Pedro Hércules de Sousa Dantas
Orientador: Glauber Dias Gonçalves

Análise de Custo e Desempenho de Aplicações Baseadas na Tecnologia *Blockchain*

Picos - PI
03 de março de 2023

Pedro Hércules de Sousa Dantas
Orientador: Glauber Dias Gonçalves

Análise de Custo e Desempenho de Aplicações Baseadas na Tecnologia *Blockchain*

Trabalho de conclusão do curso submetido para Universidade Federal do Piauí para conclur o curso de Bacharel em Sistemas de Informação.

Universidade Federal do Piauí
Campus Senador Helvídio Nunes de Barros
Bacharelado em Sistemas de Informação

Picos - PI
03 de março de 2023

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca José Albano de Macêdo

D192a Dantas, Pedro Hércules de Sousa

Análise de custo e desempenho de aplicações baseadas na tecnologia *Blockchain* [recurso eletrônico] / Pedro Hércules de Sousa Dantas – 2023.
62 f.

1 Arquivo em PDF
Indexado no catálogo *online* da biblioteca José Albano de Macêdo-CSHNB
Aberto a pesquisadores, com restrições da Biblioteca

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal do Piauí, Bacharelado em Sistemas de Informação, Picos, 2023.
"Orientador: Dr. Glauber Dias Gonçalves"

1. *Blockchain*. 2. Segurança dos dados. 3. Análise de custo. 4. Ethereum. I. Gonçalves, Glauber Dias. II. Título.

CDD 005.3

Emanuele Alves Araújo CRB 3/1290

ANÁLISE DE CUSTO E DESEMPENHO DE APLICAÇÕES BASEADAS NA TECNOLOGIA BLOCKCHAIN

PEDRO HÉRCULES DE SOUSA DANTAS

Monografia apresentada como exigência parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data de Aprovação

Picos – PI, 20 de março de 2023

Glauber Dias Gonçalves

Prof. Glauber Dias Gonçalves

Francisco Airton P. da Silva

Prof. Francisco Airton Pereira da Silva

Prof. Fredison Muniz de Sousa

Agradecimentos

Agradeço a todos que contribuíram nesta jornada que decidi percorrer, especialmente a Deus e à minha família, que sempre estiveram presentes em todos os momentos e sempre me apoiaram nos estudos e nas minhas escolhas. Gostaria de agradecer também ao meu orientador, o Professor Dr. Glauber Dias Gonçalves, que sempre me orientou muito bem e teve um papel fundamental na elaboração deste trabalho. Além disso, agradeço aos meus colegas pelo companheirismo e disponibilidade para estudar e aprender juntos.

Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito.
Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes.
Marthin Luther King

Resumo

Blockchain é uma tecnologia disruptiva que oferece recursos que aumentam a segurança dos dados, possibilitando o registro seguro e descentralizado de dados ou transações entre entidades (pessoas e/ou organizações) que não precisam ter confiança mútua. Existe um crescente interesse por aplicações dessa tecnologia em diversas áreas, mas o seu uso requer a escolha de uma rede pública ou permissionada. O tipo de rede vai impactar nas qualidades não funcionais, principalmente no custo e desempenho. Neste trabalho é proposta uma metodologia para estimar o custo da infraestrutura por transações confirmadas na *blockchain*, considerando redes públicas e permissionadas. Para isso, analisamos a relação entre o custo monetário do recurso computacional necessário para executar uma aplicação *blockchain* e a vazão máxima obtida por esse recurso em transações por segundo. Os resultados desse trabalho mostram os limites de escalabilidade desses tipos de rede e o compromisso destas redes entre custo e desempenho em aplicações baseadas em *blockchain*.

Palavras-chaves: blockchain. hyperledger fabric. ethereum.

Abstract

Blockchain is a disruptive technology that offers features that increase data security, allowing the secure and decentralized recording of data or transactions between entities (people and/or organizations) that do not need to have mutual trust. There is a growing interest in the applications of this technology in different areas, but its use requires the choice of a public or licensed network. The type of network will impact non-functional qualities, primarily cost and performance. In this work, a method is proposed to estimate the infrastructure cost per confirmed transactions on *blockchain*, considering public and permissioned networks. For this, we analyze the relationship between the monetary cost of the computational resource needed to run a *blockchain* application and the maximum throughput obtained by this resource in transactions per second. The results of this work show the scalability limits of these types of networks, and the compromise of these networks between cost and performance in blockchain-based applications.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

tps	Transações por segundo
PoW	Algoritmo de consenso *Proof of Work* (Prova de trabalho)
PoS	Algoritmo de consenso *Proof of Stake* (Prova de participação)
EVM	*Ethereum Virtual Machine* (Máquina Virtual Ethereum)
dApps	Aplicativos descentralizados
NFT	*Non-fungible Token* (Token não fungível)
BFT	Algoritmo de consenso tolerante a falhas bizantinas
EMR	Registro médico eletrônico
EC2	*Amazon Elastic Compute Cloud* (Serviço da Amazon para computação em nuvem elástica)

