

MinIndy: Um Framework para Automatizar a Implantação e o Gerenciamento de Redes Blockchain Hyperledger Indy

Alan Veloso¹, Jefferson Sousa^{1,2}, Bruno Evaristo², Diego Abreu¹,
Filipe Saraiva¹, Antônio Abelém¹

¹ Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

² Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

aveloso@ufpa.br, {jcsousa, elderb}@cpqd.com.br, diego.abreu@itec.ufpa.br,
{saraiva, abelem}@ufpa.br

Resumo. A plataforma blockchain Hyperledger Indy, voltada para redes de gestão de identidade, tem ganhado importância, mas a instanciação de uma rede completa em produção é complexa e exige experiência. Para reduzir essa complexidade, este artigo apresenta o MinIndy, um framework projetado para automatizar a instalação, configuração e gerenciamento de redes Indy sem comprometer o desempenho. Portanto, o MinIndy é uma alternativa viável para indivíduos e organizações que buscam adotar redes blockchain Indy com menor intervenção manual. O MinIndy foi avaliado através do desempenho da sua rede e os resultados mostram que a rede construída com o framework não possui perda de desempenho em comparação com uma construída sem.

Abstract. The Hyperledger Indy blockchain platform, aimed at identity management networks, has gained importance, but instantiating a complete network in production is complex and requires experience. To reduce this complexity, this paper presents MinIndy, a framework designed to automate the installation, configuration, and management of Indy networks without sacrificing performance. Therefore, MinIndy is a viable alternative for individuals and organizations looking to adopt Indy blockchain networks with less manual intervention. It was evaluated through the performance of its network and the results show that the network built with the framework has no loss of performance compared to one built without it.

1. Introdução

Blockchain é uma tecnologia com aplicações em várias áreas que buscam tirar proveito de suas propriedades, tais como transparência, segurança e descentralização [Monrat et al. 2019]. Uma solução para redes blockchain focada em identidade descentralizada é a Hyperledger Indy¹ (chamada a partir daqui somente de Indy), mantida e desenvolvida pela Hyperledger Foundation. A rede da Sovrin² é uma das redes permissionadas mais conhecidas baseadas na Indy. Participar de redes como essa pode trazer benefícios para as organizações, como a eliminação de intermediários, a redução de custos e maior segurança e privacidade dos dados dos usuários.

¹<https://www.hyperledger.org/projects/hyperledger-indy>

²<https://sovrin.org/>

Geralmente, para participar de uma rede blockchain baseada na Indy, as organizações precisam instanciar e configurar um nó, essa é uma tarefa demorada e propensa a erros, até mesmo para profissionais com experiência com a tecnologia [Silva et al. 2022]. Para ser realizado de forma precisa e segura, esse processo requer conhecimento e compreensão das etapas de maneira especializada. Entretanto, nem todas as organizações ou pessoas podem alocar o tempo necessário para realizar esse processo, ou não possuem o conhecimento especializado para isso. Assim, isso pode impossibilitar o desenvolvimento das aplicações baseadas nessa tecnologia.

A atualização de uma nova versão da plataforma Indy é demorada. No momento da redação deste artigo, a versão da Indy é compatível com o Ubuntu 20.04, apesar da versão mais recente de suporte de longo prazo disponível ser o Ubuntu 22.04. Embora seja tecnicamente possível realizar os ajustes necessários para que a plataforma Indy opere eficientemente no Ubuntu 22.04, este processo é propenso a erros que podem prolongar significativamente o tempo de implantação e gestão. Adicionalmente, usuários podem não ter experiência suficiente manipulação de sistemas operacionais baseados em Linux têm maior probabilidade de cometer erros. Tais equívocos podem introduzir vulnerabilidades de segurança que afetam a integridade da rede, um aspecto crítico nas redes blockchain.

Outro desafio é a fragmentação das ferramentas necessárias para a implantação e gestão de uma rede Indy. A instalação de uma rede Indy, por exemplo, requer o uso de pelo menos três ferramentas distintas (uma para gerar as chaves criptográficas dos atores iniciais da rede, uma para gerar as chaves criptográficas do nó e iniciá-lo, e outra para gerar os arquivos gênese da rede blockchain) para completar o processo. Além disso, cada uma dessas ferramentas tem seus próprios pré-requisitos de software; embora haja sobreposições dos pré-requisitos, não são os mesmos. Outro processo comum no gerenciamento de redes blockchain é a inclusão de um novo nó na rede, esse processo exige ainda outra ferramenta (responsável por converter a base das informações criptográficas do novo nó) para ser realizado. Essa dispersão de ferramentas aumenta a complexidade de iniciar e manter uma rede Indy, representando um desafio para os operadores da rede.

Portanto, para mitigar os problemas mencionados, é necessário simplificar o processo de instanciação, configuração e gerenciamento dos nós da rede. Assim, assegurando a independência da plataforma Indy em relação ao sistema operacional e provendo as funcionalidades necessárias para implementar e gerenciar uma rede Indy homogênea sem a necessidade de mais de uma ferramenta.

Nesse contexto, este trabalho tem como objetivo simplificar o processo de implantação e gerenciamento de uma rede Indy por meio da automatização com Ansible³ do processo de instanciação e configuração dos nós e da virtualização com Docker⁴ dos componentes necessários. A automatização reduz parcial ou totalmente a necessidade de realizar etapas de configuração, diminuindo o tempo total do processo e o tempo associado a essas etapas. Além disso, evita possíveis erros, desde que os parâmetros da automatização estejam corretamente definidos. Ao mesmo tempo, a virtualização impede que os componentes necessários para as redes Indy dependam do sistema operacional base. No entanto, é fundamental que a rede continue operando de forma eficiente para atender às necessidades dos usuários, ou seja, a automatização e a virtualização não devem preju-

³<https://www.ansible.com/>

⁴<https://www.docker.com/>

dicar significativamente o desempenho da rede ao introduzir restrições. Nesse contexto, a proposta, denominada MinIndy, mantém o mesmo desempenho da rede em comparação com o método recomendado pela Hyperledger Foundation, com base em métricas relevantes para redes blockchain, como latência, taxa de transferência e escalabilidade [Fan et al. 2020].

