Avaliação Comparativa de Contratos de Identidade Descentralizada em Plataformas Blockchain Permissionadas

Jeffson Celeiro Sousa[1,2], **Bruno Evaristo**[1,2],
Antonio Mateus de Sousa[1], **Ismael Ávila**[1]

[1] Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

[2]Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

{jcsousa, elderb, amateus, avila_an}@cpqd.com.br

Resumo. *Este trabalho avalia o desempenho de contratos inteligentes para gestão de identidades digitais descentralizadas (DIDs) em redes blockchain baseadas em Ethereum. Foram analisadas operações-chave do ciclo de vida de identidades utilizando Hyperledger Caliper em ambiente permissionado com consenso QBFT. As métricas de vazão, latência e uso de recursos indicam que a abordagem apresenta boa escalabilidade e flexibilidade, destacando seu potencial para soluções de identidade autossoberana (SSI) em contextos regulados.*

Abstract. *This work presents a performance evaluation of smart contracts for managing decentralized digital identities (DIDs) on Ethereum-based blockchain networks. Key identity lifecycle operations were benchmarked using Hyperledger Caliper in a permissioned environment with QBFT consensus. Metrics such as throughput, latency, and resource usage demonstrate the scalability and flexibility of the approach, reinforcing its viability for Self-Sovereign Identity (SSI) solutions in regulated and enterprise contexts.*

1. Introdução

A Identidade Autossoberana (SSI) propõe uma alternativa aos modelos tradicionais de gerenciamento de identidade digital, reduzindo a dependência de autoridades centralizadas e promovendo maior privacidade e controle ao usuário, conforme definido por padrões como W3C DID e Verifiable Credentials.

O Hyperledger Indy foi pioneiro na aplicação prática da SSI, operando como um ledger público permissionado com consenso RBFT, amplamente utilizado por redes como Sovrin e frameworks como Hyperledger Aries para resolução de DIDs e gerenciamento de credenciais.

Diante de limitações de escalabilidade e interoperabilidade, surgiu o Indy Besu, que migra a lógica SSI para o Hyperledger Besu, utilizando contratos inteligentes em Solidity. Embora métodos como did:ethr explorem essa abordagem, ainda há escassez de estudos sobre o desempenho de contratos de identidade em redes permissionadas. Este artigo visa preencher essa lacuna por meio de uma análise comparativa da execução de contratos DID na rede Besu, avaliando métricas sob diferentes condições experimentais.

O restante do trabalho está estruturado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados, a Seção 3 descreve a proposta, a Seção 4 detalha a metodologia de avaliação, e discute os resultados, e a Seção 5 traz as conclusões e direções futuras.

2. Trabalhos Relacionados

Diversos estudos têm investigado o desempenho de plataformas blockchain como Ethereum, Hyperledger Fabric e Indy, impulsionados por sua crescente adoção em ambientes corporativos e institucionais. O *Hyperledger Caliper* tem se consolidado como ferramenta padrão nesses trabalhos, por oferecer uma estrutura de benchmarking padronizada e reprodutível para redes permissionadas e públicas.

[Kaushal e Kumar 2024] utilizaram o Caliper para avaliar uma rede Fabric em um cenário de monitoramento remoto de pacientes (RPM), observando estabilidade no desempenho sob diferentes taxas de transação. Kshirsagar et al.[Kshirsagar e Pachghare 2022] propuseram o mecanismo de consenso *Proof of Scope*, que superou algoritmos como Raft e PoW-Ethash com ganhos de até 38% em latência e 22% em vazão. [Melo et al. 2024] propuseram um modelo de desempenho baseado em *Stochastic Petri Nets*, validado com alto grau de confiança. O trabalho demonstrou a sensibilidade do desempenho da Hyperledger Fabric ao tamanho dos blocos e às políticas de endosso.

[Choi e Won-Ki Hong 2021] compararam uma rede Ethereum privada com a testnet Ropsten, concluindo que a rede privada apresentou menor latência, maior vazão e maior estabilidade, sobretudo em transações simples. No contexto da identidade descentralizada, [Bastos et al. 2024] apresentaram o *MinIndy*, uma ferramenta para automação da implantação e gestão de redes Hyperledger Indy, mantendo desempenho equivalente ao modelo manual, com uso de Docker e Ansible.

Para o Hyperledger Besu, estudos ainda são escassos. Em [Fan et al. 2022], foi conduzida uma avaliação abrangente com Caliper, analisando os algoritmos de consenso PoA, IBFT 2.0 e QBFT. Os resultados mostraram que o QBFT suporta até 14 validadores sem degradação perceptível de performance, sendo o tempo e o tamanho de bloco fatores determinantes para o desempenho. [Mostarda et al. 2023] propuseram uma ferramenta de benchmarking específica para redes Besu operadas por múltiplas organizações, revelando anomalias em validadores que incluíam blocos vazios ou com poucas transações. Essa abordagem superou as limitações do Caliper ao oferecer análises mais detalhadas e adaptadas a ambientes reais.

