SBS: Soluções para Blockchains Seguras

Coordenador:
Marco Amaral Henriques

Research Group on Applied Security - ReGrAS

Contexto e Motivação

- Segurança de blockchains depende de vários fatores.
- Problemas focados neste trabalho:
  - vulnerabilidade das assinaturas digitais tradicionais (ECDSA) trazida pelo computador quântico;
  - principais mecanismos de consenso são:
    - ineficientes (Proof-of-Work) ou
    - exigem gerenciamento de complexos comitês de validação (Proof-of-Stake).

Objetivos do Projeto

- Aprimorar a segurança e eficiência das blockchains em duas frentes principais:
  - segurança criptográfica: implementar e avaliar o uso de criptografia pós-quântica em blockchains;
  - eficiência do mecanismo de consenso: aprimorar, implementar e avaliar um novo mecanismo de consenso PoS probabilístico, sem comitê de validação.

Segurança criptográfica

- Algoritmos de assinatura pós-quânticos são imprescindíveis para proteger transações e contratos inteligentes.
- Estratégias:
  - Implementação e avaliação de assinaturas pós-quânticas padronizadas pelo NIST ou ainda em estudos.
  - Uso de protocolos híbridos otimizados, combinando algoritmos tradicionais e pós-quânticos.
    - Algoritmos pós-quânticos são ainda jovens e podem ruir.

Desafios da Criptografia Pós-Quântica

- Desempenho: cálculo e verificação de assinaturas podem ser mais lentos que em métodos tradicionais, como ECDSA ou EdDSA.
- Armazenamento: assinaturas e chaves pós-quânticas são muito maiores, impactando o armazenamento e a comunicação na blockchain.
- Segurança: algoritmos pós-quânticos parecem ser seguros contra ataques quânticos, mas não foram suficientemente testados e analisados (não passaram no teste do tempo).
  - Necessário implementar protocolos híbridos: mais pesados!
  - Necessário otimizar implementações pós-quânticas e híbridas.

Eficiência de mecanismos de consenso

Mecanismos mais usados

- Proof-of-Work (PoW):
  - simples e seguro (Bitcoin usa desde 2009);
  - alto consumo de energia => centralização do poder computacional em poucos agentes pelo mundo.
- Proof-of-Stake (PoS):
  - baixíssimo consumo de energia (comparado ao PoW);
  - segurança complexa na gestão de comitês de validação.

Novo mecanismo CPoS

Committeeless Proof-of-Stake

- PoS probabilístico sem comitê de validação.
- Menor complexidade de gestão (auto-controlado).
- Evita centralização.
- Pode prover maior distribuição de recompensas e taxas.
- Evita ataques a comitês de validação (para corrompê-los).
- Desafios:
  - Potencial sobrecarga da rede.
  - Vulnerabilidade a ataques de conluio em larga escala.

Implementação e Avaliação

- Implementar, testar e avaliar:
  - novos algoritmos pós-quânticos: Hyperledger Besu
  - novo mecanismo de consenso: Hyperledger Besu
- Uso do testbed da RNP para testes com vários nós:
  - Avaliação dos custos computacionais e de comunicação com cripto pós-quântica.
  - Avaliação do novo mecanismo CPoS.

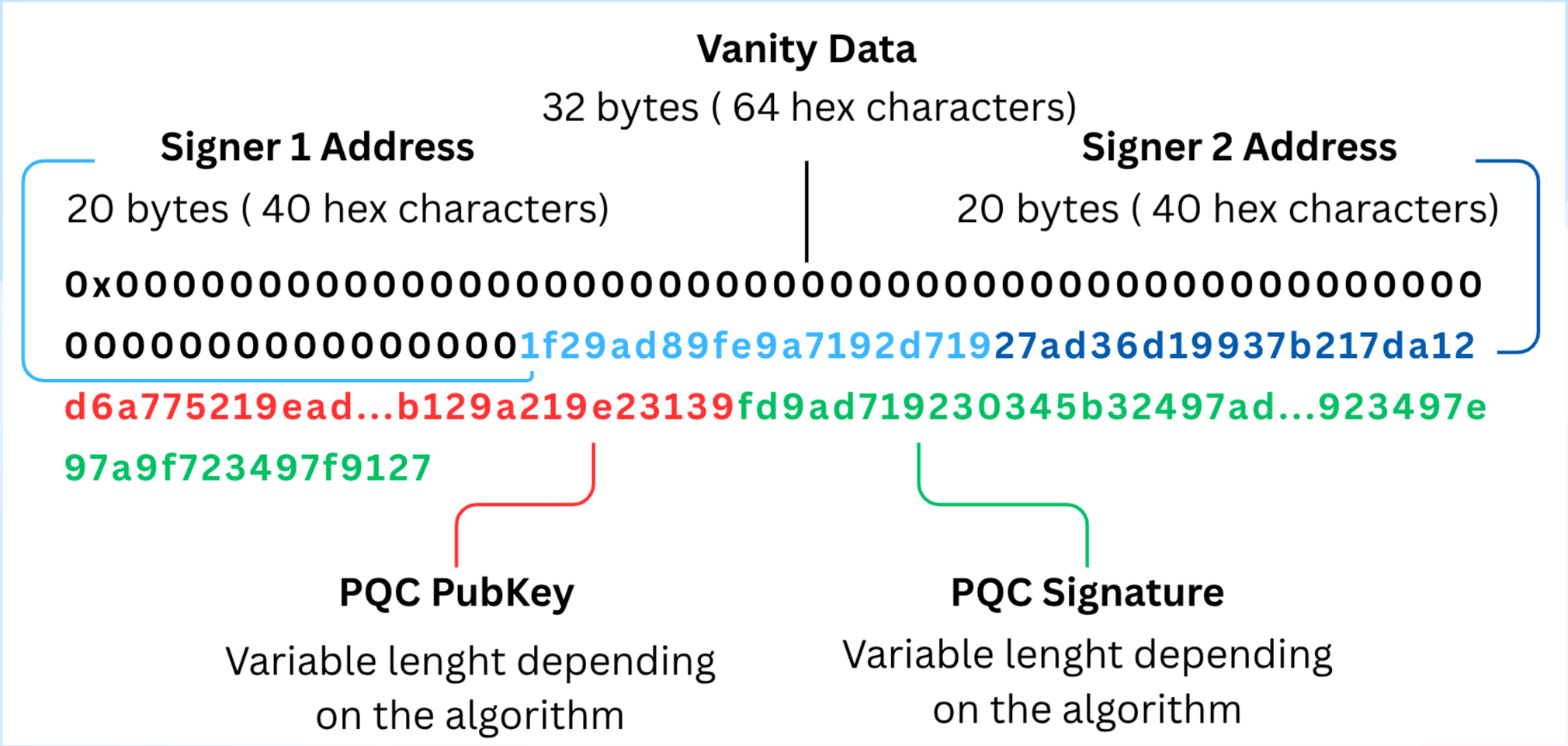
Avaliação de novos algoritmos pós-quânticos

- Arquitetura introduz assinaturas pós-quânticas na estrutura de dados do blockchain Ethereum (Hyperledger Besu) sem alterar os campos fundamentais.
- Adotou-se uma abordagem de assinaturas híbridas: cada bloco ou transação é assinado tanto pelo esquema clássico (ECDSA/secp256k1) quanto por um algoritmo PQC adicional.
- Rede continua reconhecendo e validando assinaturas ECDSA
- Dados da assinatura pós-quântica trafegam em campos estendidos, servindo como camada extra de segurança e evidência criptográfica.