A proposta apresentada neste artigo estende um trabalho anterior [Veloso et al. 2023], evoluindo o desenvolvimento da proposta (disponível em repositório no GitHub do autor⁵) e avaliando-a em um cenário usando uma ferramenta específica para avaliação de redes Indy, disponibilizada pelo próprio projeto base de redes Indy. Essa avaliação demonstra a viabilidade de utilizar o *framework* para a construção de redes Indy sem perda de desempenho em comparação com uma rede sem o *framework*, torna-o viável para construção das redes em ambiente de produção com menor esforço.

A hipótese validada foi que a automatização e virtualização não prejudicam significativamente o desempenho da rede em condições similares às do método recomendado pela Hyperledger Foundation, denominado aqui como método tradicional, ao executar operações comuns necessárias para aplicações de identidade descentralizada, como, por exemplo, criar Identificadores Descentralizados (*Decentralized identifier* - DID), obter DID, e outros. Para isso, foi realizada uma avaliação experimental de desempenho comparando a rede instanciada pelo MinIndy com uma instanciada pelo método tradicional.

Portanto, o artigo traz a seguinte contribuições:

- Um *framework* específico para a instanciação, configuração e gerenciamento de redes blockchain utilizando a plataforma Indy.
- Disponibilização do *framework* com o código aberto, possibilitando o desenvolvimento conjunto da comunidade, adicionado novas funcionalidades, novos desdobramento e a replicação dos resultados obtidos nesse estudo.
- Realização de uma avaliação de desempenho da rede instanciada com o *framework* e comparada com a avaliação de uma construída com a método tradicional, essa última não foi realizada nem mesmo pela própria Hyperledger Foundation.

O restante do artigo está organizado da seguinte forma: a metodologia utilizada para o desenvolvimento e avaliação é apresentada na Seção 3; a proposta do *framework* é apresentado na Seção 4; a descrição detalhada da configuração de avaliação de desempenho é descrito na Seção 5; os resultados da avaliação são apresentados na Seção 6; e por fim, as conclusões são apresentados na Seção 7.

2. Trabalhos Relacionados

Diversos estudos visam automatizar a implantação de redes blockchain, com propostas tanto na pesquisa acadêmica quanto na indústria. De maneira geral, o foco tem sido nas plataformas permissionadas, principalmente no Hyperledger Fabric [Shi et al. 2019, Zikos et al. 2022, Mathwale 2023].

A prioridade pela plataforma Fabric é proveniente principalmente do grande interesse nela, decorrente da arquitetura modular que ela apresenta. Entretanto, outras plataformas também são de interesse, como a Hyperledger Sawtooth em [Shi et al. 2019] e Hyperledger Indy no Hyperledger Bevel⁶.

⁵<https://github.com/alanveloso/minindy/>

⁶<https://www.hyperledger.org/projects/bevel>

A principal motivação para essas propostas é que os processos de instanciação e gerenciamento das plataformas blockchain, principalmente as permissionadas, são demorados, propensos a erros e dependentes de conhecimento específico da plataforma, umas em maior grau que outras. Um conjunto dessas propostas obtidas no estado da arte, através uma revisão sistemática, e no estado da prática, fornecidos pela própria Hyperledger Foundation e obtidos mediante consulta com especialistas, são apresentados a seguir.

O artigo [Shi et al. 2019] propõe uma *framework* teórica chamado BIRACIAL (*Blockchain-infRAstructure CustomIzation and Auto-profiLing*), que automatiza a implantação de blockchains permissionadas em ambientes virtualizados. Esse *framework* visa otimizar a seleção da plataforma blockchain e dos algoritmos de consenso para aplicações específicas, considerando os requisitos tanto da blockchain quanto da infraestrutura virtual. O método de avaliação envolve a execução de testes que comprovaram a eficácia do BIRACIAL na automatização da implantação de blockchains Hyperledger Sawtooth, bem como no monitoramento e análise de desempenho. Os resultados dos testes de desempenho e implantação auxiliam na escolha das plataformas blockchain e algoritmos de consenso, bem como na configuração eficiente da infraestrutura virtual subjacente.

Em [Tran et al. 2022], o NVAL (*Network Deployment and Evaluation framework*) visa automatizar os processos de implantação e avaliação de redes blockchain, sejam elas permissionadas ou não. Contudo, a proposta trata-se apenas de um documento teórico do *framework*, sem disponibilizar o código-fonte para constatação dos resultados obtidos. Os autores justificam informando que o *framework* pode ser construído utilizando qualquer programa de automatização em conjunto com o NodeJS. A avaliação da proposta é realizada por meio de um estudo de caso, que envolve a implantação e avaliação de diversas arquiteturas de rede blockchain em um ambiente de testes controlado. O estudo incluiu a implantação de 65 redes blockchain com 12 arquiteturas distintas, gerando 295 conjuntos de dados de avaliação.