Trabalho	Blockchain	Caliper	Consenso Avaliado	Modelo Reprodutível	Avaliação DID	Ferramenta Personalizada
[Kaushal e Kumar 2024]	Fabric	✓	Solo	✗	✗	✗
[Kshirsagar e Pachghare 2022]	Fabric	✓	Proof of Scope	✗	✗	✗
[Melo et al. 2024]	Fabric	✓	Solo	✓	✗	✗
[Choi e Won-Ki Hong 2021]	Ethereum	✓	PoW	✗	✗	✗
[Bastos et al. 2024]	Indy	✗	RBFT	✓	✓	✗
[Fan et al. 2022]	Besu	✓	QBFT, IBFT 2.0, PoA	✗	✗	✗
[Mostarda et al. 2023]	Besu	✓	QBFT	✓	✗	✓
Proposta	Besu	✓	QBFT	✓	✓	✗

Tabela 1. Resumo dos trabalhos relacionados e suas características principais.

A Tabela 1 resume os principais aspectos dos trabalhos discutidos. Em geral, este trabalho se diferencia principalmente em dois pontos: (i) por realizar uma avaliação

de desempenho focada em contratos inteligentes voltados à identidade descentralizada (DID) na Hyperledger Besu, baseando-se em operações fundamentais do ciclo de vida de identidades digitais; e (ii) por apresentar um cenário reprodutível com configurações completas de rede, contratos e benchmarking disponibilizados publicamente.

3. Proposta de Arquitetura e Cenário de Avaliação

Esta seção propõe uma arquitetura para avaliar o desempenho de contratos inteligentes de identidade descentralizada (DID) nas plataformas *Hyperledger Indy* e *Indy Besu*, visando uma comparação sistemática quanto a desempenho, escalabilidade e complexidade operacional.

O *Hyperledger Besu* é um cliente Ethereum modular, compatível com EVM e utilizado em redes permissionadas com suporte a contratos em Solidity. Ele permite integração com ferramentas como `ethers.js` e Hardhat, e oferece métricas via Prometheus. A iniciativa *Indy Besu* implementa contratos inteligentes que replicam as operações do Indy, como `createDid`, `updateDid` e `createCredentialDefinition`, possibilitando identidades autossoberanas em ambientes Ethereum, compatíveis com métodos como `did:ethr` e `did:indy:besu`.

Tabela 2. Comparação entre funções do Indy Besu e operações do Hyperledger Indy (descrições resumidas)

Função no Indy Besu	Operação Correspondente no Hyperledger Indy	Descrição
`createDid`	`NYM`	Registra um novo DID com chave pública e metadados.
`updateDid`	`NYM`	Atualiza dados associados a um DID existente.
`createRevocationRegistry`	`REVOC_REG_DEF`	Cria um registro para gerenciar revogação de credenciais.
`createOrUpdateEntry`	`REVOC_REG_ENTRY`	Adiciona ou atualiza o status de revogação de credenciais.
`createSchema`	`SCHEMA`	Define os atributos de um novo esquema de credenciais.
`createCredentialDefinition`	`CRED_DEF`	Define parâmetros para emissão de credenciais com base em um esquema.

O *Hyperledger Indy* é uma plataforma especializada em DIDs, baseada em um *ledger* permissionado com consenso RBFT. Possui dois componentes principais: o *Indy Ledger* (com transações como `NYM`, `SCHEMA`, `CRED_DEF`) e o *Indy SDK*, que permite interações seguras com o *ledger*. Apesar da adoção, o Indy enfrenta limitações de interoperabilidade e evolução de código.

A *Indy Besu* surge como alternativa moderna, migrando a lógica de identidade para contratos inteligentes, preservando a semântica original das transações e reduzindo requisitos computacionais.

A Tabela 2 associa funções do Indy Besu (contratos em Solidity) às operações equivalentes no Indy tradicional (transações no *ledger*), como `createDid` $\leftrightarrow$ `NYM`, e `createSchema` $\leftrightarrow$ `SCHEMA`. Essa equivalência fundamenta a metodologia de avaliação de desempenho entre as abordagens.

A configuração experimental dos ambientes avaliados e os parâmetros de execução utilizados nos testes. Os experimentos foram conduzidos de forma controlada, va-

riando a taxa de envio de transações — definida como o número total de requisições de transações enviadas por segundo por todos os *workers* (req/s) — de 20 até 120 req/s, com incremento de 10 e duração fixa de 10 segundos por rodada.

Todos os artefatos utilizados neste estudo — incluindo códigos-fonte, arquivos de configuração, contratos inteligentes, módulos de carga, logs e resultados experimentais — estão disponíveis publicamente em nosso repositório reprodutível[1].