Campo extra para assinatura PQC

- Exploramos o campo ExtraData do cabeçalho de bloco
- Normalmente contém 32 bytes de *vanity*, uma lista de endereços dos validadores, e 65 bytes da assinatura ECDSA do propositor do bloco.
- Estendemos o campo para incluir também a chave pública e a assinatura PQC do validador. Cada bloco, portanto, passou a carregar duas assinaturas: a padrão ECDSA (usada pelo protocolo para verificar o autor do bloco) e uma assinatura pós-quântica gerada com a chave PQC do mesmo validador.

Campo ExtraData estendido para assinaturas PQC



Assinaturas de transações

- Nas transações: adotada estratégia semelhante.
- Besu não possui campo nativo para múltiplas assinaturas
- Utilizamos o campo “data” da transação para embutir assinaturas pós-quânticas.
- Transações podem carregar “payload PQC” no campo data: normalmente é usado para dados de chamada de contrato ou mensagens arbitrárias.
- Pacote inclui a chave pública pós-quântica do remetente e sua assinatura PQC referente àquela transação.

Comparação entre formato de transações

Transação original
nonce = Inteiro **to =** Endereço (20 bytes) **value =** Inteiro (wei) **gas =** Inteiro **gasPrice =** Inteiro (wei) **data =** Parâmetros para *smart contracts*, etc. **chainID =** Inteiro

Transação PQC
nonce = Inteiro **to =** Endereço (20 bytes) **value =** Inteiro (wei) **gas =** Inteiro **gasPrice =** Inteiro (wei) **data =** Payload PQC (PubKey + Assinatura) **chainID =** inteiro

Resumindo a arquitetura de testes

- Rede permissionada Hyperledger Besu modificada, rodando alguns nós validadores (com Clique PoA) e nós não validadores.
- Cada validador com dois pares de chaves: um ECDSA (secp256k1) e um pós-quântico (ML-DSA, SLH-DSA ou MAYO).
- Nós reconhecem apenas endereços Ethereum derivados das chaves ECDSA, mantendo a compatibilidade com a infraestrutura original.

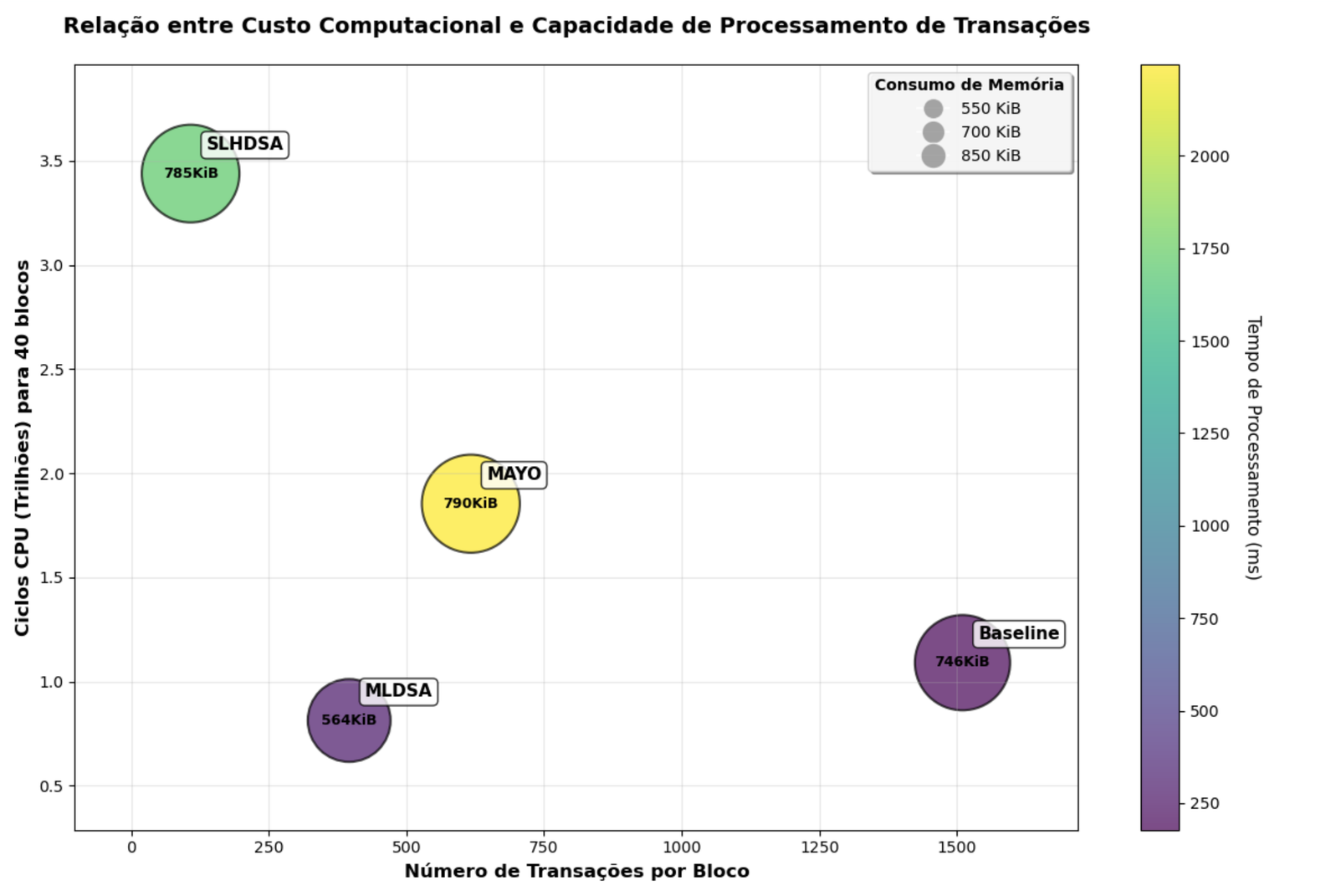
Avaliação de desempenho

Tamanhos de chaves e assinaturas em algoritmos de PQC

Algoritmo	Nível	Chave Pública (B)	Chave Privada (B)	Assinatura (B)
ML-DSA-44	1	1 312	2 560	2 420
ML-DSA-65	3	1 952	4 032	3 309
ML-DSA-87	5	2 592	4 896	4 627
SLH-DSA (SHA2-128s)	1	32	64	7 856
SLH-DSA (SHA2-128f)	1	32	64	17 088
SLH-DSA (SHA2-192s)	3	48	96	16 224
SLH-DSA (SHA2-256s)	5	64	128	29 792
MAYO-1	1	1 420	24	454
MAYO-2	1	4 912	24	186
MAYO-3	3	2 986	32	681
MAYO-5	5	5 554	40	964