Nos trabalhos de [Zikos et al. 2022] e [Mathwale 2023], são apresentadas propostas relacionadas à implantação e gerenciamento de redes Hyperledger Fabric. Em [Zikos et al. 2022], a plataforma HFabD+M é introduzida, com uma implementação de prova de conceito e informações sobre o ambiente experimental. No entanto, não são fornecidos detalhes específicos sobre a metodologia de avaliação ou testes. Entretanto, o código do projeto está disponível no GitHub⁷, indicando sua natureza de código aberto para validação dos resultados e possíveis avaliações. Por outro lado, [Mathwale 2023] apresenta o *framework* AHFD (*Automated Hyperledger Fabric Deployment*), que automatiza a implantação e configuração de redes Hyperledger Fabric, destacando a eficiência na redução do tempo de configuração e implantação. Contudo, não são especificados detalhes sobre a metodologia usada para alcançar essas conclusões, nem é mencionada a disponibilidade aberta da solução para validação dos resultados.

Como mencionado anteriormente, também são encontradas propostas no estado da prática com o mesmo objetivo. Os *frameworks* apresentados a seguir possuem um conjunto comum de programas utilizados para o seu desenvolvimento, sendo: Ansible, como a ferramenta de automatização dos processos de instanciação e gerenciamento das plataformas blockchain; Docker e Kubernetes, como as ferramentas de virtualização baseada em *container* e gerenciamento de *containers*, respectivamente; e *scripts* Shell para

⁷<https://github.com/ioanziko/hyperledger>

realizar configurações e processos preliminares. São eles: Hyperledger Bevel⁸, Minifabric⁹ e Microfab¹⁰.

O *framework* Bevel surge como uma opção que visa facilitar o desenvolvimento acelerado de redes blockchain, incluindo a Indy. No entanto, o Bevel requer uma série de softwares como pré-requisitos e um conhecimento aprofundado sobre a operação deles, além da familiaridade com o próprio *framework*, para ser utilizado eficientemente. Existem também outras iniciativas, como o Minifabric e o Microfab, focadas em redes Fabric, apesar de mais simples em comparação com o Bevel, são para a plataforma Fabric exclusivamente. Portanto, a Indy, especializa em identidade descentralizada, ainda carece de iniciativas simples para o processo de instanciação, sob o amparo da Hyperledger Labs¹¹¹².

Em resumo, as propostas existentes atualmente para automatizar a implantação e gerenciamento de redes blockchain de plataformas permissionadas tem como principal foco a plataforma blockchain Fabric, outras plataformas blockchain são contempladas apenas quando as propostas visam ser generalistas, ou seja, não há um trabalho focado na plataforma Indy. Essas propostas ao tentarem englobar várias plataformas blockchain tão distintas entre si no processo de implantação e gerenciamento podem torná-las complexas e exigirem conhecimento específico para manipulá-las. Portanto, do nosso ponto de vista, propostas focadas em uma única plataforma é a melhor alternativa para simplificar a implantação e gerenciamento da plataforma blockchain, sendo esse o caso do MinIndy proposto nesse artigo. Além disso, *frameworks* de propósito geral são mais adequados quando há a necessidade de manipulação de diversas plataformas blockchain, quando há a necessidade de apenas uma plataforma, o tempo e o conhecimento adquirido na manipulação de um *framework* mais complexo pode ser em vão.

Alguns dos trabalhos apresentados nesta seção serviram de base para o desenvolvimento da proposta apresentada neste trabalho. Principalmente em relação às ferramentas utilizadas para o desenvolvimento dos *frameworks* para estar alinhado tanto com o estado da arte quanto com o estado da prática. O processo de desenvolvimento é detalhado na Seção 3 a seguir.

3. Metodologia

A metodologia utilizada neste trabalho foi dividida em três partes: (i) definição dos principais processos para a instalação e a configuração de uma rede blockchain Indy; (ii) desenvolvimento do *framework* para automatizar esses processos; e (iii) comparação experimental do desempenho de uma rede instanciada com MinIndy com uma instanciada segundo as indicações da Hyperledger Foundation.

Para (i) definir os principais processos para a instalação e configuração de uma rede blockchain Indy, foram coletadas e sumarizadas as informações contidas na documentação oficial da Hyperledger Foundation. Essa abordagem garante que os processos identificados sejam baseados nas melhores práticas e orientações estabelecidas pela comunidade de desenvolvimento da Indy.

⁸<https://www.hyperledger.org/projects/bevel>

⁹<https://labs.hyperledger.org/labs/minifabric.html>

¹⁰<https://labs.hyperledger.org/labs/microfab.html>

¹¹Organização responsável pela curadoria de projetos relacionados às soluções Hyperledger

¹²<https://labs.hyperledger.org>

Na etapa (ii), inclui o processo de seleção das ferramentas utilizadas para o desenvolvimento do *framework*. Para isso, foram analisadas outros *frameworks* com funções similares tanto as que englobavam a Indy quanto as que eram direcionadas para outras plataformas Hyperledger, esse levantamento foi apresentado na Seção 2. Entretanto, grande parte dos trabalhos encontrados na literatura não tinha o código aberto, portanto, o aproveitamento do que foi desenvolvido nessas propostas foram restritas a arquitetura, funções, ferramentas e outras informações teóricas. Desse modo, a principal fonte de informação para o desenvolvimento foram as propostas disponibilizadas pela Hyperledger Foundation através da Hyperledger Labs¹³, ela fornece uma lista dos projetos curados pela Hyperledger.

Ainda na etapa (ii), após a definição das ferramentas utilizadas no desenvolvimento, foram desenvolvidos os *scripts* que automatizassem os processos de instanciação, configuração e gerenciamento de redes Indy. Esses *scripts* automatizam a instalação e a configuração dos principais passos para instanciar um nó Indy, possibilitando adequar diversos aspectos relacionados ao funcionamento e segurança da rede. Além de automatizar processos importantes para o gerenciamento de redes, como a interrupção de um nó e início desse nó com as informações do registro distribuídos já existentes. Além de utilizar uma ferramenta de virtualização para evitar a dependência dos componentes da rede Indy do sistema operacional base. Os resultados são apresentados em detalhes mais a frente na Seção 4.