Para efeito de comparação, avaliamos o desempenho de operações relacionadas à gestão de Identidades Descentralizadas (DID) em dois contextos distintos:

- **Cenário 1 — Hyperledger Indy:** Em [Bastos et al. 2024], foi avaliado uma rede Indy, implantada sobre quatro máquinas virtuais com as seguintes especificações: 4 vCPUs (Intel Xeon E312xx a 2.0 GHz), 4 GB de RAM, rodando Ubuntu 20.04. Esses nós foram configurados como validadores RBFT em uma rede permissionada.
- **Cenário 2 — Hyperledger Besu:** Implantamos uma rede blockchain baseada no Hyperledger Besu em um servidor dedicado com Ubuntu 22.04, 32 GB de RAM e 12 núcleos de CPU. A rede foi configurada com 4 nós validadores utilizando o consenso QBFT e 2 *bootnodes*, seguindo as recomendações da documentação oficial para ambientes de produção.

3.1. Cenários de Teste

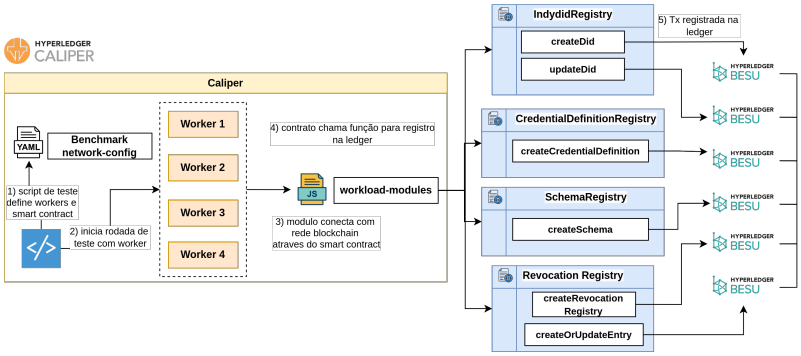

Figura 1. Arquitetura de avaliação de performance dos contratos de identidade na rede Hyperledger Besu com Hyperledger Caliper.

A Figura 1 apresenta a arquitetura utilizada para a execução do cenário de avaliação de desempenho dos contratos inteligentes de identidade digital descentralizada implantados na rede Hyperledger Besu. O processo é conduzido com o auxílio da ferramenta *Hyperledger Caliper*, que permite simular múltiplos clientes (workers) enviando transações para o ledger por meio de chamadas aos contratos Solidity responsáveis pelas funções de identidade.

Cada módulo conecta-se à rede Besu e realiza chamadas a funções dos contratos, de acordo com o tipo de operação avaliada: `createDid` e `updateDid` (*IndydidRegistry*); `createCredentialDefinition` (*CredentialDefinitionRegistry*); `createSchema` (*SchemaRegistry*); `createRevocationRegistry` e `createOrUpdateEntry` (*RevocationRegistry*).

[1] `https://github.com/jeffsonsousa/evaluation-contracts-indy-besu`

4. Resultados

As Figuras 3 e 4 demonstram que a rede Besu superou a Indy nas operações de escrita, alcançando picos de 37,5 TPS para `createDid`, 58 TPS para `createSchema` e 49 TPS para `createCredentialDefinition`, enquanto a Indy atingiu, no máximo, 14, 9 e 8 TPS, respectivamente. Esses resultados representam ganhos de até 600% na vazão com contratos inteligentes. Em ambos os ambientes, as operações de leitura (`getDid`, `getSchema`) mantiveram latência inferior a 5 segundos, com comportamento estável mesmo sob carga elevada, indicando que o principal gargalo está concentrado nas transações de escrita e no consenso.

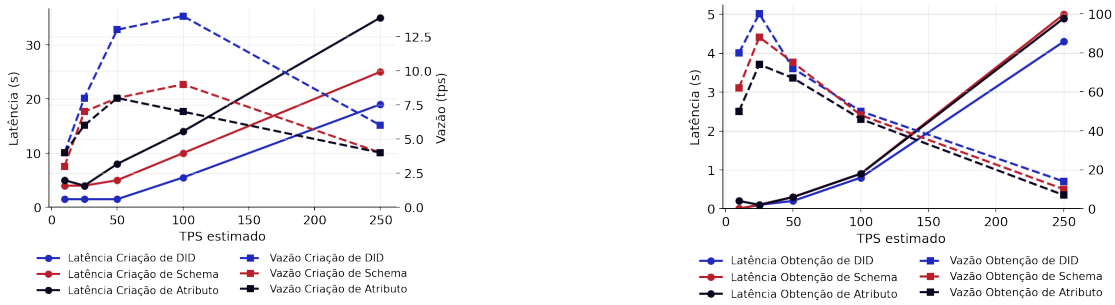

Figura 2. Comparação entre latência e vazão das operações de criação e obtenção Cenário 1. Adaptado de [Bastos et al. 2024].