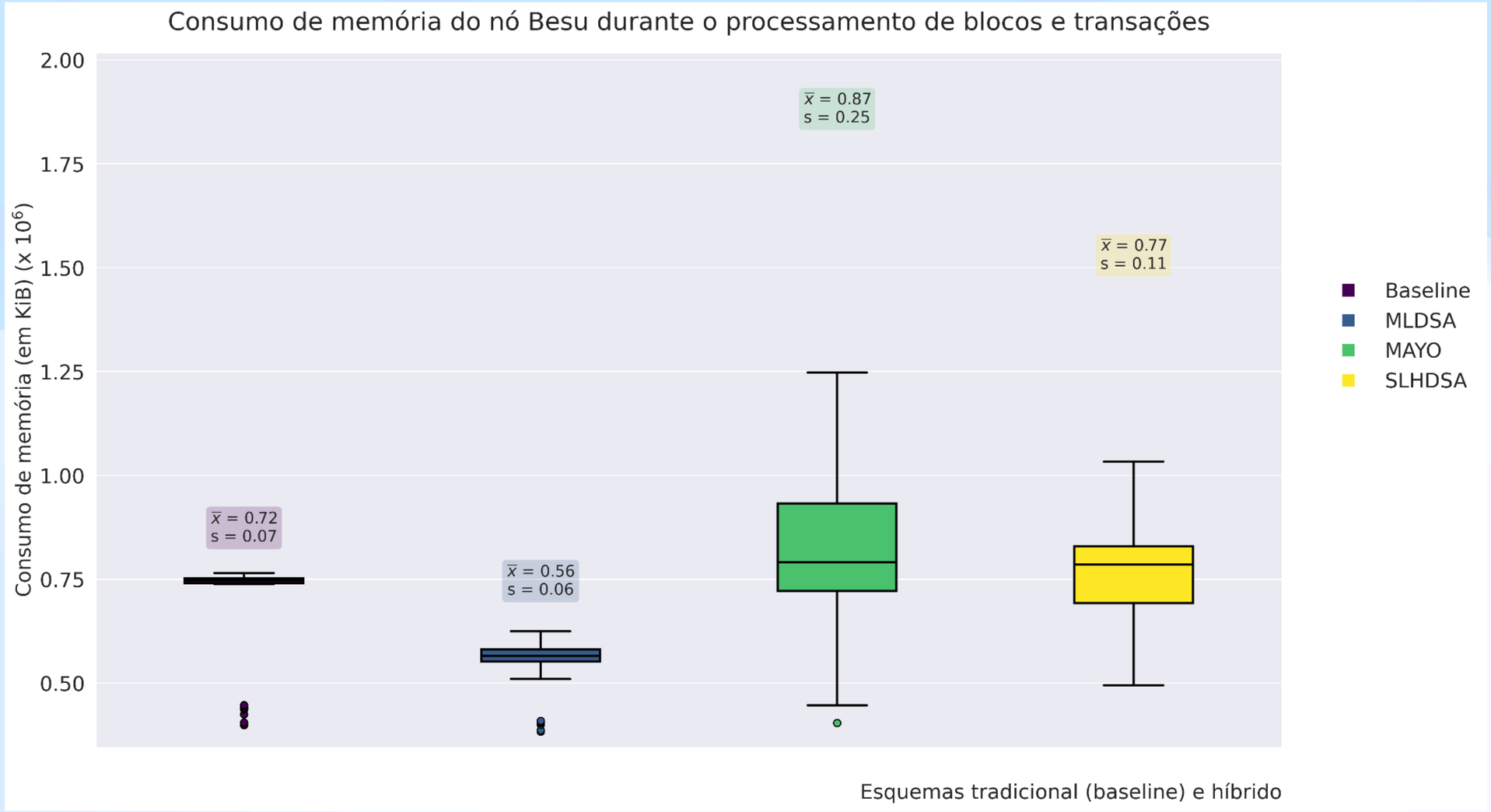
Avaliação de desempenho

Relação entre custo computacional e capacidade de processamento de transações.