Para (iii) comparar o desempenho de uma rede instanciada com o MinIndy com uma instanciada conforme as recomendações da Hyperledger Foundation, uma estratégia específica para esse fim fornecida pela própria Hyperledger Foundation¹⁴ foi utilizada. A avaliação foi realizada utilizando uma topologia de rede semelhante àquela usada em uma publicação [Kelsey 2023] da própria Hyperledger Foundation para avaliação da solução Hyperledger Fabric 2.5, adaptada para as redes Indy e considerando os recursos computacionais disponíveis.

Diferentemente da rede Fabric, a rede Indy necessita de pelo menos quatro nós completos (Node1, Node2, Node3 e Node4) para entrar em produção, como é possível ver na Figura 1. Além disso, ao contrário do que ocorre na Fabric, na Indy não há um ordenador, sendo o processo realizado pelo protocolo de consenso Plenum, presente em todos os pares. O *Registro Distribuído* é responsável por armazenar e propagar informações sobre identidades, credenciais e outros objetos de domínio.

A ferramenta *Processes Based Load Script* [Hyperledger Foundation 2018], fornecida pela Hyperledger Foundation, foi utilizada para gerar as cargas. Para gerar carga de trabalho na rede foram simulados diferentes números de clientes e diferentes volumes de transações para cada cliente. As demais descrições do processo de avaliação podem ser vistas Seção 5. O resultado da metodologia descrita nesta seção é a proposta MinIndy descrita em mais detalhes na seção seguinte (Seção 4).

4. MinIndy

Esta seção descreve o MinIndy, a arquitetura da solução, bem como as ferramentas utilizadas no desenvolvimento, e outras informações importantes do seu desenvolvimento.

¹³<https://labs.hyperledger.org/>

¹⁴<https://github.com/hyperledger/indy-node/tree/main/scripts/performance>

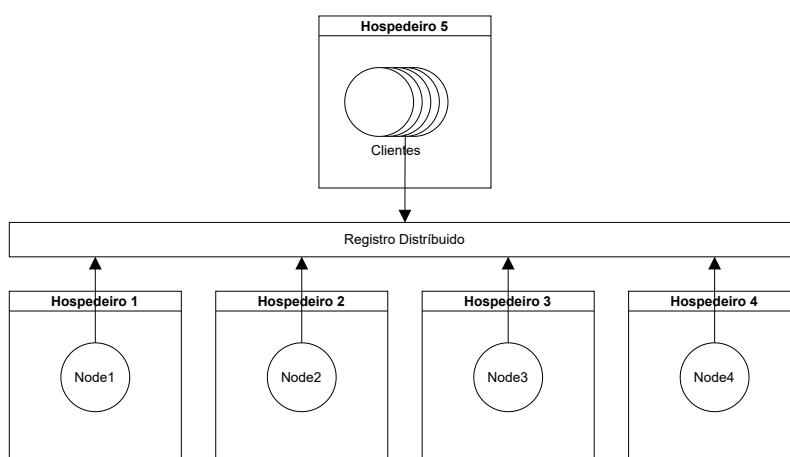


Figura 1. Visão geral da topologia de avaliação de desempenho.

Serão apresentados uma visão geral de uma rede Indy, com os integrantes, componentes e os processos identificados como os principais para a implantação e gerenciamento de uma rede Indy com base na documentação do Indy [Hyperledger Foundation 2022]. Esses processos serão automatizados pelo MinIndy. Também serão apresentadas as configurações padrão utilizadas para automatização.

Os integrantes das redes Indy podem ter dois papéis, *Trustee* e *Steward*: os *Trustees* são as pessoas responsáveis por gerenciar a rede e proteger a integridade da governança da rede. Em uma rede de produção, é necessário ter, no mínimo, três *Trustees*, ou seja, três pessoas diferentes são obrigatórias, mas é desejável ter mais; um *Steward* é uma organização responsável por manter um nó da rede. Inicialmente, quatro *Stewards* são fundamentais para estabelecer uma nova rede, ou seja, são necessárias quatro organizações diferentes. Mais *Stewards* podem ser adicionados posteriormente.

Os *Stewards* operam os nós validadores (*Validator*) da rede. O *Validator* é o principal componente que forma uma rede Indy, é a máquina que se tornará parte de uma rede Indy. Um *Validator* permitirá que a organização faça parte do que é chamado de consenso. Por padrão, um *Steward* só tem permissão para operar um *Validator* por rede.

Os dois processos identificados como os principais para a instanciação de uma rede Indy são: a criação de uma rede e a adição de um novo nó. Esses processos são descritos de maneira geral a seguir:

- Criação de uma Rede: A etapa de criação de uma rede Indy envolve a criação de informações de identificação criptográficas dos *Trustees* e *Stewards*. Além disso, os *Stewards* também devem definir e criar informações de rede e criptográficas dos seus *Validators* como, endereço IP, chave pública BLS (Boneh–Lynn–Shacham) e outros. Essas informações são utilizadas para definir os administradores e os nós confiáveis iniciais, respectivamente. Após todas as informações e outras informações gerais da rede terem sido definidas e compartilhadas entre os *Validators*, é possível inicializar a rede.
- Adição de um Novo Nó: Para adicionar um novo nó é necessário que um administrador da rede, ou seja, um *Trustee*, adicione um novo *Steward*, para que este tenha a permissão de adicionar um *Validator*. Após o *Steward* ter definido as informações de rede e de identificação necessários, usará os arquivos de configuração da

rede para iniciar o seu *Validator*. Por fim, o *Steward* adicionará o seu nó à rede.