Lista de símbolos

$\in$	Símbolo que indica pertencimento a um conjunto.
$=$	Símbolo de igual.
$\leq$	Símbolo para menor ou igual.
$\mid$	Símbolo que representa "tal que".

Sumário

1 Introdução

Blockchain é uma tecnologia disruptiva com impactos nas relações entre pessoas, consumo e produção de bens e serviços (XU; WEBER; STAPLES, 2019). Essa tecnologia possibilita o registro seguro e descentralizado de dados ou transações entre entidades (pessoas e/ou organizações) que podem não se conhecer, e assim não terem confiança mútua. Logo, os dados e transações entre essas entidades são registrados de forma imutável, com acesso público ou privado para fins de verificação de autenticidade e derivação de novas transações. Isso se tornou possível a partir da evolução e unificação de outras tecnologias, em especial, criptografia assimétrica e protocolos de consenso distribuídos via comunicação par a par, que são a essência de *blockchains* (GREVE et al., 2018).

Existe um crescente interesse por novas aplicações dessa tecnologia no meio corporativo e nos serviços públicos, além das já conhecidas aplicações para cripto ativos Bitcoin e Ethereum (NAKAMOTO, 2008; BUTERIN et al., 2014). Os recursos da tecnologia *blockchain* como os contratos inteligentes estendem o seu uso em diferentes domínios de aplicações corporativas. Contudo, essa tecnologia encontra-se ainda em fase de amadurecimento e necessita de ferramentas para gerenciamento de custos e recursos computacionais (i.e., infraestrutura) que permitirão a sua adoção por organizações nos setores da indústria, serviços e governos. Atualmente os modelos de infraestrutura mais adotados para a tecnologia *blockchain* são as redes públicas e as redes permissionadas, sendo que o desempenho e o custo associados são questões essenciais para a definição de qual modelo *blockchain* utilizar.

Nesse contexto, métodos que permitam analisar benefícios e custos das infraestruturas computacionais necessárias para implantação e o funcionamento de uma rede *blockchain* são essenciais para orientar o corpo técnico e executivo das organizações a planejarem uma possível adoção da tecnologia *blockchain*. Esses atores necessitam avaliar as opções de rede pública ou privada e o problema em questão é entender o impacto desses dois modelos no consumo de recursos computacionais e por conseguinte identificar a infraestrutura com melhor compromisso entre desempenho e custo para a aplicação *blockchain*.

A maioria das propostas de literatura que lidam com essa questão focam na aplicação para a rede pública (LEAL; CHIS; GONZÁLEZ-VÉLEZ, 2020; ROUHANI; DETERS, 2017; ZHANG et al., 2020) ou rede permissionada (BALIGA et al., 2018; THAKKAR; NATHAN; VISWANATHAN, 2018; WANG; CHU, 2020; XU et al., 2021). Poucos trabalhos ainda focam na análise de uma aplicação típica para ambas as redes (MONRAT; SCHELÉN; ANDERSSON, 2020; MALIK et al., 2019). Contudo, nenhuma dessas propostas buscam identificar a infraestrutura que leva ao melhor desempenho, considerando simultaneamente o fator custo para redes públicas e permissionadas.

Neste trabalho descrevemos um método para estimar o custo da infraestrutura por

transação confirmada na *blockchain*, considerando redes públicas e permissionadas. Para isso, analisamos a relação entre o custo monetário do recurso computacional necessário para executar uma aplicação *blockchain* típica e a vazão máxima obtida por esse recurso em transações por segundo. Desenvolvemos uma aplicação para inserção e consultas de registros em *blockchain* seguindo padrões de projeto gerais que atendem à plataforma *Ethereum* e *Hyperledger Fabric* simultaneamente (XU et al., 2017). Em seguida, conduzimos experimentos realistas para avaliações quantitativas sob o método proposto, aumentando gradativamente o poder dos recursos computacionais e a carga de trabalho imposta à aplicação. Dessa forma exploramos o melhor compromisso entre custo e desempenho para várias infraestruturas executarem aplicações *blockchain* em redes públicas ou permissionadas via uma única métrica que é o custo por transação.

