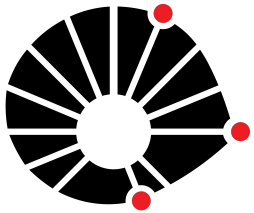
Evaluating the network traffic on an improved version of the Committeeless Proof-of-Stake blockchain consensus algorithm



George Gigilas Junior, Filipe F. Ferreira, Marco A. A. Henriques

Universidade Estadual de Campinas - Unicamp

Motivação

- Blockchain: gerenciamento de dados distribuído
- Nós convergem para uma mesma visão
  - Consenso para adicionar próximo bloco
- Mecanismos de consenso:
  - Proof-of-Work (PoW): alto consumo de energia
  - Proof-of-Stake (PoS): mais detalhes em breve
  - Committeeless PoS (CPoS): alternativa promissora!

Proof-of-Stake (PoS)

- Consiste em sorteios a cada rodada
  - Como em uma loteria
  - Poder computacional não dá vantagem
  - Consumo de energia desprezível comparado com PoW
- Exige comitê para validar sorteios e bloco criado
  - Gestão do comitê é complexa

Committeeless Proof-of-Stake (CPoS)

- Não possui comitê
  - Nós confirmam sorteio localmente
- Blocos confirmados após algumas rodadas
- τ : número médio de blocos sorteados por rodada
  - Apenas um bloco é agregado à blockchain por rodada
  - $\tau \cong 1$: podem ocorrer rodadas sem blocos
  - $\tau > 1$: aumenta tráfego; maior robustez contra ataques

Problema

- CPoS ainda é jovem e pouco testado
- Trabalhos anteriores focaram no consenso
  - Blocos mais leves, sem transações
- Escolha dos parâmetros pode congestionar a rede
  - Dificulta obtenção do consenso

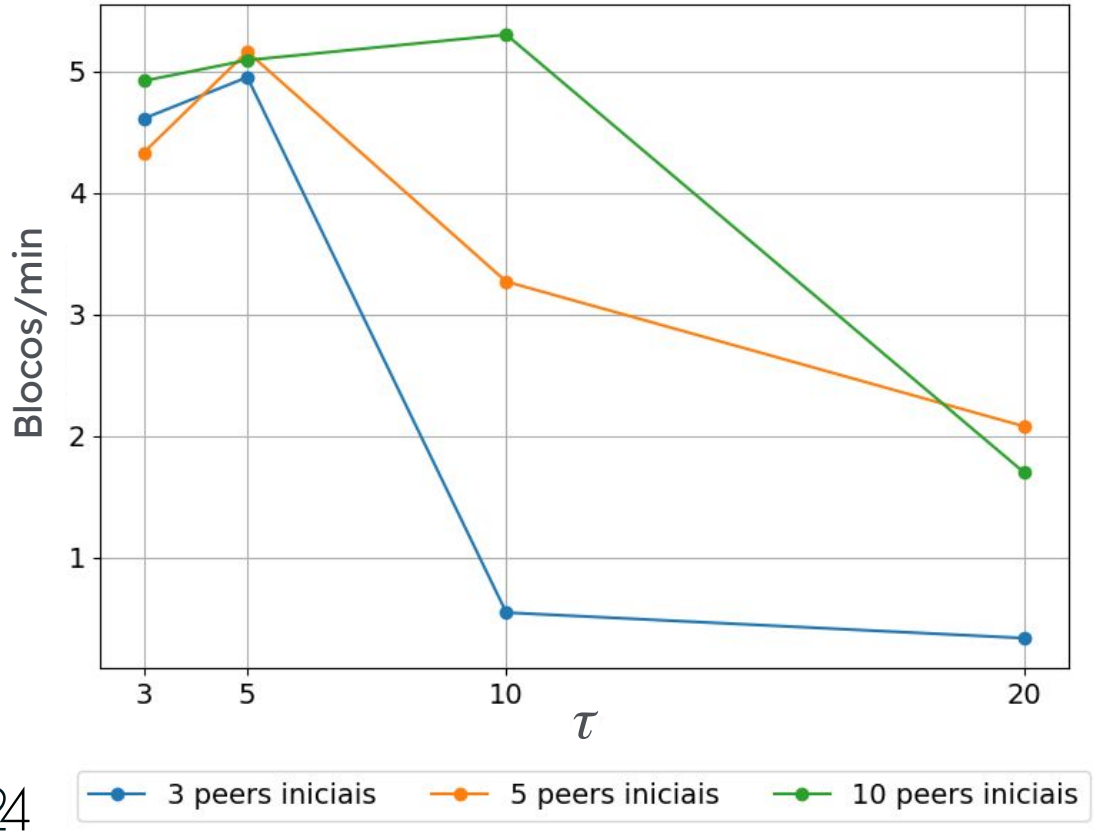
Objetivo

- Completar os blocos com transações
  - Torna a simulação mais próxima de um caso real
- Reduzir o número de mensagens na rede
  - Controle do número de pares por nó
- Avaliar impactos das mudanças implementadas