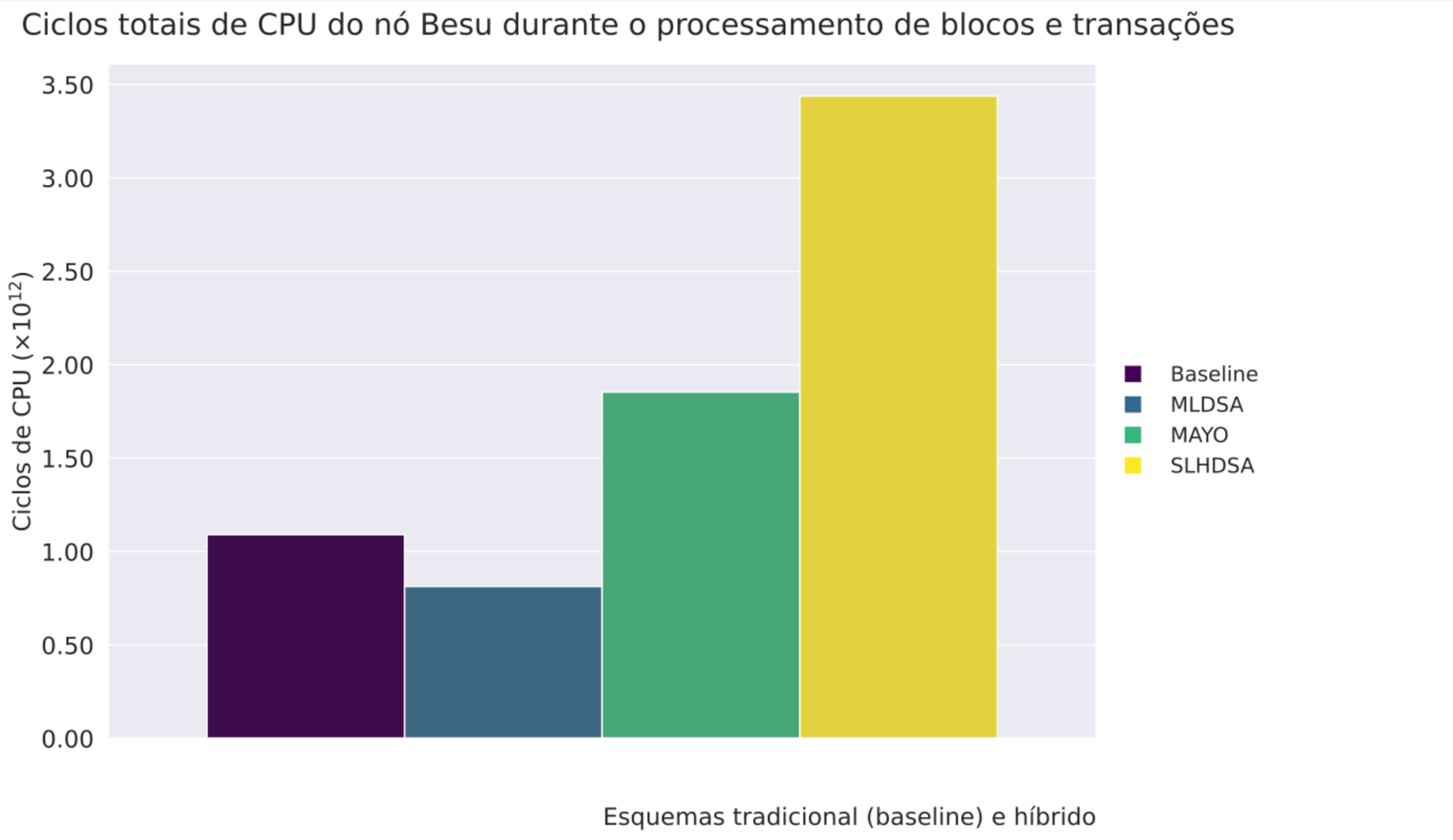
Avaliação de desempenho

Consumo de memória para processar 40 blocos com transações



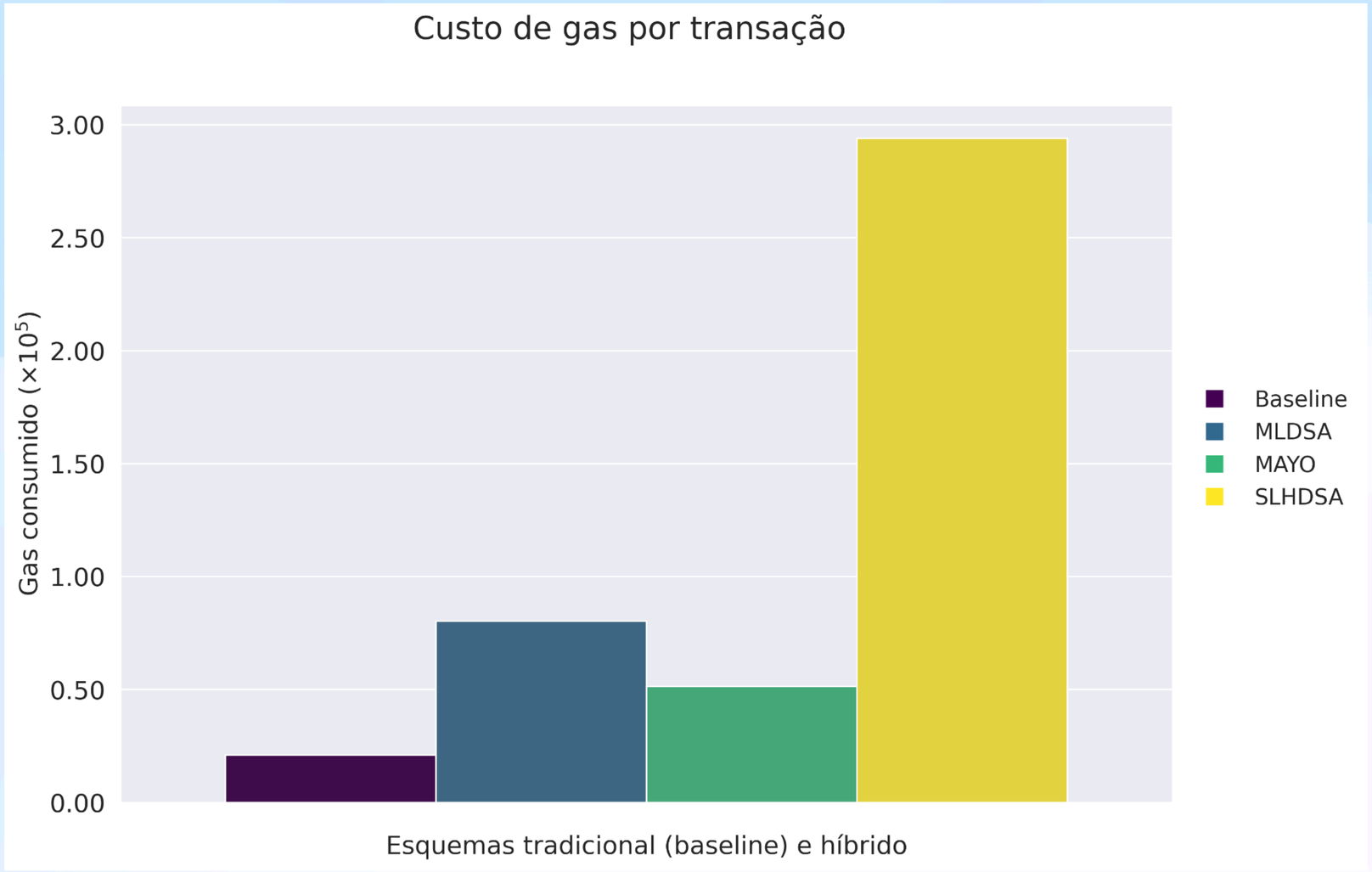
Avaliação de desempenho

Ciclos de CPU para processar 40 blocos com transações



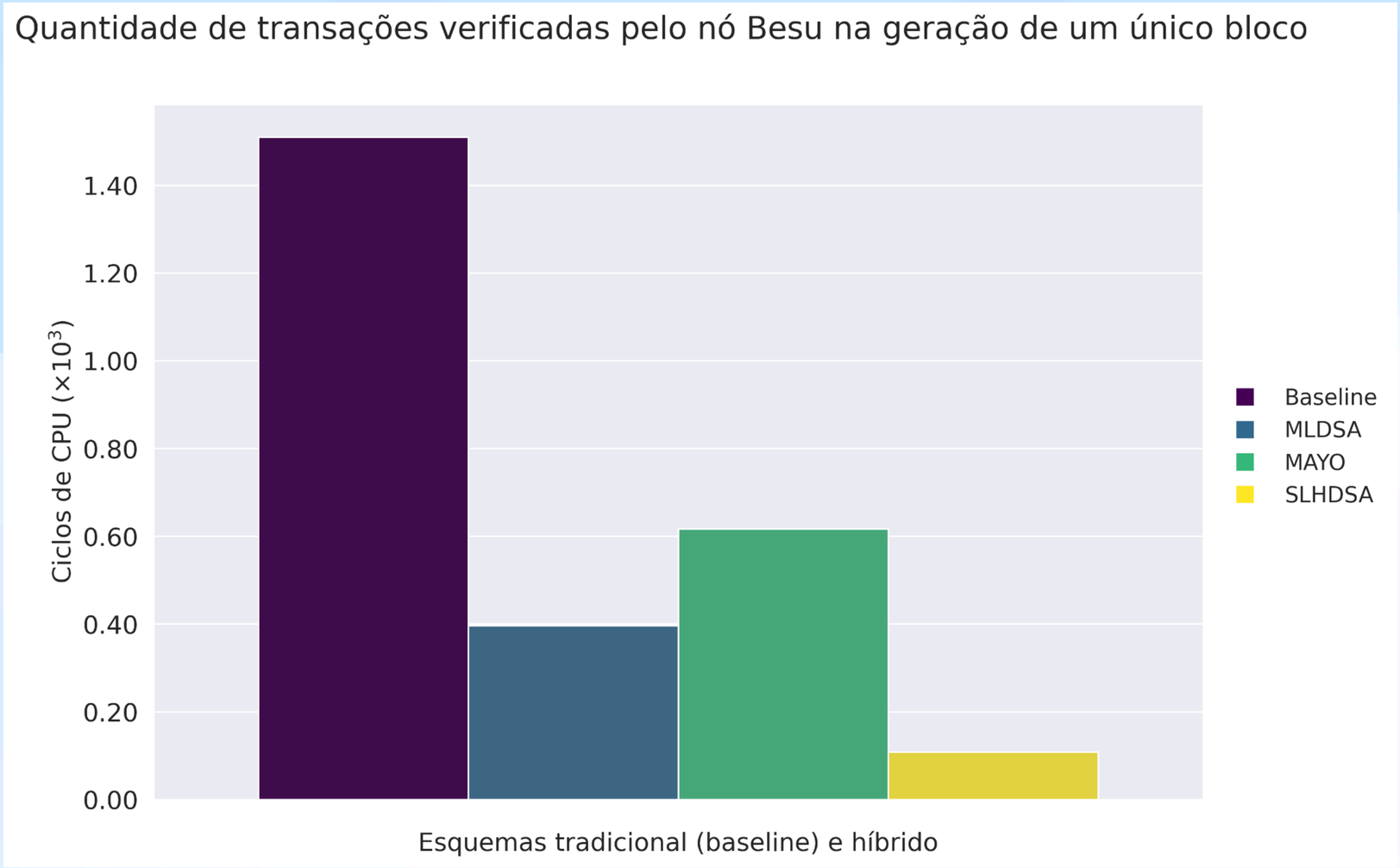
Avaliação de desempenho

Custo de gás para verificar cada transação em um nó Besu



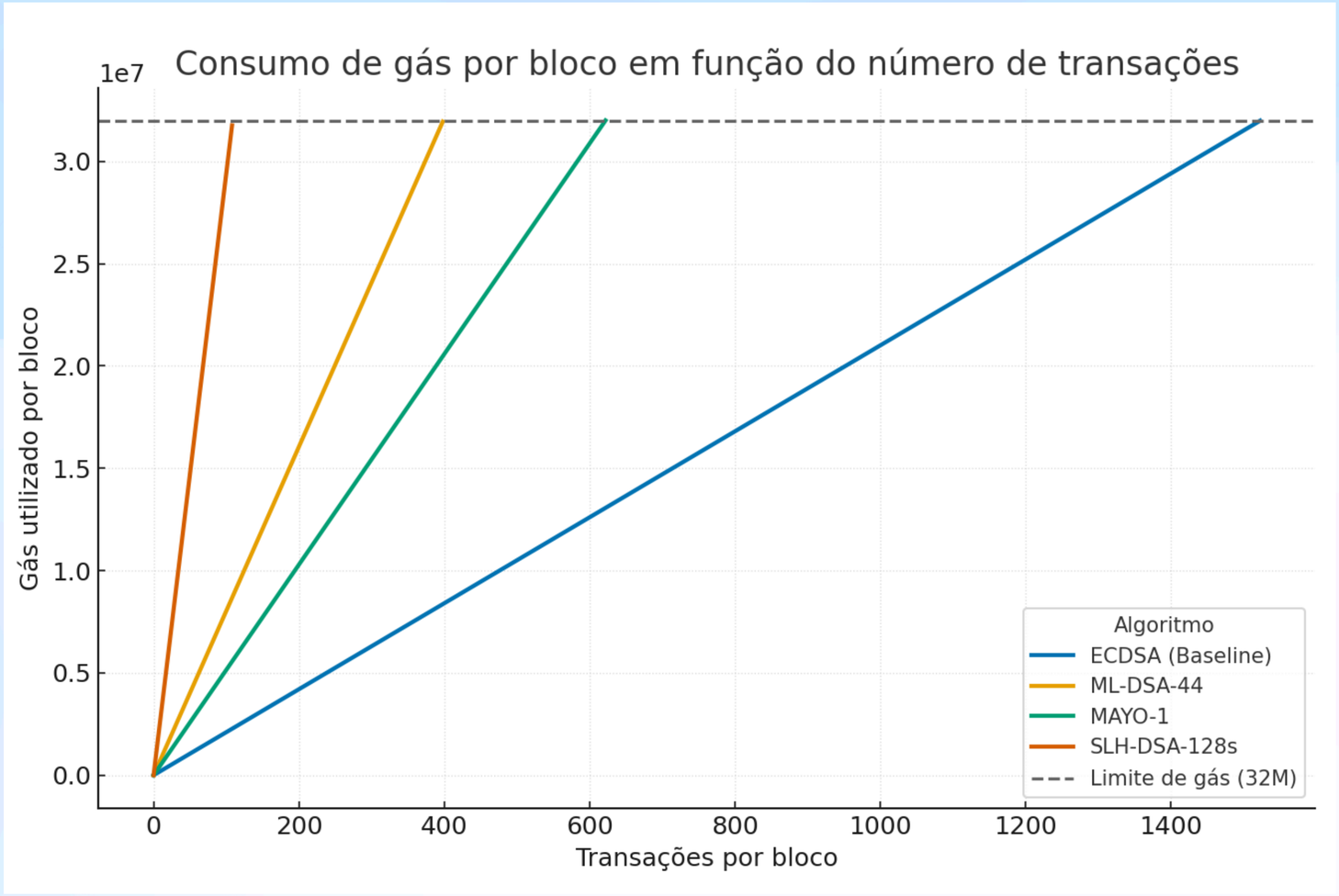
Avaliação de desempenho

Quantidade máxima de transações processadas em um único bloco



Avaliação de desempenho

