PROJETO iliaDB Blockchain em evolução.

PQC Group UTFPR

Benchmark de Blockchain Pós-Quântica



Alexandre Augusto Giron

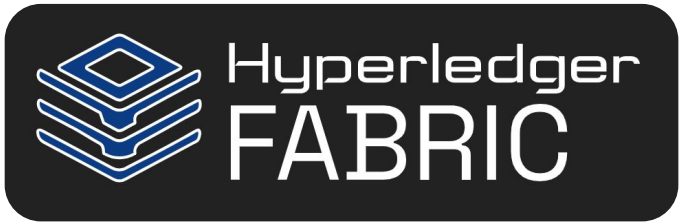
UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Roteiro da Apresentação

1. **Blockchains e a Ameaça Quântica**
2. **Solução: Criptografia Pós-Quântica**
3. **Trabalhos do BBPQ**
4. **Resultados Esperados**
5. **Referências & Agradecimentos**

Blockchain como uma tecnologia consolidada

- **Útil para diversas aplicações**
  - Rastreamento (logística/ cadeia transparente)
  - Identidade e credenciais digitais
  - Automatização de processos, contratos e de transações
  - Tokenização de ativos, NFTs...
  - Estônia: um dos primeiros países a utilizar blockchain em serviços de governo
    - Emirados Árabes Unidos, Austrália, EUA, Suécia, Singapura, Japão também estão utilizando
- **Tecnologias abertas**
  - Exemplo: Ecossistema Hyperledger
    - **Hyperledger Fabric**



Hyperledger Fabric

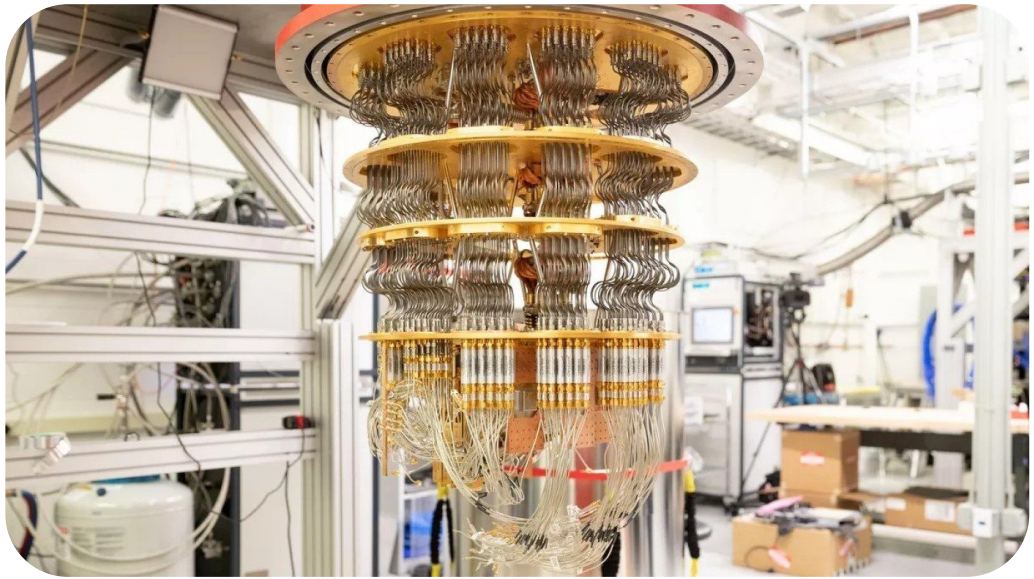
- **Diversos Casos de Uso**
  - Agricultura, *e-gov*, saúde, contratos inteligentes, educação ...
  - Veja mais em: https://lf-hyperledger.atlassian.net/wiki/spaces/LMDWG/pages/18710749/Use+Cases



- *Hashes* Criptográficos e Criptografia de Chaves Públicas
  - **Primitivas básicas para a Segurança das Blockchains**
  - Autenticação de transações
  - Integridade Forte (“Strong integrity”)
  - Conexões seguras com **TLS** (*Transport Layer Security*) entre nodos da rede