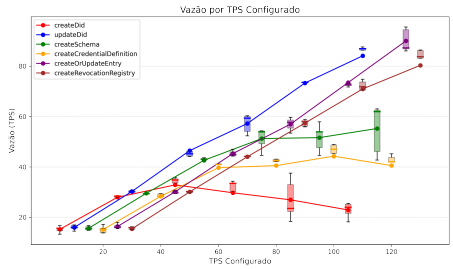

Figura 3. Vazão Cenário 2.

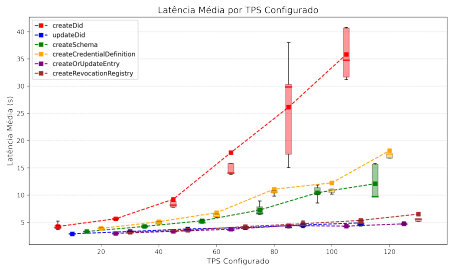

Figura 4. Latência Cenário 2.

A escalabilidade das plataformas foi testada com cargas crescentes de clientes simultâneos. A partir de 50 clientes, observou-se degradação progressiva do desempenho em ambas as redes. Porém, enquanto a Indy teve quedas de até 60% na vazão e picos de latência que quadruplicaram, a Besu manteve uma redução inferior a 30% em vazão e uma elevação de latência mais controlada, inferior a 50%. Esse resultado sugere que a arquitetura baseada em contratos inteligentes da Indy Besu é mais adequada para ambientes com maiores requisitos de escalabilidade horizontal.

Os resultados sugerem que a abordagem baseada no Hyperledger Besu possui vantagens claras em termos de modularidade, desempenho e suporte à escalabilidade. A arquitetura com contratos inteligentes desacopla a lógica de identidade da camada de consenso, permitindo otimizações mais diretas e facilitando a adoção de novos padrões como `did:ethr`.

5. Conclusão e Trabalhos Futuros

Este trabalho apresentou uma análise comparativa entre o Hyperledger Indy, avaliado com o framework MinIndy, e a arquitetura Indy Besu baseada em contratos inteligentes sobre

o Hyperledger Besu, no contexto de operações de identidade descentralizada (DID). A partir da execução de funções-chave do ciclo de vida de identidades e credenciais, os resultados demonstraram que o Indy Besu oferece desempenho superior, com menor latência, maior vazão e uso de recursos mais estável. Além disso, sua arquitetura modular facilita a integração com o ecossistema Ethereum e a adoção de métodos DID compatíveis, destacando-se como uma alternativa escalável e moderna ao modelo tradicional do Indy.

Como trabalhos futuros, propõem-se extensões para avaliar aspectos de segurança e privacidade, como resistência a transações maliciosas e controle de revogação em massa. Também se sugere a exploração de cenários multi-organizacionais com interoperabilidade entre redes permissionadas, além da análise de custo computacional e energético em ambientes de larga escala. Por fim, a simulação de falhas poderá contribuir para entender a resiliência das arquiteturas frente a eventos adversos.

6. Agradecimentos

Os autores agradecem o apoio dado a este trabalho, pelo MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do FUNTTEL e administrados pela FINEP, no âmbito especificamente do projeto TECSEG - Desenvolvimento de tecnologias e metodologia de avaliação e investigação de segurança para redes e aplicações de governo digital, Contrato 01.21.0163.01, Referência 1196/21.

Referências

Bastos, M., Veloso, A., Sousa, J., Evaristo, B., Abreu, D., and Abelém, A. (2024). Minindy: Automating the deployment and management of hyperledger indy networks. In *11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*.

Choi, W. and Won-Ki Hong, J. (2021). Performance evaluation of ethereum private and testnet networks using hyperledger caliper. In *22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*.

Fan, C., Lin, C., Khazaei, H., and Musilek, P. (2022). Performance analysis of hyperledger besu in private blockchain. In *2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 64–73.

Kaushal, R. K. and Kumar, N. (2024). Exploring hyperledger caliper benchmarking tool to measure the performance of blockchain based solutions. In *11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*.

Kshirsagar, A. and Pachghare, V. (2022). Performance evaluation of proof of scope consensus mechanisms on hyperledger. In *IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*.

Melo, C., Gonçalves, G., Silva, A. S., and Soares, A. (2024). Performance modeling and evaluation of hyperledger fabric: An analysis based on transaction flow and endorsement policies. In *IEEE Symposium on Computers and Communications (ISCC)*.

Mostarda, L., Pinna, A., Sestili, D., and Tonelli, R. (2023). Performance analysis of a besu permissioned blockchain. In *Advanced Information Networking and Applications*, pages 279–291.