Consumo de *gas* por bloco em relação ao número de transações



Avaliação de desempenho

Consumo de *gas* por bloco em relação ao número de transações

Algoritmo	Gás/tx	Tx/bloco (máx)	Redução vs ECDSA
ECDSA (Baseline)	21.000	1.510	—
ML-DSA-44	80.248	396	≈74%
MAYO-1	51.440	617	≈59%
SLH-DSA-128s	294.048	108	≈93%

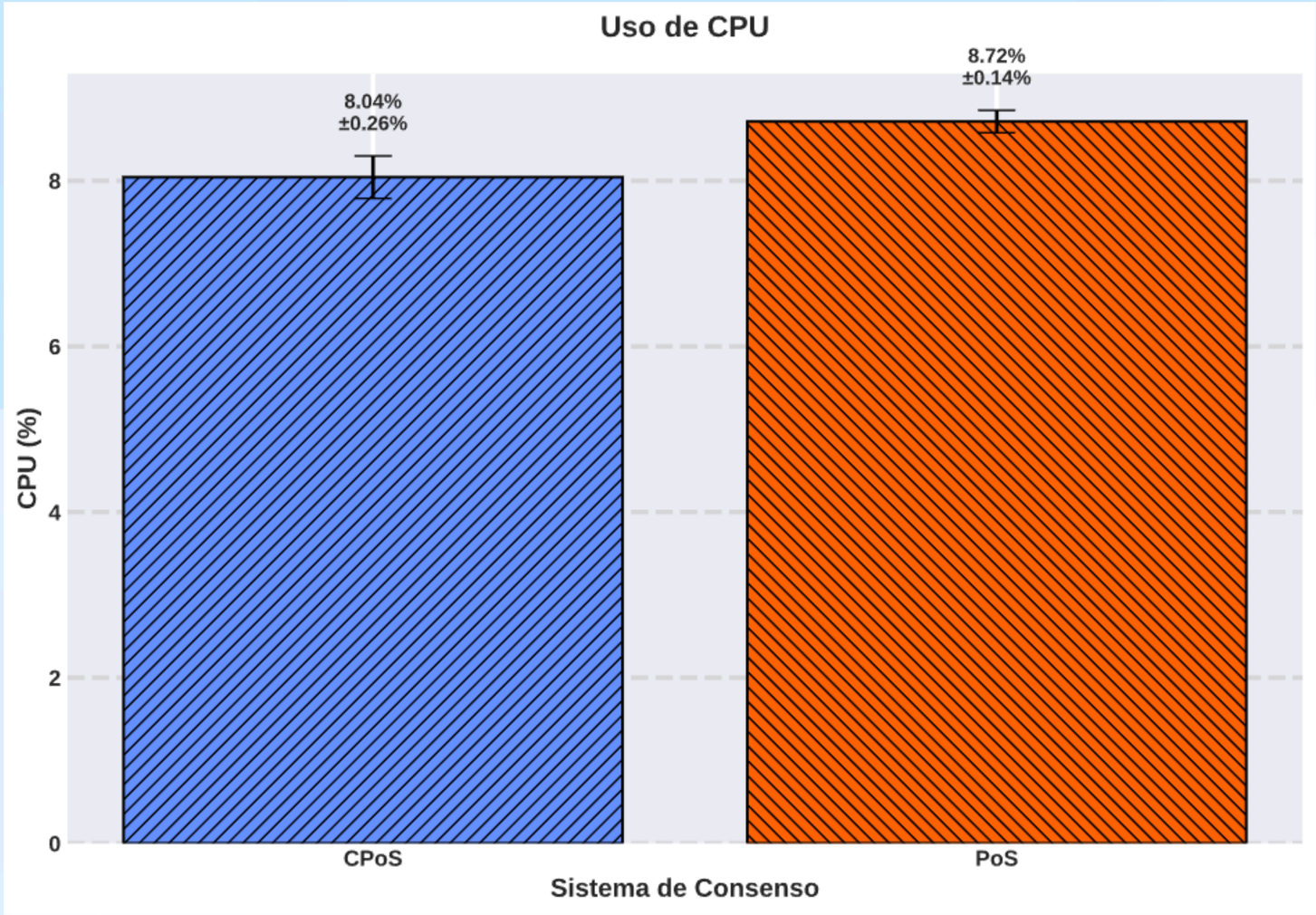
Avaliação de novo mecanismo de consenso

- Nesta frente buscamos aprimorar a segurança e eficiência das blockchains basedas no esquema de consenso Proof-of-Stake (PoS ou Prova de Posse).
- No PoS é comum recorrer a um comitê de validação para confirmar que um bloco proposto por um nó da rede é confiável, está de acordo com as regras da rede e pode ser anexado definitivamente à blockchain.
- Esse comitê é um ponto de vulnerabilidade pois, se seus membros são conhecidos a priori, existe a chance de que sejam corrompidos.
- Isso traz um outro problema para o consenso que adota os comitês de validação: complexidade, que custa mais tempo de processamento, requer mais recursos, cria um nível de centralização indesejado e pode gerar erros.