Modificações Aplicadas

- Adição de transações aleatórias nos blocos
  - Tamanho médio do bloco: 200 kB
- Restrição do número de peers por nó
  - Valor inicial configurável
  - Valores máximo e mínimo (ajuste automático)
  - Menos mensagens na rede

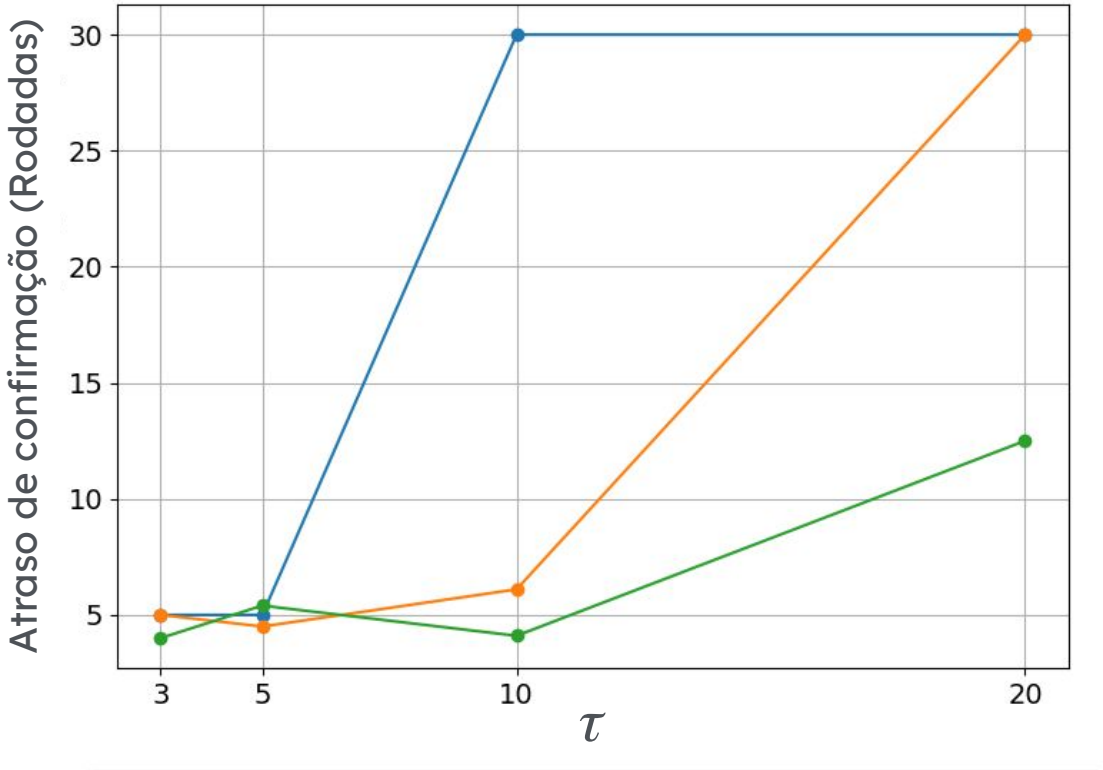
Blocos/min vs τ



Configuração:

- 30 rodadas de 10s de duração
- 25 nós
- Bloco de 200 kB

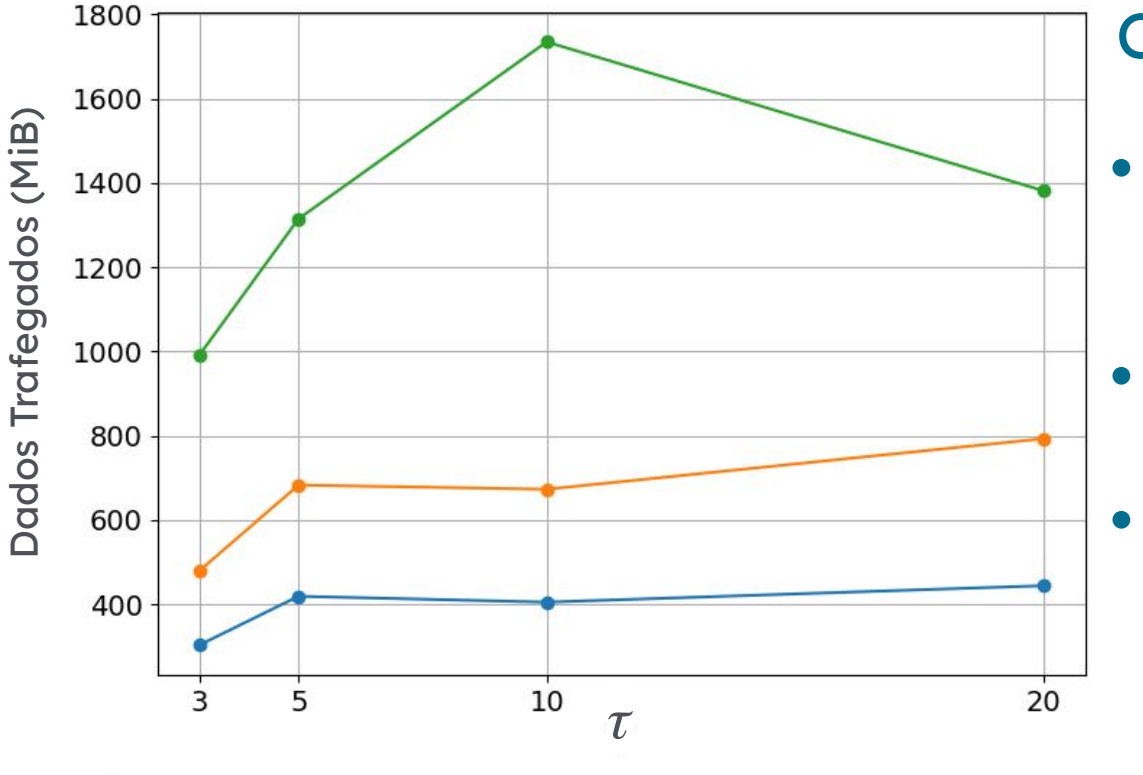
Atraso de Confirmação vs τ



Configuração:

- 30 rodadas de 10s de duração
- 25 nós
- Bloco de 200 kB

Dados Trafegados vs τ



Configuração:

- 30 rodadas de 10s de duração
- 25 nós
- Bloco de 200 kB

Conclusões

- CPoS se mostra promissor
  - Mais avaliações são necessárias
- Atual versão permite avaliações mais realistas
- Diminuição do número de pares reduz tráfego

Trabalhos futuros

- Buscar novas formas de reduzir o tráfego na rede
  - Exemplo: transmitir apenas transações do bloco vencedor da rodada
- Experimentos com mais nós e mais espalhados
- Testes com nós desonestos

Obrigado!

- George Gigilas Jr., Filipe F. Ferreira, Marco A. A. Henriques
- Contato: g216741@dac.unicamp.br

UNICAMP

ReGrAS
SECURITY RULES.
UNICAMP

SLIDES EXTRAS

Mecanismo alternativo de divulgação

- Inicialmente, apenas o cabeçalho do bloco é divulgado
- Após consenso, divulga conteúdo completo
  - Autor do bloco faz a divulgação
- Se mostrou efetivo em reduzir o volume de dados

Avaliação - 3 peers iniciais

Tau	Round Time	Blocks/min	Confirmation delay (rounds)	# of messages	Data sent (MiB)
3	5s	8.66	5.3	3,469	265
3	10s	4.61	5.0	3,872	303
3	15s	2.72	4.5	3,886	306
5	5s	7.12	5.3	5,018	371
5	10s	4.95	5.0	5,304	419
5	15s	2.79	5.9	5,112	395
10	5s	4.60	6.6	6,055	401
10	10s	0.55	> 30	6,482	405
10	15s	0.64	> 30	6,119	370
20	5s	0.81	> 30	7,400	454
20	10s	0.34	> 30	7,079	444
20	15s	0.31	> 30	7,168	443

30 rodadas, 25 nós

Avaliação - 5 peers iniciais

Tau	Round Time	Blocks/min	Confirmation delay (rounds)	# of messages	Data sent (MiB)
3	5s	9.37	4.1	6,001	467
3	10s	4.33	5.0	6,154	479
3	15s	3.31	4.1	7,158	569
5	5s	9.82	4.6	8,180	631
5	10s	5.16	4.5	8,577	683
5	15s	3.52	4.5	8,825	707
10	5s	6.79	6.3	9,408	678
10	10s	3.27	6.1	9,507	673
10	15s	1.83	9.6	9,758	707
20	5s	4.48	6.9	10,793	735
20	10s	2.08	> 30	11,528	793
20	15s	0.68	> 30	11,681	772