A Ameaça Quântica à Criptografia

- Algoritmo Quântico de Peter Shor
  - **Criptografia de chaves públicas** mais usada hoje é **vulnerável**!
  - Solução eficiente para o problema matemático no qual esquemas populares são baseados
  - RSA, ECDSA, EdDSA...
  - Curvas Elípticas em geral



A (ou uma) **Solução**

- *Post-Quantum Cryptography* (**PQC**) */ Quantum-resistant / Quantum-safe*
- Criptografia resistente ao computador quântico
- Cenário da Criptografia Pós-Quântica
  - Usuários utilizando computadores atuais (arquiteturas convencionais); vs
  - Adversários utilizando computadores quânticos

Criptografia Pós-Quântica ≠ Criptografia Quântica!

Quando aplicar a solução? (Exemplos)

https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en



Note 30-LegacyRSA. The acceptability deadline for the legacy use of modulus of size above 1900 bits, but less that 3000 bits, is set to December 31, 2025. A later acceptability deadline for user/data authentication with this particular algorithm may be set on a national level.

BankInfoSecurity
https://www.bankinfosecurity.com › ... · Traduzir esta página

Australia to Phase Out Weak Encryption Algorithms by 2030

17 de dez. de 2024 — **Australia has rolled out an ambitious road map** to prepare for future quantum-enabled cyberattacks. Regulators are ready to set an end date ...

Migração para PQC: exemplos

- **Blockchains conhecidas já têm planos de migração para PQC**
  - Ethereum: https://www.btq.com/blog/ethereums-roadmap-post-quantum-cryptography
  - PQFabric [1], QRL [2], PQC em Bitcoin [3], ...
- **Algumas conclusões**
  - "*necessidade de esquemas mais eficientes para blockchain e DLT*" [4]
  - Avaliar novas alternativas PQC
  - Experimentos práticos e mais realistas
  - Disponibilizar com reprodutibilidade

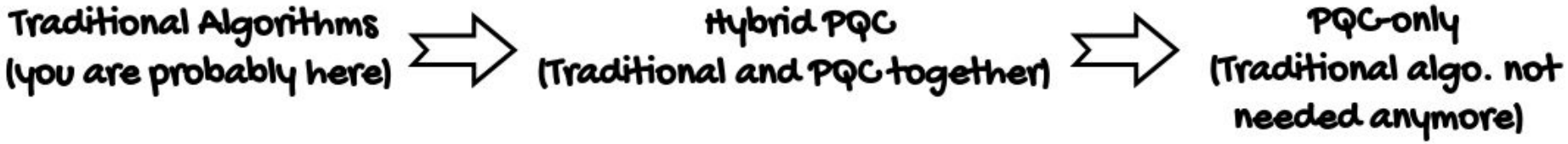
Desafios & Exemplos que fracassaram

- **Desafios:**
  - A confiança nos algoritmos novos
  - A confiança nas implementações novas
  - Problemas de ***crypto agility***
  - Complexidade das infraestruturas, hardware criptográfico, ...

- **Problemas de Adoção de PQC:**
  - Criptomoeda "XYZ" (sem citar nomes): operou por ~3,4 anos com o algoritmo PQC *Rainbow*