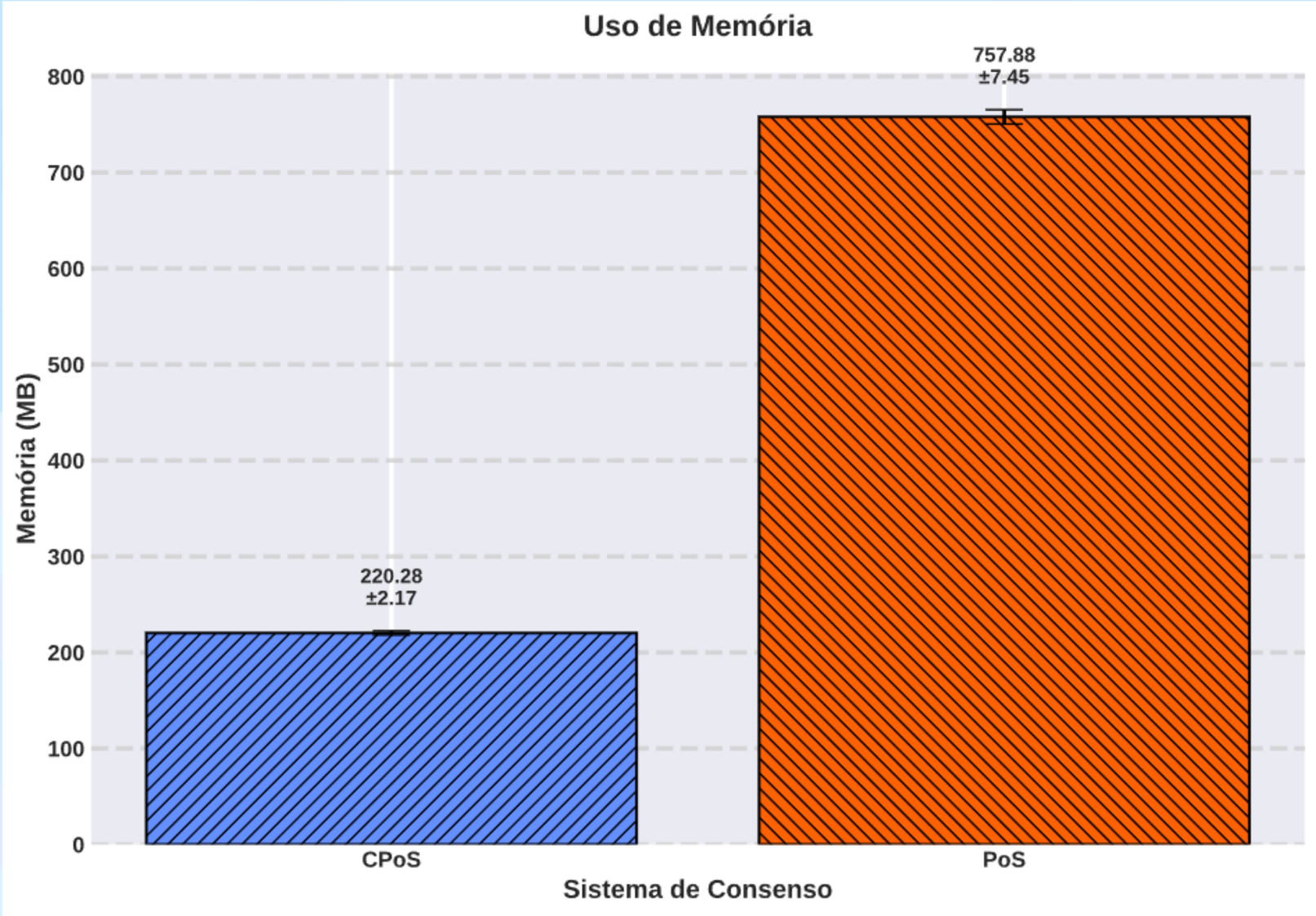
Committeeless Proof-of-Stake: CPoS

- Mecanismo de consenso baseado em PoS, mas sem exigir comitês de validação.
- É probabilístico e permite que nós que formam a rede consigam chegar, com uma probabilidade elevada, a um consenso sobre a validade de um bloco
- Baseia-se nas mensagens com propostas de blocos que circulam pela rede.
- Não é necessário configurar, proteger, gerenciar e desmanchar comitês de validação.
- Todos os nós da rede têm iguais condições de validar ou de recusar um bloco baseados nas informações que recebem e nas regras do protocolo que têm embutidas em seu código.
- Parâmetros de configuração desse mecanismo podem exigir um grande número de nós sorteados, sobrecarregando a rede.