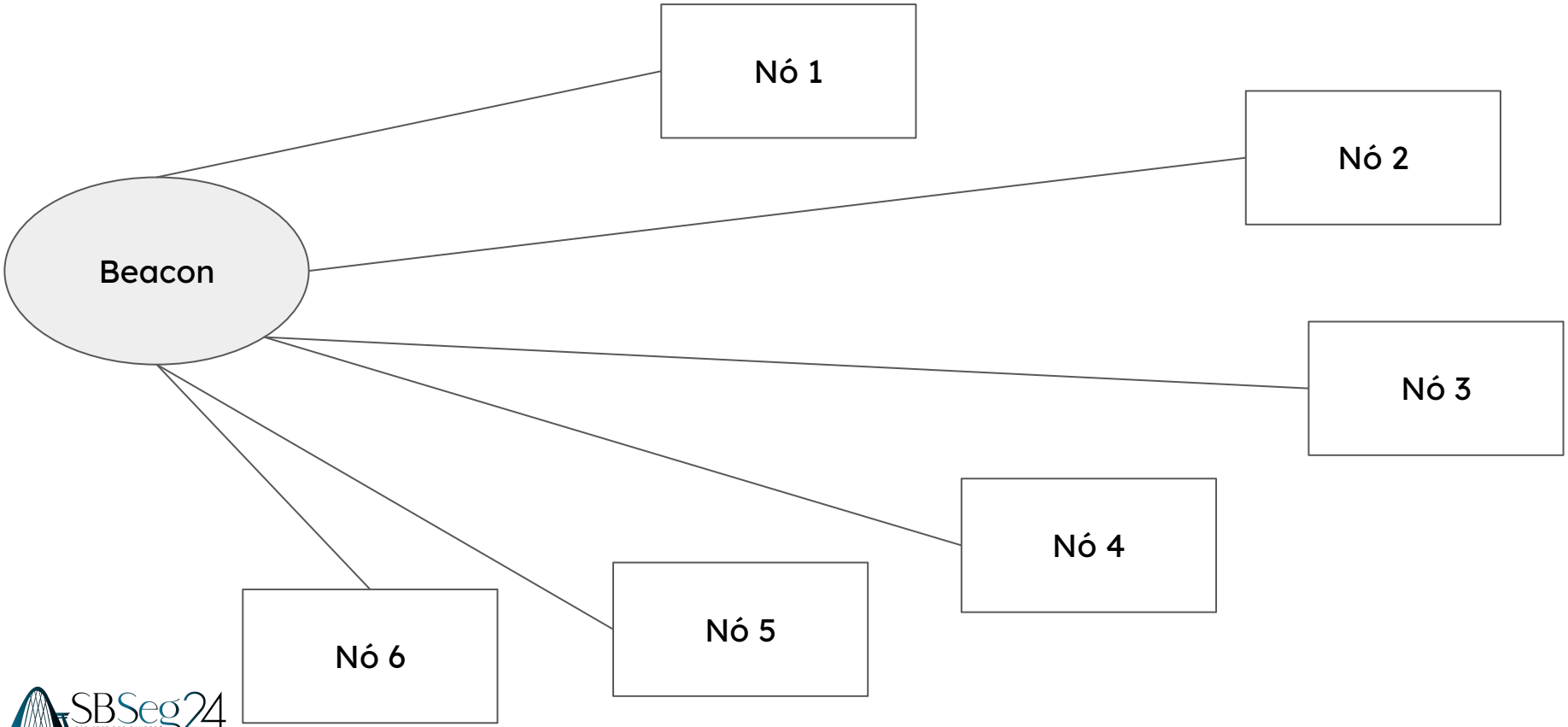
30 rodadas, 25 nós

Avaliação - 10 peers iniciais

Tau	Round Time	Blocks/min	Confirmation delay (rounds)	# of messages	Data sent (MiB)
3	5s	9.73	4.9	12,487	976
3	10s	4.92	4.0	12,575	991
3	15s	3.48	3.8	12,714	1,000
5	5s	9.76	4.3	14,921	1,160
5	10s	5.09	5.4	16,561	1,315
5	15s	3.52	4.6	16,785	1,339
10	5s	9.51	4.5	19,831	1,556
10	10s	5.30	4.1	21,703	1,735
10	15s	3.61	4.1	22,290	1,780
20	5s	3.46	5.8	17,014	1,185
20	10s	1.70	12.5	18,787	1,382
20	15s	1.11	8.7	18,586	1,350

30 rodadas, 25 nós

Topologia da Rede



Topologia da Rede