A instanciação de uma rede Indy possibilita a personalização de algumas configurações. Para esta proposta, serão utilizadas as configurações padrão da rede Sovrin, sendo amplamente aceitas entre as iniciativas que utilizam a tecnologia Indy. Além disso, é a rede cujo desenvolvimento conta com o maior número de organizações contribuintes, tornando as configurações utilizadas mais atraentes para a maioria dos interessados. Assim, ao automatizar as configurações dessa rede, possibilita que outras organizações façam parte da rede Sovrin e também construam suas próprias redes baseadas nessas configurações.

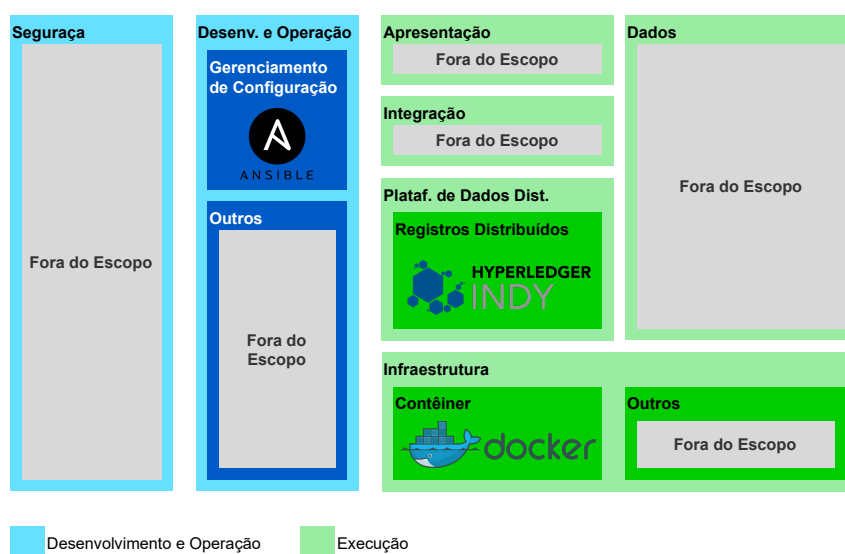


Figura 2. Arquitetura do MinIndy.

A arquitetura de referência [Hyperledger Foundation 2019], fornecida pela Hyperledger Foundation, serviu de base para o desenvolvimento da arquitetura do MinIndy apresentada na Figura 2. O MinIndy abarca os níveis de desenvolvimento e operação, plataformas de dados distribuídos e infraestrutura. Os demais níveis estão fora do escopo, por já serem tratados por aplicações de escolha do usuário ou por adicionarem complexidade não essenciais à solução.

Os recursos de *desenvolvimento e operação* permitem desenvolver serviços dentro ou fora do registro distribuído e baseados em SDKs e IDEs (por exemplo, APIs da Web). Também pode se tratar da manutenção, do monitoramento e da administração do registro distribuído e seus serviços. O MinIndy atua especificamente no gerenciamento de configuração, que envolve a automação de *scripts* e permite que os operadores configurem redes blockchain similarmente, usando alterações mínimas de configuração. O MinIndy utiliza o Ansible, uma ferramenta de automação de TI que simplifica tarefas de gerenciamento de infraestrutura, como a configuração de nós da rede blockchain, permitindo que os operadores configurem redes blockchain semelhantemente, com mudanças mínimas de configuração. Por exemplo, o Ansible permite automatizar a criação de nós da rede com configurações específicas, economizando tempo e reduzindo erros.

A *plataforma de dados distribuídos* forma o núcleo da solução. O MinIndy dá suporte à blockchain Hyperledger Indy. No nível de *infraestrutura*, estão as funcionalidades

dades necessárias para executar ou implantar os diferentes serviços de uma arquitetura blockchain. Os recursos de *container* permitem que os usuários implantem e gerenciem a rede Indy usando virtualização baseada em containers. Eles também permitem que um desenvolvedor empacote e envie um aplicativo com todas as partes necessárias, como bibliotecas e outras dependências. Optou-se pelo Docker, garantindo um ambiente uniforme e consistente de execução e possibilita a instalação e a execução em ambientes compatíveis com o Docker, independentemente do sistema operacional ou da plataforma de nuvem.

5. Avaliação

Esta seção descreve a avaliação realizada e a ferramenta utilizada, as configurações e o ecossistema.

5.1. Configuração da Ferramenta de Avaliação de Desempenho

A ferramenta *Processes Based Load Script* [Hyperledger Foundation 2018] é disponibilizada no projeto Indy Node e foi utilizada por funcionar com redes Indy, diferente da ferramenta Caliper¹⁵, que apesar de utilizada para avaliação de desempenho de redes blockchain, ainda não possui suporte para Indy. A principal vantagem de utilizar essa ferramenta é a de ser possível representar diferente número de clientes que podem injetar cargas de trabalho na rede de diferente tipos de transações.

As configurações a seguir foram definidas e configuradas na ferramenta, onde é possível variar o número de clientes, número de transações por lote, número de lotes por segundo, tipo de transações e o tempo de duração.

- **Número de clientes:** define o número de processos independentes a serem executados. Cada processo usará seu próprio identificador e carteira, e enviará o número solicitado de transações especificados;
- **Número de transações por lote:** define o número de transações em um lote;
- **Número de lotes por segundo:** define a taxa de envio de lote em por segundo.;
- **Tipo de transações:** especifica o tipo de requisição que pode ser feita para a rede. Há suporte a diferente comumente usado por aplicações de identidade, como: *criar de DID*, *obter de DID*, *criar de esquema*, *obter de esquema*, *criar de atributos*, *obter de atributos* e outras;
- **Tempo de duração:** define o tempo de duração do envio de transações.