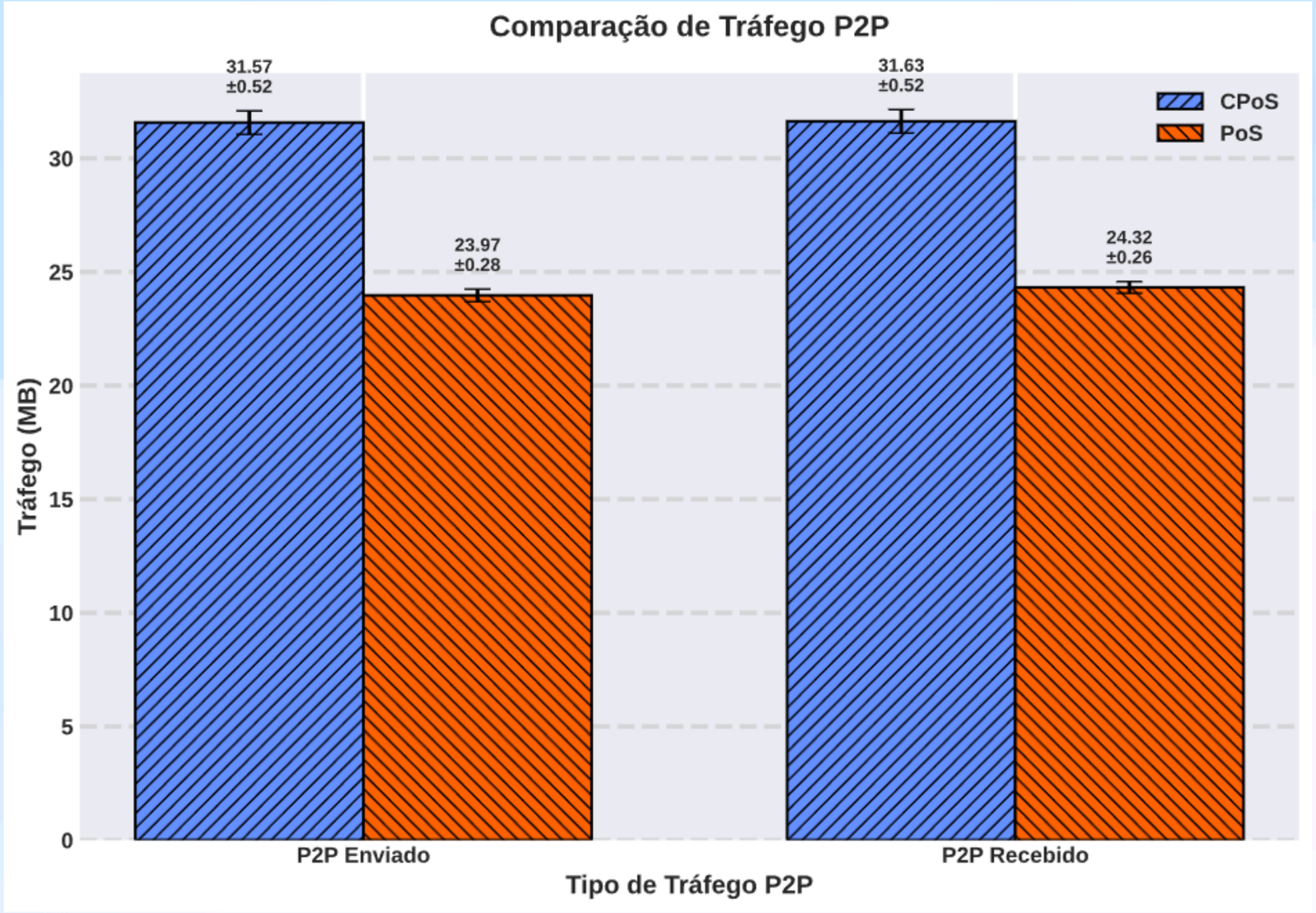
Avaliação de desempenho CPoS



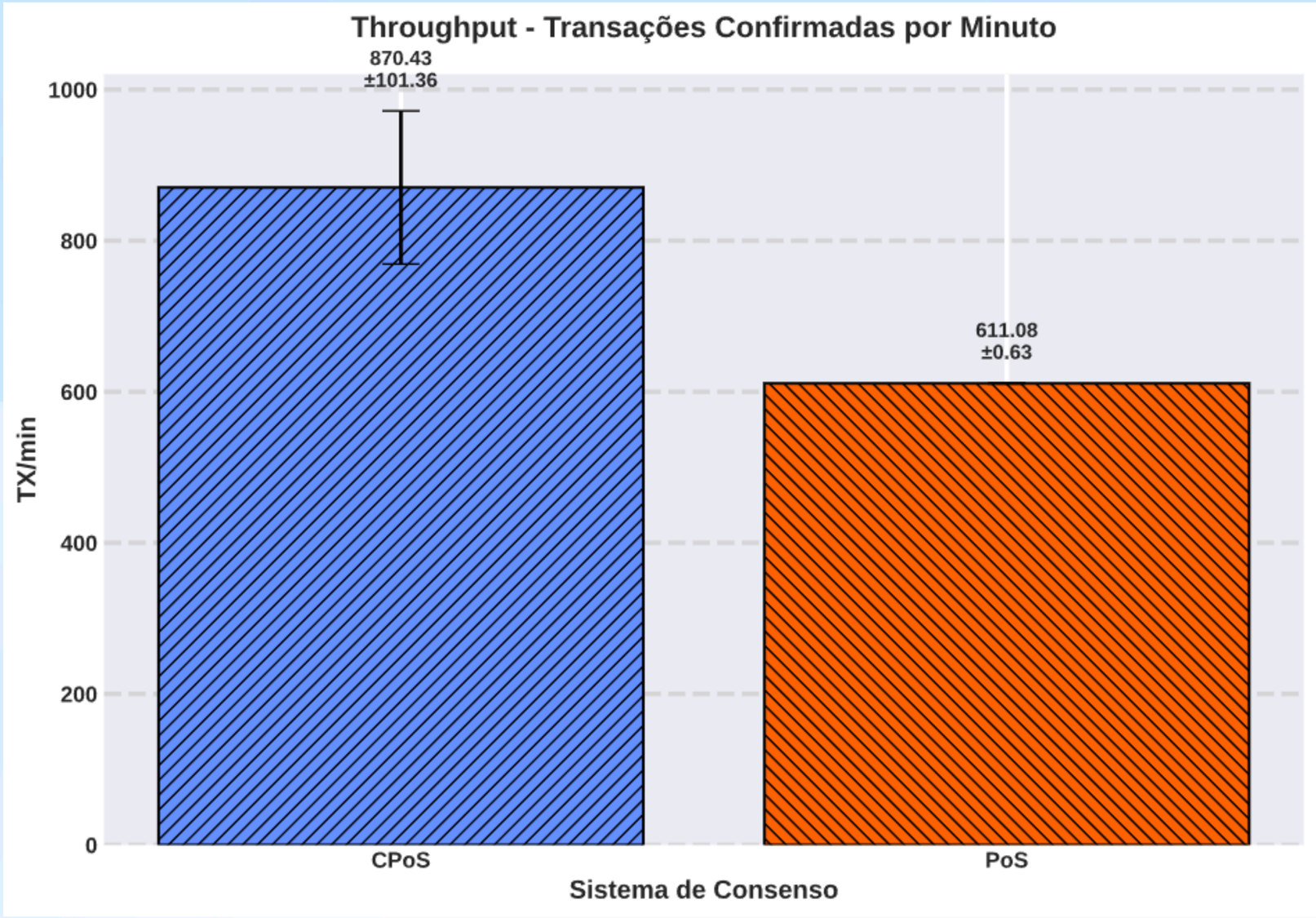
Avaliação de desempenho CPoS



Avaliação de desempenho CPoS



Avaliação de desempenho CPoS



Infraestrutura

Testbed RNP

- Utilização da infraestrutura do testbed de blockchains da RNP.
- Possibilidade de escalar experimentos para vários nós.
  - Possibilitou realizar testes mais confiáveis de desempenho para ambas as abordagens.

Impacto e Relevância

- Contribuição para a segurança e a evolução da tecnologia blockchain.
- Fortalecimento da pesquisa e desenvolvimento em criptografia pós-quântica.
- Formação de recursos humanos qualificados nas áreas de blockchain e cripto pós-quântica.

Conclusões

Uso de PQC na Besu

- Os experimentos evidenciaram o impacto direto dos algoritmos PQC sobre o consumo de gás, o número de transações por bloco e o uso de recursos computacionais, destacando o trade-off entre robustez criptográfica e escalabilidade.
- Esquemas ML-DSA-44 e MAYO-1 apresentam melhor relação entre segurança e eficiência.
- Assinatura baseada em hashes, SLH-DSA-128s, impõe custos significativamente mais altos.

Conclusões

Adoção de CPoS

- Uso de recursos computacionais bem próximo do PoS.
- Taxa de confirmamação de transações por minuto similar à do PoS.
- Uso de Besu facilitou bastante a mudança de consenso, pois se mostrou agnóstica em relação a este.

Conclusões

- O projeto SBS: Soluções para Blockchains Seguras procurou desenvolver soluções para proteger as blockchains contra as ameaças futuras.
- Os resultados podem impactar positivamente a segurança e a eficiência de blockchain, melhorando suas condições de uso em diversas áreas.

Equipe do Projeto

- Coordenador: Marco Amaral Henriques
- Colaboradores:
  - Rossano Pablo Pinto (doutorando)
  - Rodrigo Pierini (mestre)
  - Felipe Rampazzo (mestre)
  - Rodrigo de Meneses (mestrando)

Muito obrigado!

Marco Amaral Henriques

maah@unicamp.br