Modo Híbrido: o que é & **suas vantagens**

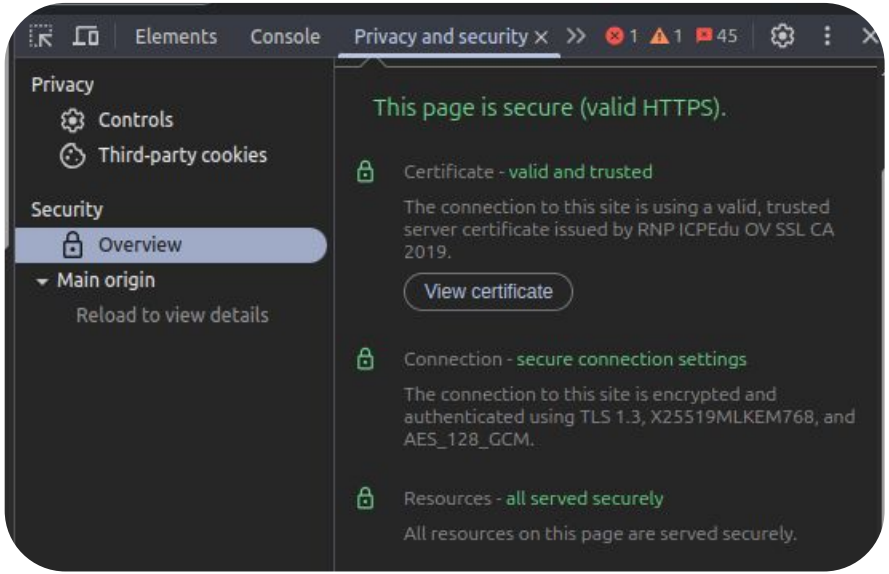


- Sobre a **Confiança**
  - Combinar dois (ou mais) algoritmos: ex. um pré e outro pós-quântico
  - A segurança permanece enquanto ao menos um não foi quebrado

- Pontos **Positivos**:
  - Transição não-disruptiva
  - Confiança na criptografia atual
  - Nível de escrutínio de software
  - Regulações e conformidade

PQC e o modo híbrido já é uma realidade!

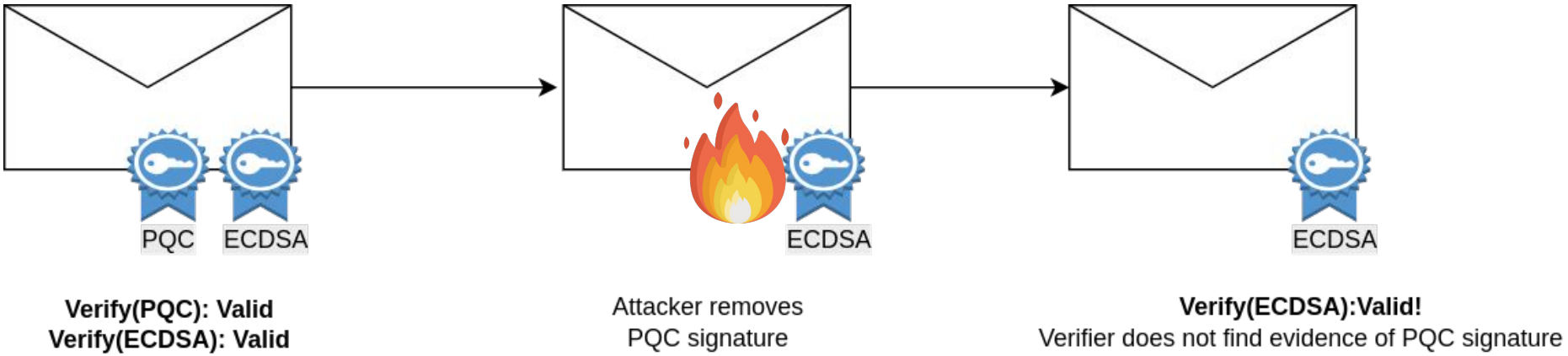
- Google Chrome v116 (*default* na versão v131), Firefox v132+
- iMessage PQ3: iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4
- OpenSSH v9 e v10
- Amazon AWS (Common Runtime versão 2.30.22)
- ...
- Mas a adoção não é tão simples!



