# Análise de desempenho e otimização de protocolos de comunicação no mecanismo de consenso CPoS

**Inácio Defilippi Gonçalves** *i288637@dac.unicamp.com.br*
**Marco Amaral Henriques** *maah@unicamp.br*

Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (UNICAMP)

**Resumo**

*A tecnologia blockchain tem potencial para descentralizar a confiança digital, mas sua adoção em massa enfrenta desafios de infraestrutura. As soluções atuais frequentemente exigem um compromisso entre segurança, descentralização e eficiência energética. O mecanismo de consenso Committeeless Proof-of-Stake (CPoS) propõe uma alternativa sustentável baseada em sorteios probabilísticos locais. Este trabalho busca avaliar o CPoS em um ambiente distribuído realista, simulando as condições adversas da internet. Sabe-se que, embora seguro, o protocolo sofre com congestionamento de rede devido à redundância na propagação de dados. Como solução, propomos a adoção de uma estratégia de comunicação em duas etapas, de maneira a possibilitar uma redução no volume de tráfego gerado pelo mecanismo.*

**Palavras-Chave** — *blockchain*, consenso distribuído, CPoS, *Proof-of-Stake*, otimização.

## 1. Introdução

Uma *blockchain* funciona, essencialmente, como um livro-razão digital compartilhado. Ao contrário de um banco tradicional, onde um servidor central controla o saldo de todos, na *blockchain* essa informação é copiada em milhares de computadores ao redor do mundo. Para garantir que todos concordem sobre quais transações são verdadeiras e evitar fraudes, a rede utiliza um mecanismo de regras chamado consenso [1].

O grande desafio da engenharia de *blockchains* hoje é equilibrar três pilares fundamentais: segurança, descentralização e desempenho. Os mecanismos dominantes costumam falhar em atender pelo menos um desses requisitos de forma plena.

- **Proof-of-Work (PoW):** utilizado pela criptomoeda Bitcoin [2]. É extremamente robusto e descentralizado, pois exige trabalho computacional para validar transações. No entanto, esse processo demanda uma quantidade de energia proibitiva, comparável ao consumo de países inteiros, o que o torna ambientalmente insustentável a longo prazo.

- **Proof-of-Stake (PoS):** substitui a energia pelo capital (quem possui mais moedas tem maior chance de construir e publicar um novo bloco da cadeia) [3]. Embora eficiente energeticamente, muitas implementações práticas recorrem a comitês restritos de validadores para garantir velocidade, o que tende a centralizar o poder na mão de poucos participantes, aumentando a chance de serem atacados (corrompidos) para favorecer algum outro participante da rede.

### *1.1. O Mecanismo CPoS*

O protocolo analisado neste estudo, o CPoS [4], busca resolver essa equação. Ele busca eliminar a necessidade de o mecanismo de consenso PoS trabalhar com um comitê de validação, aumentando a descentralização e tornando o sistema mais seguro.

O sistema opera como uma loteria descentralizada. A cada rodada, cada computador na rede executa um sorteio interno, gerando um número aleatório criptografado. A regra básica do consenso CPoS se apoia no controle do número médio de sorteios que são bem sucedidos (número médio de nós de rede sorteados) e na comparação dos *hashes* dos blocos gerados por esses nós. Somente o bloco com o menor *hash* é aceito como vencedor para ser anexado à *blockhain* em construção [4].

O objetivo deste trabalho é analisar em detalhes o volume de tráfego gerado nesta propagação de blocos criados por nós sorteados e buscar formas de otimizar os protocolos de comunicação a fim de diminuir o tráfego na rede que pode ser alto, dependendo dos parâmetros de execução.

## 2. Metodologia

Para avaliar o desempenho dos protocolos, é desejável construir um ambiente que reproduza a complexidade da internet global, e o funcionamento de uma *blockchain* em um ambiente com muitos nós e muita atividade de produção de blocos.

### *2.1. Infraestrutura Virtualizada*

Dando sequência a trabalhos anteriores, estamos adotando a tecnologia *Docker Swarm* para instanciar uma rede composta por dezenas de nós independentes. Cada nó opera isolado em seu próprio contêiner, comportando-se como uma máquina distinta com banco de dados próprio.

Nesse contexto, fazemos uso de uma rede *overlay*. Esta tecnologia cria uma camada de abstração lógica sobre a infraestrutura física.

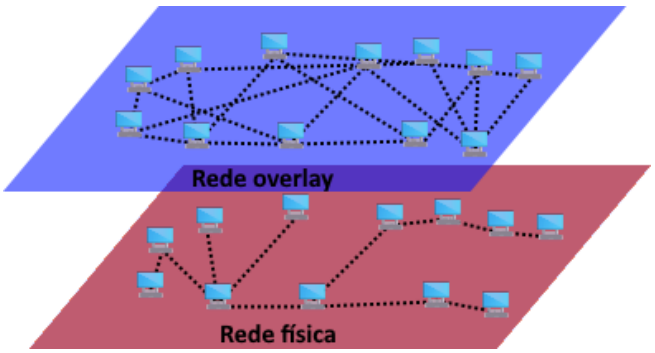


Figura 1: Esquema da rede *overlay* (azul): ela permite configurar conexões lógicas complexas entre os nós virtuais independentemente de onde os contêineres estão fisicamente hospedados (vermelho).