Neste estudo, o impacto do número, taxas e tipos de transações no desempenho do blockchain é de interesse, pois essas informações possibilitam analisar o comportamento da rede e comparar as redes em diferente situações para verificar se há alguma variação nos diferentes casos. Portanto, estes são parâmetros a serem variados no experimento, enquanto a configuração da rede permanece fixa durante todo o experimento.

5.2. Ambiente de Teste

Uma máquina virtual com 16 vCPUS, processadores Intel Xeon E312xx de 2.0 GHz, 8 GB de RAM com Ubuntu 20.04 foi usada para executar a ferramenta de teste. Outras 4 máquinas virtuais com 4 vCPUS, processadores Intel Xeon E312xx de 2.0 GHz, 4 GB

¹⁵<https://www.hyperledger.org/projects/caliper>

de RAM com Ubuntu 20.04 para serem os nós da rede Indy. Este ambiente de teste foi para compreender o desempenho das redes sem e com o MinIndy, ou seja, não é necessário considerar aspectos de hardware, por tratar-se uma comparação direta de ambas em condições iguais.

5.3. Descrição dos Casos de Teste

Para conduzir o teste de desempenho, alguns casos de teste foram definidos variando as especificações de parâmetros. O desempenho resultante da plataforma blockchain foi então registrado e analisado, em relação a três métricas de desempenho comumente utilizado em avaliação de redes blockchain [Kuzlu et al. 2019, Melo et al. 2022]: taxa de transferência, transações bem-sucedidas por segundo; latência, tempo de resposta por transação; escalabilidade, a capacidade de suportar um número crescente de participantes.

A latência é o intervalo entre o envio da transação pelo cliente (*Tempo de Envio*) e sua gravação no livro razão (*Tempo de Confirmação*). Isso pode ser expresso pela Equação 1:

$$\text{Latência} = \text{Tempo de Confirmação} - \text{Tempo de Envio} \quad (1)$$

A taxa de transferência de transações se refere ao número de transações (*Total de Transações Válidas*) que a blockchain pode processar e gravar seu resultado no livro razão distribuído em um determinado tempo (*Tempo Total*). Equação 2:

$$\text{Taxa de Transferência} = \frac{\text{Total de Transações Válidas}}{\text{Tempo Total}} \quad (2)$$

Para a avaliação do desempenho, foram adotados parâmetros específicos: cada lote contém 10 transações e são processados 10 lotes por segundo, resultando em uma taxa de 100 transações por segundo. O número de clientes foi variado em 10, 25, 50, 100 e 250. Ao utilizar diferentes quantidades de clientes simultaneamente, conseqüentemente aumenta-se o número de transações por segundo. Os tipos de transações consideradas foram: criação de DID, obtenção de DID, criação de esquema, obtenção de esquema, criação de atributo e obtenção de atributo. Esses tipos foram selecionadas por serem frequentemente utilizadas por aplicações. A duração do envio contínuo de transações para cada tipo foi estabelecido em 600 segundos (10 minutos). Cada configuração de cliente foi repetida em 10 experimentos distintos, totalizando 50 horas de avaliação de desempenho para cada rede¹⁶. Ressalta-se que não houve pré-geração de transações antes do início dos testes; assim, as transações são geradas em tempo real durante os testes, proporcionando uma representação autêntica do comportamento da blockchain ao processar transações em tempo real. Além disso, a rede não possui transações pré-existentes antes dos testes, ou seja, a rede estava vazia, e cada uma das cargas de transações seguiram sequencialmente e sem reiniciar a rede na seguinte ordem: criação de DID, obtenção de DID, criação de esquema, obtenção de esquema, criação de atributo e obtenção de atributo.

6. Resultados

Os resultados obtidos pela ferramenta de avaliação de desempenho foram interpretados para analisar as redes criadas com o método tradicional (em azul) e MinIndy (em vermelho) Figura 3. Todos os gráficos mostram a média de Taxa de Transferência (eixo

¹⁶Excluindo-se o tempo de inicialização necessário pela ferramenta para preparar os clientes, que varia de segundos a minutos.

das ordenadas à direita) em Transações por Segundo (tps), representado pelas linhas com marcadores triangulares, e Latência (eixo das ordenadas à esquerda) em segundos (s), representando pelas linhas com marcadores quadrados, em diferente número de clientes, variando em 10, 25, 50, 100, e 250.

É possível perceber pelos gráficos que o processo de criação de qualquer que seja a informação (DID, Esquema ou Atributo) demora mais tempo do que processo de obtenção de informação. No caso da criação, os valores de latência variam aproximadamente de 0 até 35 segundos, enquanto na obtenção deles variam de próximo de 0 até 5 segundos. As transações de criação envolvem mais processos para serem concluídas (como o consenso da informação da rede) do que a obtenção da informação, sendo apenas consulta, logo a diferença é justificável. Esse melhor desempenho também é refletido na taxa de transferência que a obtenção tem valores variando entre 10 e 250 tps, enquanto a criação varia de 2 a 14 tps. Também é importante notar que exceto pela criação de DID, que possui a taxa de transferência mais elevada em comparação com as demais, o grupo dos gráficos de transações de criação (Esquema e Atributo) possuem valores similares, o mesmo vale para o grupo dos gráficos de obtenção. Portanto, é possível concluir que independente do tipo de informação, transações de criação e obtenção vão ter comportamento similares.