1.1 Objetivos

Neste trabalho propomos um método para estimar o custo da infraestrutura por transação de uma aplicação em *blockchains* públicas e permissionadas. Conduzimos experimentos no *Ethereum* (*blockchain* pública) e *Hyperledger Fabric* (*blockchain* permissionada) com o método proposto, aumentando gradativamente o poder dos nodos e a carga de trabalho imposta nas redes.

1.1.1 Objetivos específicos

Em suma, os objetivos deste trabalho são:

- Analisar o impacto do custo e do desempenho em aplicações blockchain públicas e permissionadas, considerando simultaneamente a infraestrutura e a carga de trabalho, a fim de identificar estratégias para melhorar o desempenho e reduzir custos.
- Desenvolver uma metodologia experimental que aplica a referida análise a aplicações tipicas para redes *blockchains* públicas e permissionadas mais populares, assim como infraestruturas com diferentes capacidades computacionais.

2 Referencial Teórico

Este capítulo apresentará a definição de *blockchain*, quando surgiu, a sua importância e os seus principais modelos (pública e permissionada). Além disso, será detalhado o conceito dos protocolos *blockchain* analisados neste trabalho, sendo eles a *Ethereum* e o *Hyperledger fabric*.

2.1 Blockchain

Blockchain é uma tecnologia de armazenamento de dados distribuída cujo objetivo é armazenar e gerenciar dados de informações sobre transações de forma segura, confiável e transparente. Foi apresentada pela primeira vez por Satoshi Nakamoto em 2008 no artigo intitulado de *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, com intuito de utilizar essa tecnologia para a implementação do sistema de moeda digital *Bitcoin* (NAKAMOTO, 2008). O termo *blockchain* se refere a como os dados são estruturados dentro da rede, onde todos os dados são ordenados em blocos sendo que cada um possui uma lista de transações. Cada bloco possui uma representação criptográfica (*hash*) do bloco antecessor, assim o ligando a uma cadeia de blocos encadeados. Deste modo, o histórico de transações na blockchain não podem ser alteradas ou removidas sem invalidar o *hash* do bloco (XU et al., 2017).

Figura 1 – Representação de como os blocos na blockchain são encadeados.

Segundo Greve et al. (2018) a *blockchain* é uma tecnologia que oferece suporte distribuído confiável e seguro para a realização de transações em uma rede, no qual participantes não se conhecem e não necessariamente possuem confiança entre si. Desta forma, elimina a necessidade de uma terceira entidade intermediária confiável para a realização de transações como bancos, governos, cartórios, etc. Além disso, também reduz custos de transações ao eliminar a necessidade de terceiros confiáveis (XU et al., 2017). Para garantir tal segurança e confiabilidade, é necessário que todos os participantes cheguem a um consenso sobre o estado atual da rede. Para isso é necessário o uso de algoritmos de consenso, no qual irão validar as transações e adicionar novos blocos na *blockchain*. Existem diversos algoritmos de consenso, os mais populares são o *Proof of Work (PoW)*, *Proof of Stake (PoS)* e o *Practical Byzantine Fault Tolerance (PBFT)*.

A arquitetura da *blockchain* é baseada em uma rede P2P (*peer-to-peer*), em que os nós deste tipo de rede se conectam entre si sem a necessidade de um intermediário centralizado. Em uma rede P2P cada nó é responsável por armazenar e validar informações, e todos os nós possuem acesso aos mesmos dados. Quando uma transação é realizada na rede ela é validade e armazenada por vários nós da rede, deste modo garantindo a integridade e segurança dessas informações. A arquitetura P2P da *blockchain* possui algumas vantagens em relação a sistemas centralizados. Por exemplo, essa arquitetura é menos suscetível a falhas e ataques, pois não possui um ponto único de falha na rede. Outra vantagem é que não é possível censurar informações ou dados, pois não é possível que um único participante censure as transações da rede.