A *overlay* permite definir conexões aleatórias entre os participantes, construindo uma topologia desorganizada (*Peer-to-Peer*) similar à da internet pública. Isso cria um cenário onde os dados precisam saltar por vários nós para chegar ao destino, introduzindo atrasos e desafios reais de propagação.

## 3. Soluções propostas e resultados esperados

Serão realizados testes de estresse para tentar revelar quais são os principais gargalos do CPoS em relação ao tráfego de blocos que são gerados.

### *3.1. O Custo da Redundância*

Como o sorteio é probabilístico e executado localmente, é comum que, em uma mesma rodada, múltiplos nós sejam sorteados e se considerem vencedores simultaneamente [4].

Na implementação atual, todos esses potenciais vencedores tentam propagar seus blocos completos (arquivos pesados contendo milhares de transações) para toda a rede ao mesmo tempo.

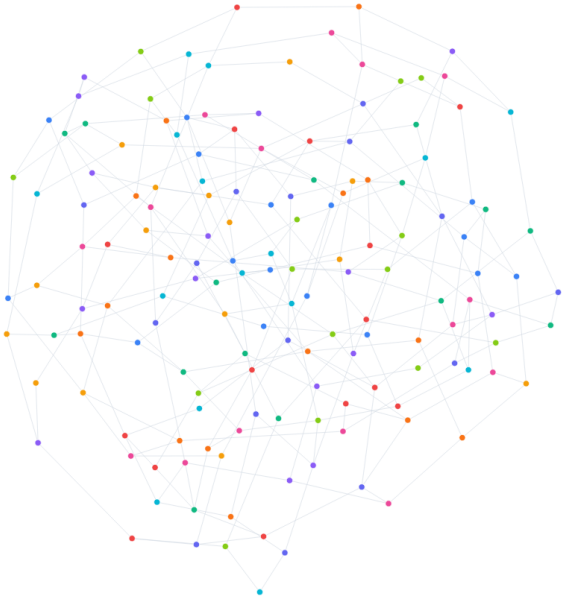

Figura 2: Visualização da topologia experimental: a alta densidade de conexões ilustra o risco de saturação de banda quando múltiplos nós tentam difundir grandes volumes de dados simultaneamente.

Isso gera uma saturação da largura de banda. A rede fica congestionada com dados redundantes, pois apenas o bloco daquele que tiver o o menor valor de *hash* será efetivamente confirmado. Esse comportamento desperdiça recursos e limita severamente a capacidade da rede de crescer, pois a quantidade de dados propagados cresce exponencialmente com o número de nós.

### *3.2. Proposta: comunicação por etapas*

A principal otimização para este problema, sugerida como trabalho futuro na dissertação de Martins [4], é dividir o protocolo de comunicação em duas fases distintas:

1. **Propagação de provas (cabeçalho):** o nó envia inicialmente apenas o cabeçalho do bloco. Este é um pacote minúsculo que contém a prova do sorteio (o "número sorteado") e outros metadados, mas exclui o corpo pesado das transações.
2. **Solicitação de bloco (corpo):** os demais nós da rede recebem esses cabeçalhos os comparam e identificam quem tem o menor valor. Somente então eles solicitam o envio do corpo pesado do bloco (as transações) para o nó considerado vencedor.

Essa abordagem tem o potencial de filtrar o tráfego na origem, liberando a capacidade da rede para processar um volume muito maior de tráfego gerado pelos nós da rede. No entanto, ela traz riscos à segurança da *blockchain*, já que nós maliciosos podem abusar dessa estratégia, não enviando o bloco na segunda etapa e gerando, assim, muita dificuldade para a continuação da produção de novos blocos..

## 4. Impactos da Pesquisa

A viabilização técnica desta otimização poderá trazer impactos diretos para a aplicabilidade da tecnologia:

- **Sustentabilidade:** reforça a viabilidade de manter uma rede segura através de sorteios matemáticos leves, mas sem depender de um comitê de validação que pode gerar vulnerabilidades de segurança.
- **Escalabilidade:** ao reduzir os requisitos de largura de banda, o sistema permite que mais nós participem da rede baseada em CPoS, dando à mesma melhores características de escalabilidade.

## 5. Conclusão

A transição do CPoS da teoria para a experimentação prática indica que sua escalabilidade pode ser limitada por uma comunicação excessiva e redundante de blocos gerados. A proposta da propagação de blocos em duas etapas deverá mitigar esse problema. Assim, o CPoS poderá se posicionar como uma alternativa viável para futuras aplicações descentralizadas que demandem segurança e sustentabilidade.

## Agradecimentos

Ao grupo de pesquisa ReGrAS pelo suporte na infraestrutura de testes.

## Referências

[1] I. Bashir, *Mastering Blockchain*, 1st ed. Packt Publishing Ltd., 2017.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” [Online]. https://bitcoin.org/bitcoin.pdf, 2009.

[3] S. King and S. Nadal, “PPCoin: Peer-to-peer crypto-currency with proof-of-stake,” [Online]. https://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.

[4] D. F. G. Martins, “Um novo mecanismo de consenso probabilístico para blockchains públicas; Dissertação de Mestrado,” [Online]. http://repositorio.unicamp.br/Busca/Download ?codigoArquivo=507683, 2021.