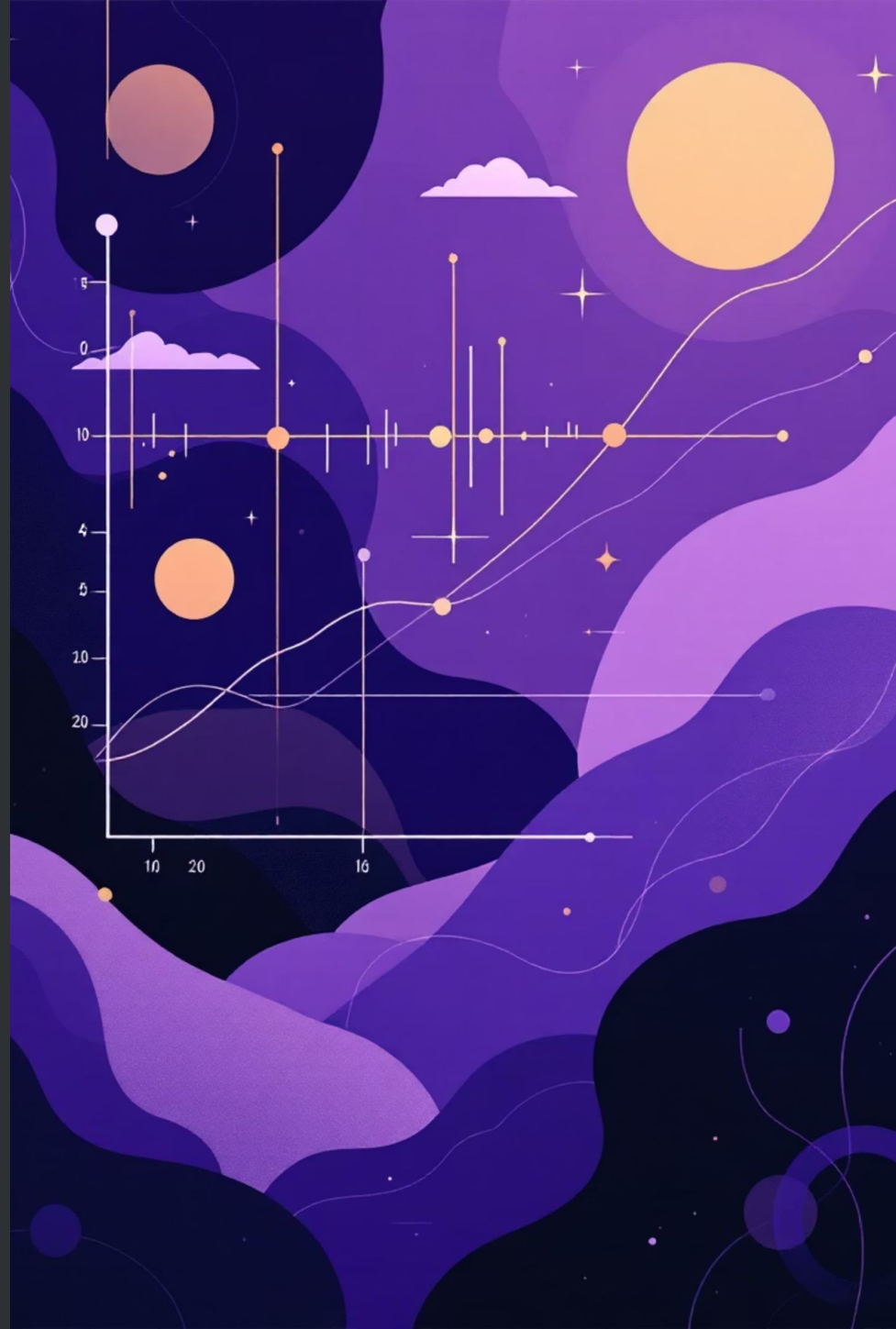
5000

Simulações

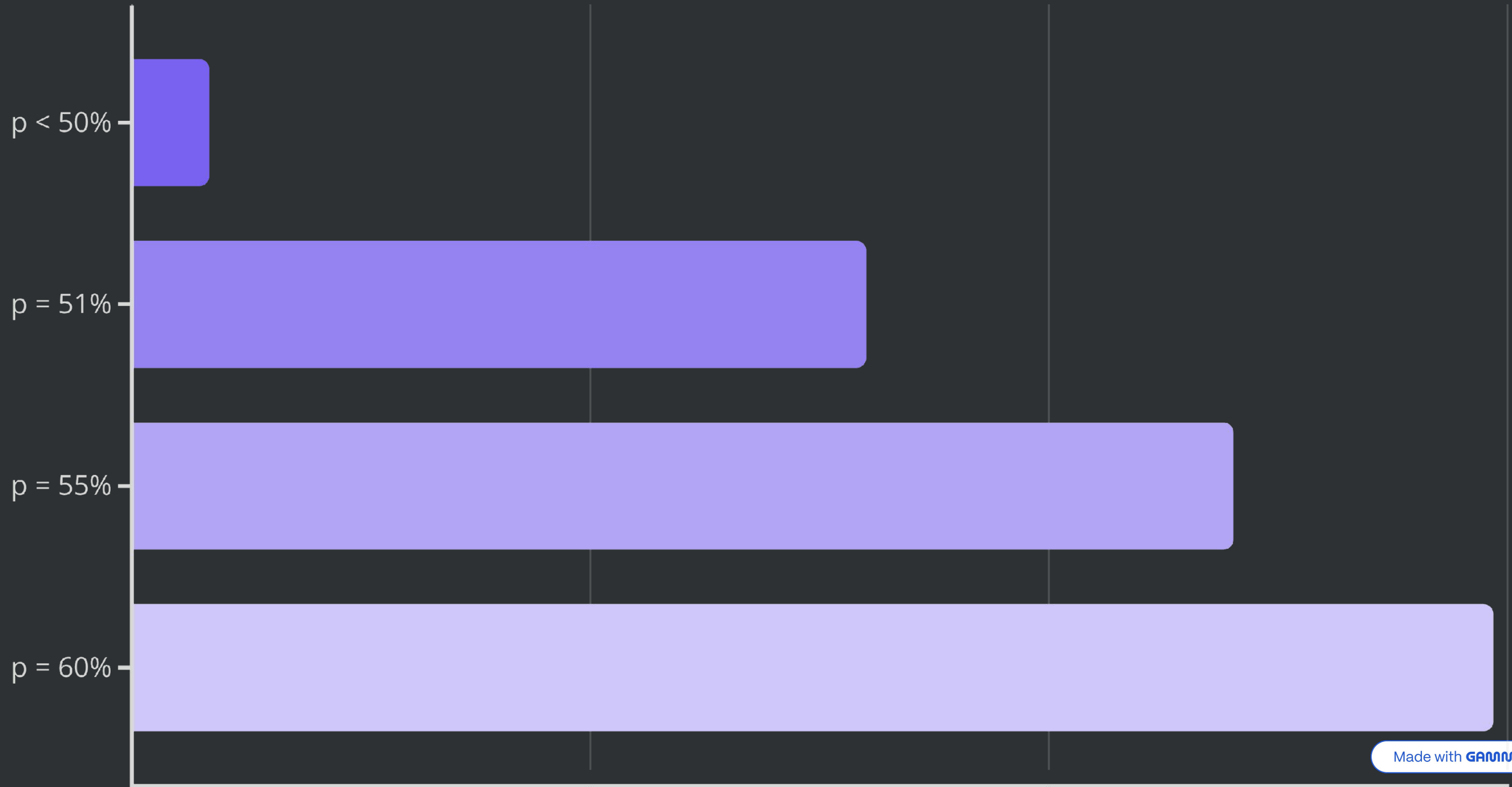
Rodadas para estimativa confiável

O modo batch executa milhares de tentativas independentes, calculando a taxa de sucesso do atacante para diferentes valores de **p** (poder de hash) e **k** (número de confirmações).