*Obs: para a **autenticação** a PQC ainda não está consolidada (ex: Processo de padronização do NIST: "On Ramp")*

Conhecendo possíveis ataques no híbrido

“Stripping attacks”: exemplo



Conhecendo o **BBPQ - Propostas**



- **Propostas**
  - Integrar e Avaliar a eficiência da PQC em Blockchains (com ênfase em Hyperledger Fabric)
  - **Melhorar** o uso do modo híbrido
    - Ex: *ed25519-AVX2*
    - Padrão “**composite**”
    - Assinaturas mais **compactas**
  - Adaptar o Hyperledger Fabric para **incluir PQC**:
    - Nas operações de autenticação (assinatura digital)
    - Nas conexões entre os nodos da rede (ex: TLS)

Conhecendo o BBPQ - Equipe

- Equipe
  - Alexandre Boutrik
  - Eduardo Bif Pitol
  - Danilo Solek
  - Gabriel dos Santos Schmitz
  - Alexandre Augusto Giron
- Curso de Engenharia de Computação da UTFPR

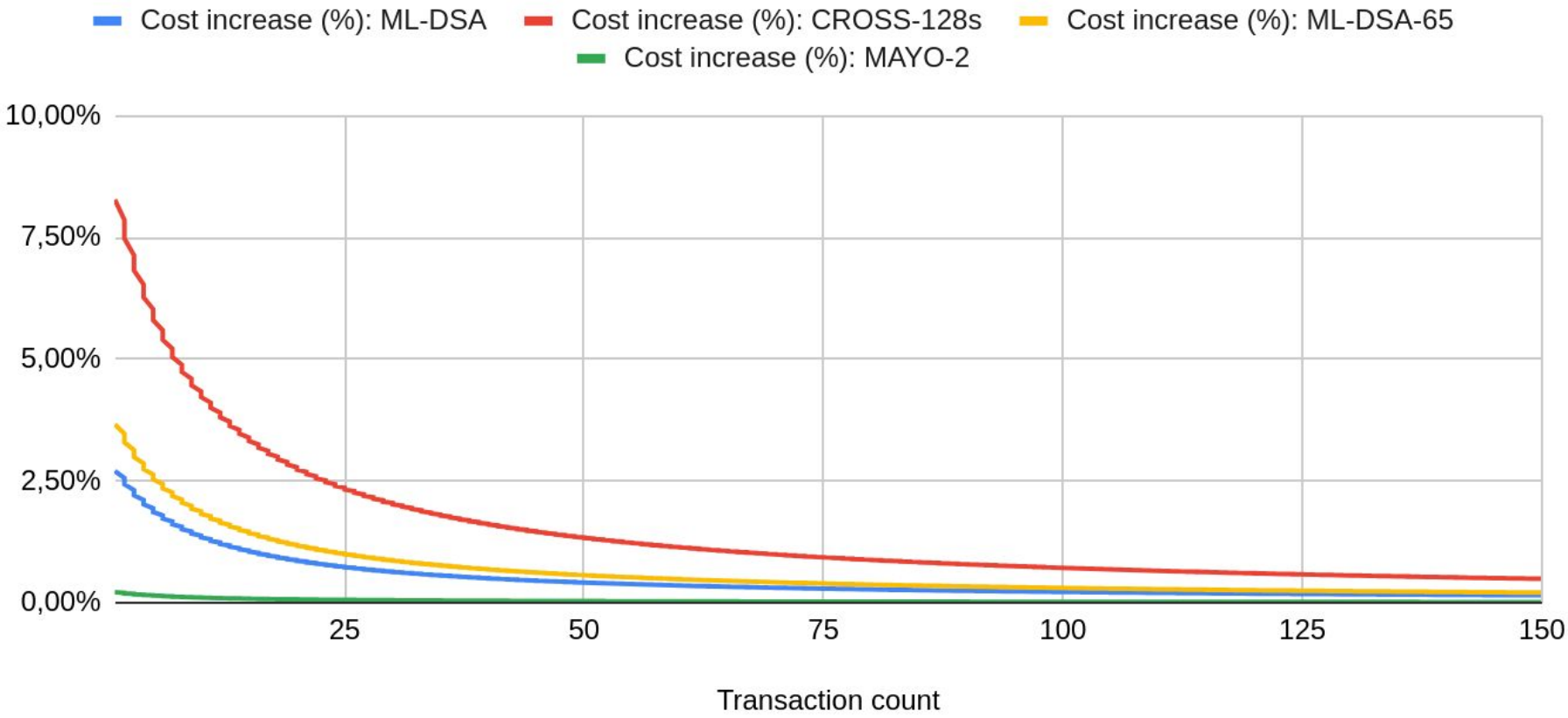


Conhecendo o BBPQ - Resultados Preliminares

- Atividades de **Desenvolvimento**
  - Plantel de algoritmos na API (“go-std”): **34 variantes PQC integradas**
  - Uso do modo híbrido
  - Prefixos para **proteção** contra “*stripping attacks*”
  - Integração com Hyperledger Fabric (em andamento)