A maior taxa de transferência para criação, de qualquer que seja a informação, é de próximo de 14 tps alcançada pela criação de DID na rede construída com o MinIndy (Figura 3(a)). Enquanto a maior latência para criação é obtido pela rede construído com a metodologia tradicional ao realizar a criação de atributo (Figura 3(e)), ficando próximo de 35 segundos. Os menores valores para latência e taxa de transferência são próximo de 0 na obtenção de qualquer informação (Figuras 3(b), 3(d) e 3(f)) e próximo de 2 na criação de atributo (Figura 3(e)).

Nos gráficos tanto para criação quanto para obtenção, de qualquer que seja a informação, a latência segue o mesmo padrão de evolução, apresentando pouca diferença de uma rede para outra. Sendo praticamente o mesmo padrão de evolução no caso da Figura 3(b).

Neste estudo, o número total de clientes suportado foi escolhido como o parâmetro de medição de escalabilidade. Diante disso, como é possível acompanhar nos gráficos, para as configurações de hardware selecionados, a rede escala até 50 clientes, após isso, há uma estabilização e/ou queda (ou aumento dependendo da métrica). Contudo, a partir de 250 clientes, a máquina responsável por simular os clientes não os simulou de maneira eficiente por limitações de recursos computacionais, principalmente tempo de computação, impactando na avaliação. É importante observar que nenhuma das transações foi negada, ou seja, todas as transações enviadas para ambas as redes foram confirmadas, ou seja, não foi possível alcançar o limite da rede.

No geral, é possível verificar a partir dos gráficos uma alternância entre as redes com melhor desempenho, às vezes a rede construída com o MinIndy tem melhor desempenho, ou seja, menor latência e maior taxa de transferência, e o contrário também é verdade. Isso implica que o MinIndy não inclui carga computacional que possa prejudicar excessivamente o desempenho da rede Indy para os tipos de transação avaliados, tornando o desempenho da rede construída com a ferramenta similar à da rede que utiliza a metodologia tradicional.

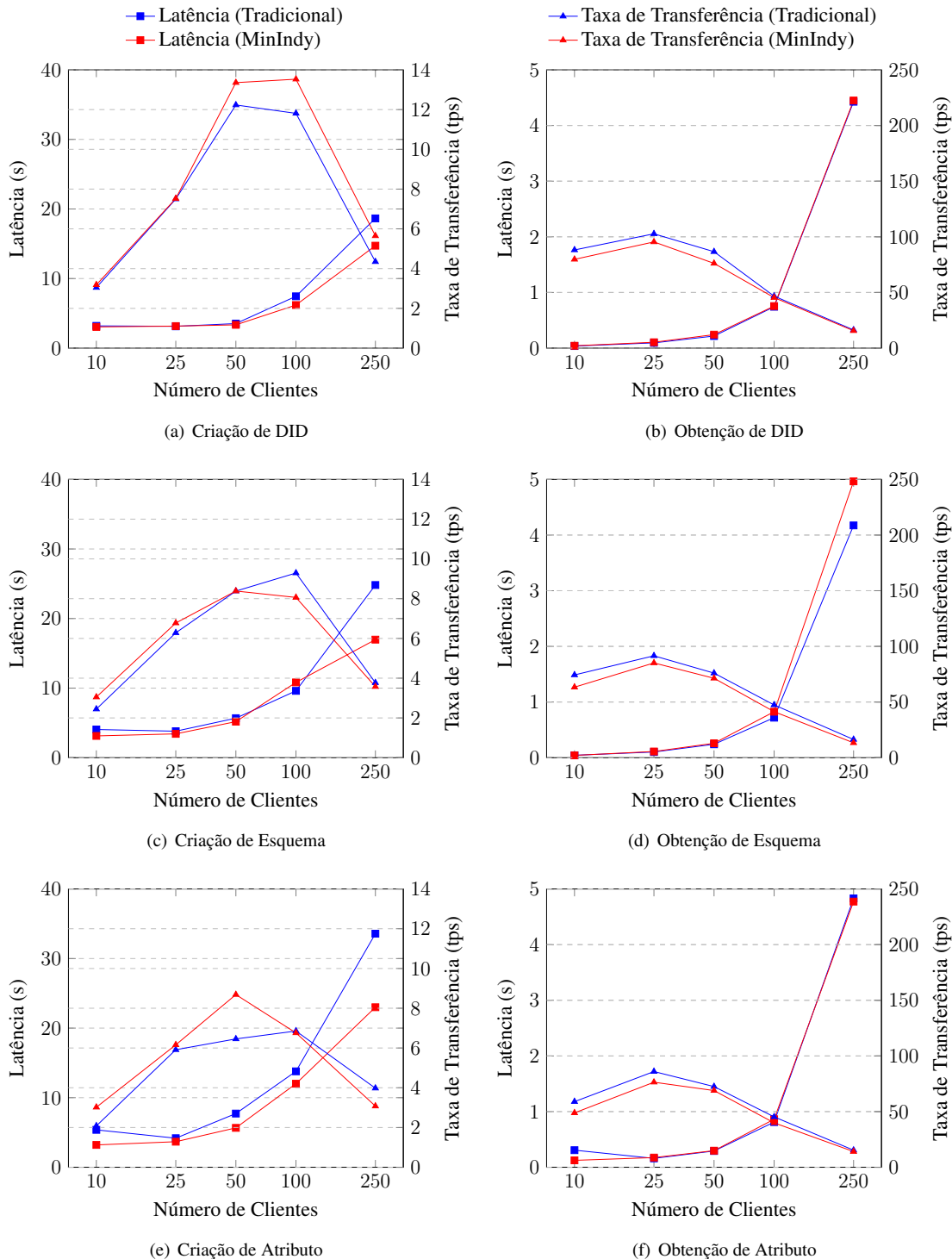


Figura 3. Comparação de Latência e Taxa de Transferência com o Número de Clientes.