python src/simulate_attack51.py --mode batch --p 0.51 --k 6 --trials 5000



Resultados Principais



Limitações e Contexto Prático

O que o modelo simplifica

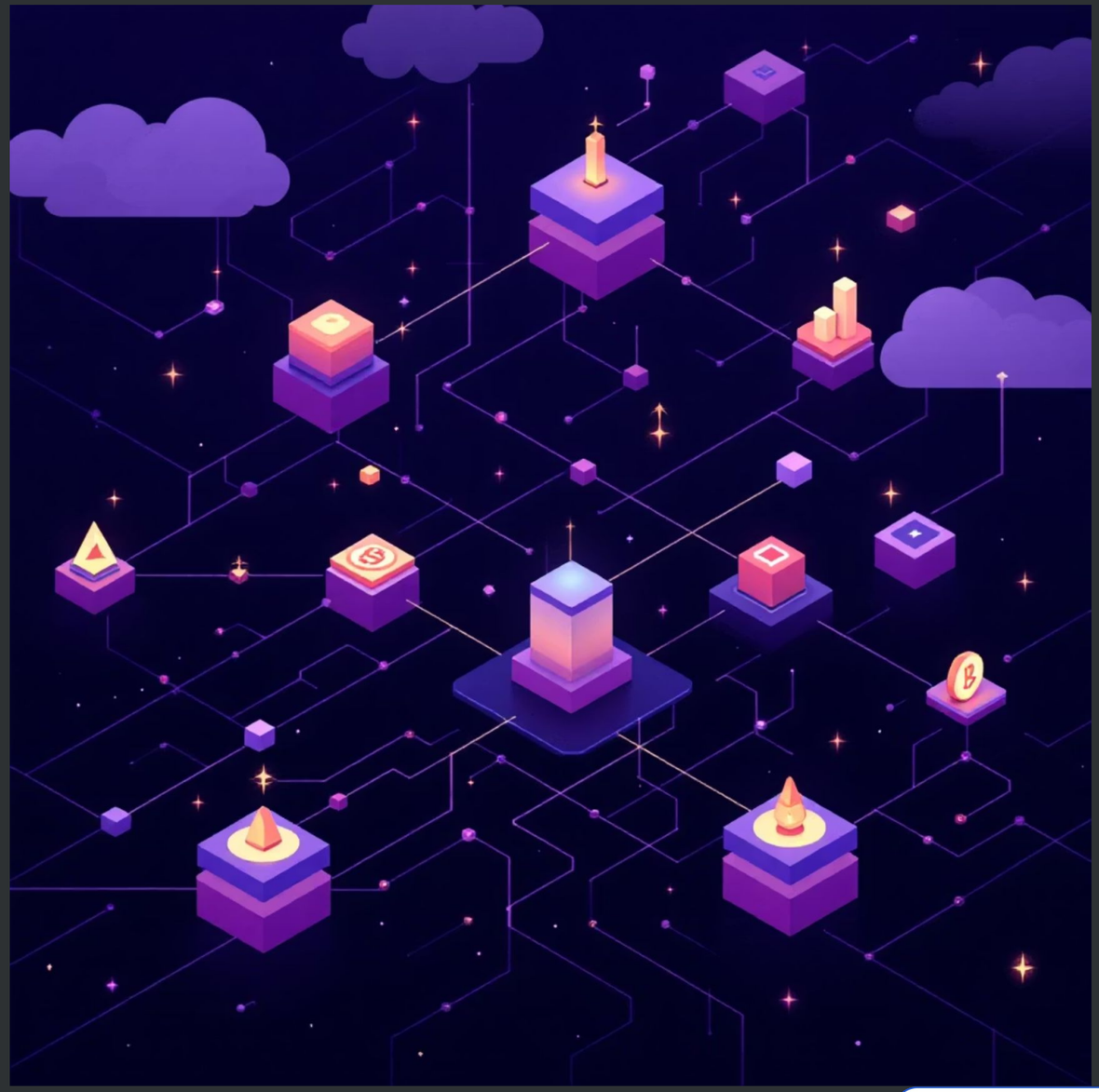
Latência de rede: blocos se propagam instantaneamente na simulação

Incentivos econômicos: não considera custos de mineração ou taxas de transação

Pools de mineração: assume um único atacante monolítico

Estratégias avançadas: não implementa selfish mining ou outras táticas

Apesar dessas simplificações, o modelo captura a essência do problema: a vulnerabilidade criada pelo controle majoritário do consenso.



Aplicação Didática

Conclusões e Aprendizados

Visualização Clara

A simulação torna tangível um conceito teórico complexo

Quantificação Precisa

Demonstramos matematicamente o impacto do poder de mineração

Implicações de Segurança

Confirmamos que a descentralização é fundamental para a confiança

> "A segurança de uma blockchain depende fundamentalmente da distribuição do poder computacional. Este projeto demonstra, de forma prática e acessível, por que a honestidade da maioria não é apenas desejável — é **essencial**."

Referências: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System • Rosenfeld, M. (2014). Analysis of Hashrate-Based Double Spending

Link do vídeo

https://youtu.be/x0Jwx-ioepc

Link do github

https://github.com/BrunoKazuya/Blockchain-e-criptomoedas---ataque-51-.git

Autoavaliação: 10/10

Por acreditar ser um tema válido e descrito de forma correto ao longo da apresentação e com o que o trabalho se propõe a avaliar, considero que 10/10 é uma nota válida