- Atividades de **Pesquisa**
  - Experimentos (***benchmarks***) para conhecer os impactos (em andamento)
  - Estimativas de custo de armazenamento (*storage*)
  - **Publicações**: Apresentação de resultados preliminares no SBSeg 2025 (sessão de pôsteres)

Cost increase Estimate over ECDSA - Fabric 2.5.12 test network



Conhecendo o BBPQ - Resultados Esperados

- Recomendar melhores escolhas subsidiadas por *benchmarks* no cenário nacional
  - *ex: Redes de curta vs longa distância*
- Disponibilizar implementação para a comunidade
- Publicação & Divulgação Científica

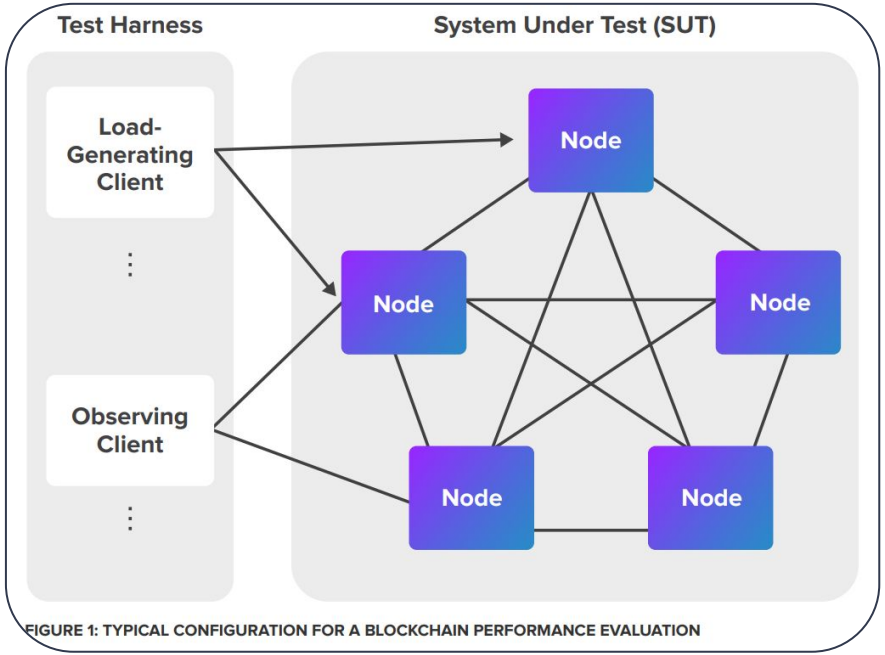


FIGURE 1: TYPICAL CONFIGURATION FOR A BLOCKCHAIN PERFORMANCE EVALUATION

https://www.lfdecentralizedtrust.org/learn/publications/blockchain-performance-metrics

Agradecimentos

- **Em nome do BBPQ, gostaríamos de agradecer:**
  - Ao apoio da RNP/Projeto ILÍADA
  - Ao Observatório Nacional de Blockchain







OBSERVATÓRIO
NACIONAL DE
BLOCKCHAIN

Referências

[1] HOLCOMB, Amelia et al. Pqfabric: a permissioned blockchain secure from both classical and quantum attacks. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2021. p. 1-9.
[2] ABBAS, Shahroz, SULTANA, Ajmery e KADDOUM, Georges. Quantum-Safe Blockchain in Hyperledger Fabric. IEEE Networking Letters, p. 1–1, 2024. DOI: 10.1109/LNET.2024.3522966.
[3] The Quantum Resistant Ledger: https://www.theqrl.org/.
[4] LEÓN-CHÁVEZ, Miguel Ángel; PERIN, Lucas Pandolfo; RODRÍGUEZ-HENRÍQUEZ, Francisco. Post-Quantum Digital Signatures for Bitcoin. In: Principles and Practice of Blockchains. Cham: Springer International Publishing, 2022. p. 251-270.
[5] HOLMES, Stephen. Impact of post-quantum signatures on blockchain and DLT system. In: DLT. 2023.