7. Conclusão e Trabalhos Futuros

Este artigo apresentou o MinIndy, um *framework* que simplifica o processo de implantação, configuração e gerenciamento de uma rede Indy. Para isso, foi utilizada a automação de processos de configuração e virtualização dos componentes utilizados para constituir uma rede Indy. A adoção dessa estratégia evita processos manuais necessários

utilizando o método tradicional. O objetivo deste projeto foi alcançado ao desenvolver um *framework* que simplifica o processo de criação de nós (por consequência, a criação de redes Indy) configuração e gerenciamento de modo a não causar prejuízo ao desempenho da rede.

O *framework* MinIndy é útil, tanto para o desenvolvimento quanto para a pesquisa. Para o desenvolvimento, a automatização dos processos de instanciação reduz o esforço necessário para a criação de uma rede ou nó Indy, permitindo que outros indivíduos ou organizações participem da rede, mesmo sem ter o conhecimento ou a disponibilidade para adquiri-los. Para a pesquisa, a ferramenta fornecerá uma alternativa para os pesquisadores realizarem estudos relacionados ao Indy ou suas aplicações sem precisar configurar uma rede Indy, ou ter acesso a uma rede já existente.

Decorrente de algumas limitações de recursos computacionais disponíveis, não foi possível escalar a avaliação de desempenho, como, por exemplo, com um número maior de clientes ou mais repetições. Assim, não foi possível alcançar o limite próprio da rede Indy, ou seja, nos casos em que houvesse negação de transações. Apesar da avaliação realizada no trabalho ser suficiente para validar o *framework*, escalar a avaliação traria mais robustez aos resultados. Além disso, não foi possível testar todos os tipos de transações utilizadas em aplicações de identidade. Apesar da tendência observada pelos resultados pelos outros tipos de transações, seria possivelmente refletida nos demais tipos, pode ser necessário comprová-las de maneira observável.

Outros possíveis trabalhos futuros poderiam ser a avaliação do consumo de recursos consumido por ambos os métodos de instanciação de redes Indy, avaliando se o MinIndy está consumindo mais recursos do que o método de instalação tradicional. Outro possível trabalho é a avaliação de usabilidade, pois dessa forma seria possível ter uma avaliação quantitativa da melhora da usabilidade que o MinIndy traz para o gerenciamento de redes Indy. Além disso, é possível incluir na ferramenta outras funcionalidades que podem ser úteis para os processos relacionados ao ciclo de vida das redes ou nós Indy.

Agradecimentos

Este trabalho foi realizado com o apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), da Rede Nacional de Ensino e Pesquisa (RNP) e da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), por intermédio do projetos No. 2023/00811-0, No. 2020/04031-1, No. 2021/00199-8, e projeto No. 2018/23097-3.

Referências

- Fan, C., Ghaemi, S., Khazaei, H., and Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, 8:126927–126950.
- Hyperledger Foundation (2018). Processes Based Load Script. <https://github.com/hyperledger/indy-node/tree/main/scripts/performance>. Acessado em: 31 out 2023.
- Hyperledger Foundation (2019). Architecture reference. <https://blockchain-automation-framework.readthedocs.io/en/latest/architectureref.html>. Acessado em: 26 fev 2023.

- Hyperledger Foundation (2022). Setting up a new network. <https://github.com/hyperledger/indy-node/blob/ubuntu-16.04/docs/source/NewNetwork/NewNetwork.md>. Acessado em: 14 mar 2023.
- Kelsey, D. (2023). Benchmarking hyperledger fabric 2.5 performance. <https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance>. Acessado em: 14 mar 2023.
- Kuzlu, M., Pipattanasomporn, M., Gurses, L., and Rahman, S. (2019). Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 536–540, Atlanta, GA, USA. IEEE.
- Mathwale, R. (2023). AHFD: A Framework for Deployment and Management of Hyperledger Fabric Enterprise Blockchain. In *2023 International Conference on Data Science and Network Security (ICDSNS)*, pages 1–4, Tiptur, India. IEEE.
- Melo, C., Oliveira, F., Dantas, J., Araujo, J., Pereira, P., Maciel, R., and Maciel, P. (2022). Performance and availability evaluation of the blockchain platform hyperledger fabric. *The Journal of Supercomputing*, 78(10):12505–12527.
- Monrat, A. A., Schelén, O., and Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151.
- Shi, Z., Zhou, H., Surbiryala, J., Hu, Y., De Laat, C., and Zhao, Z. (2019). An Automated Customization and Performance Profiling Framework for Permissioned Blockchains in a Virtualized Environment. In *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 404–410, Sydney, Australia. IEEE.
- Silva, M., Veloso, A., and Abelém, A. (2022). Relatos de experiências do processo de implantação do testbed de aplicações blockchain brasileiro. In *Anais do I Workshop de Testbeds*, pages 1–11. SBC.
- Tran, N. K., Babar, M. A., and Walters, A. (2022). A Framework for Automating Deployment and Evaluation of Blockchain Network. *Journal of Network and Computer Applications*, 206:103460. arXiv:2203.10647 [cs].
- Veloso, A., Sousa, J., Evaristo, B., and Abelém, A. (2023). Minindy: Uma ferramenta de início rápido do hyperledger indy. In *Anais Estendidos do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 85–88, Porto Alegre, RS, Brasil. SBC.
- Zikos, I., Sendros, A., Drosatos, G., and Efraimidis, P. S. (2022). HFabD+M: A Web-based Platform for Automated Hyperledger Fabric Deployment and Management. In *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, pages 1–6, Irvine, CA, USA. IEEE.