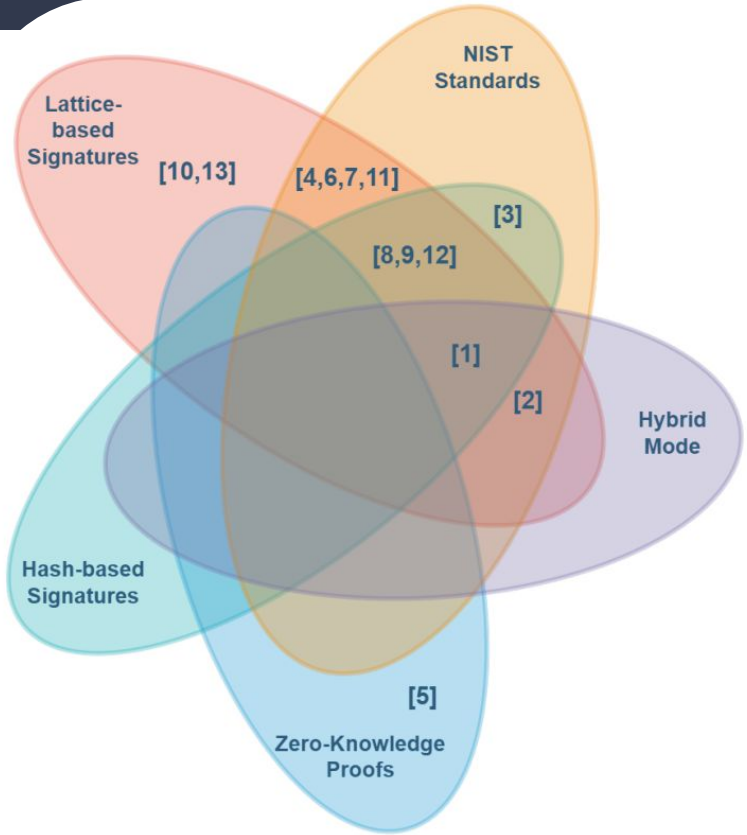
Obrigado pela atenção

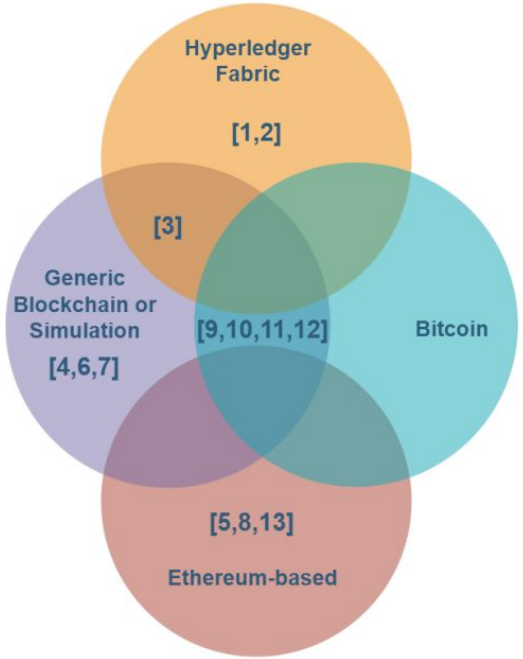
alexandregiron@utfpr.edu.br



Backups

Exemplos de Blockchains Pós-Quânticas

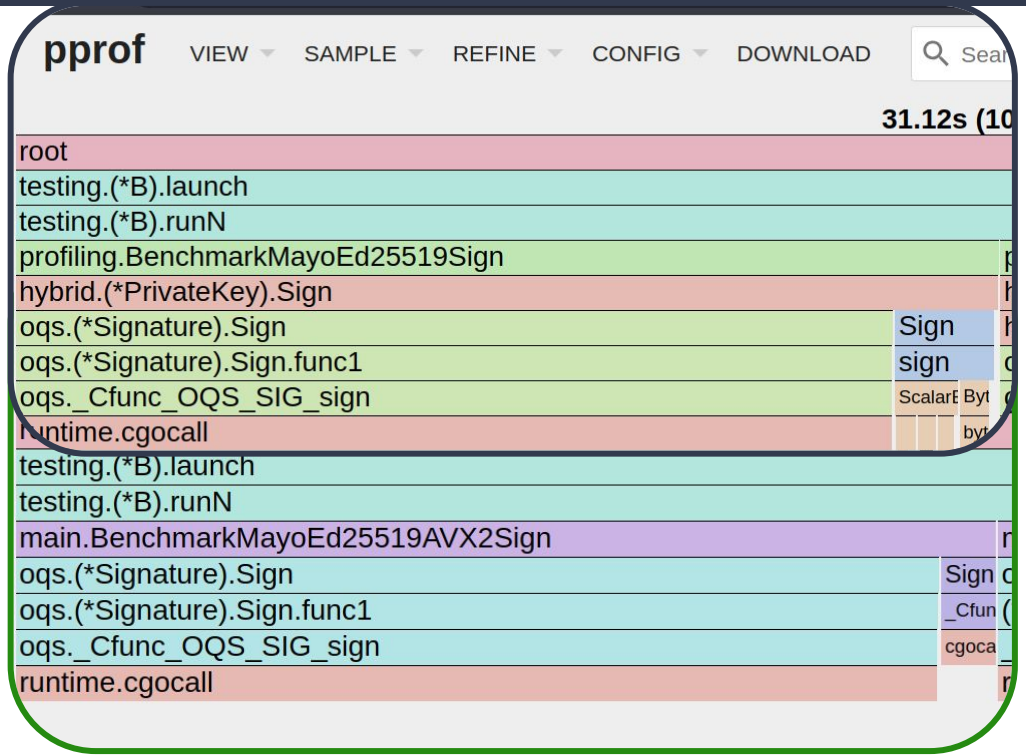




List of Related Studies:

[1] Holcomb et al. 2021
[2] Abbas et al. 2025
[3] Zhukabayeva et al. 2024
[4] Castiglione et al. 2025
[5] Fan et al. 2025
[6] Kim et al. 2024
[7] Shah et al. 2024
[8] Juaristi et al. 2024
[9] Holmes 2023
[10] Semmouni et al. 2019
[11] León-Chávez et al. 2023
[12] Pont et al. 2024
[13] Pan et al. 2025

Conhecendo o BBPQ - Resultados Preliminares



Especificação

Tabela 4: Configuração do Testbed para os experimentos de avaliação.

Tipo de Nodo	Qde	Descrição	Localização
Endorser /peer	mín: 3 max: 5	A política de *endorsement* será definida para a mínima, ou seja, a ao menos uma organização dá o "aval" à transação. Para fins de replicação,	Região Centro-Oeste (e.g., Distrito Federal)
Orderer	mín: 3 max: 5	Um número ímpar de orderers é recomendado. Com 3 ou 5 nodos, o sistema tolera 1 ou 2 nodos falhos sem interrupção do serviço. Se houver apenas um nodo ordenador, o consenso não executará e isso limitará o aspecto prático (realismo) do experimento.	Região Centro-Oeste (e.g., Distrito Federal)
"Cliente 1"	1	Conexões de "longa distância": estabelecer 1 cliente geograficamente distante, observando-se as maiores latências e número de saltos *hops* disponível na infraestrutura.	Região Sul (e.g., Porto Alegre) ou Região Nordeste (e.g., João Pessoa)
"Cliente 2"	1	Conexões de "curta distância": estabelecer 1 cliente próximo à infraestrutura.	Região Centro-Oeste