2.2 Rede blockchain pública e permissionada

As redes *blockchains* públicas foram as primeiras a serem desenvolvidas e são as mais usadas. Os dois maiores exemplos deste tipo são a *Ethereum* (BUTERIN et al., 2014) e *Bitcoin* (NAKAMOTO, 2008). Este tipo de rede é de acesso aberto, ou seja, qualquer um pode participar da rede. Deste modo, realizar ou visualizar transações de forma transparente. Por este tipo de rede ter seus recursos abertos, existem regras (i.e., papeis) que devem ser seguidas pelos participantes de modo que o sistema distribuído funcione adequadamente. Pode-se destacar dois tipos de participantes em uma rede *blockchain* pública, que são os usuários comuns e os usuários mineradores. Os usuários comuns se registram na rede *blockchain* por meio de uma carteira digital, que se trata de um software capaz de armazenar e gerenciar as criptomoedas do usuário. É através dessa carteira que o usuário consegue realizar transações dentro da rede, geralmente enviar ou receber criptomoedas, além disso, é possível que o usuário realize transações por meio dos *dApps*. Os usuários neste tipo de rede precisam pagar uma taxa para que sua transação seja pelos nós da rede, o valor desta taxa pode variar dependendo do congestionamento da rede, o tamanho da transação (i.e., quantidades de dados) e o tipo de criptomoeda utilizada na rede.

As *blockchains* permissionadas, diferente das públicas, não possui o acesso aberto, para participar deste tipo de rede é necessário a aprovação dos nós que já participam da rede. Além disso, as informações e transações realizadas somente são visíveis aos participantes, e claro, somente quem participa pode realizar transações. Os participantes deste tipo de rede podem incluir operadores de nós, administradores, desenvolvedores de contratos inteligentes, auditores e reguladores. Tais participantes formam um consórcio, que se trata de um grupo de empresas ou organizações que se juntam com o propósito de criar uma rede *blockchain* compartilhada. Em um consórcio, cada participante contribui com algum tipo de recurso para o desenvolvimento da rede, além de contribuir com a manutenção da rede. Diferentemente das redes públicas, a identidade de todos os participantes das redes permissionadas é conhecida e autenticados criptograficamente (MONRAT; SCHELÉN;

ANDERSSON, 2020). Neste modelo, não há a necessidade de mineradores, já que todos os nós atuam como validadores das transações, portanto, não há taxas para executar uma transação. O maior exemplo deste modelo de rede é o *Hyperledger fabric* (ANDROULAKI et al., 2018), uma das plataformas de *blockchains* permissionadas mais populares.

2.3 Ethereum

A rede *Ethereum* (BUTERIN et al., 2014) foi lançada em 2015, se baseia na inovação da tecnologia do *Bitcoin*, mas possui grandes diferenças. Umas delas é que o *ethereum* foi o primeiro protocolo baseado em *blockchain* a utilizar *smart contracts*, segundo (MALIK et al., 2019) isto fornece uma plataforma programável que possibilita a implantação de contratos inteligentes escritos em uma linguagem de programação *turing-completa*. A *Ethereum* é uma plataforma com o propósito de permitir a criação de aplicativos descentralizados (dApps), aplicativos que utilizam a *blockchain* e *smart contracts* para funcionar de forma descentralizada e autônoma (WOOD et al., 2014), para diversas finalidades como o registro de propriedade intelectual, venda ou leilão de NFT's (*Tokens não fungíveis*), votação eletrônica, e até jogos.

Os *smart contracts* são programas desenvolvidos para automatizar um acordo entre partes, deste modo satisfazendo condições contratuais comuns sem a necessidade de intermediários confiáveis (GREVE et al., 2018). Estes contratos são armazenados na *blockchain* com outras transações realizadas na rede. Quando um *smart contract* é acionado, a *blockchain* executa o código do contrato de forma automática, e verifica se todas as condições impostas no contrato foram atendidas. No *Ethereum* os *smart contracts* são armazenados e executados na *Ethereum Virtual Machine (EVM)*, que se trata de uma máquina virtual *Turing* completa, sendo capaz de executar qualquer programa escrito em uma linguagem para computador. No *Ethereum* os *smart contracts* são escritos na linguagem *Solidity*, que se trata de uma linguagem desenvolvida desenhada para ser executada na EVM (WOOD et al., 2014).

2.3.1 Arquitetura do Ethereum

A arquitetura que empregamos para avaliação de custos da rede pública utiliza nós privados *Ethereum*. Estes nós são configurados a partir do *Geth*, que é a implementação oficial do protocolo da rede Ethereum. Assim, pode ser criada uma instância da rede *Ethereum* com múltiplos nós sem conexão com a rede principal ou com redes de teste para execução de experimentos, ou utilização de forma privada. A Figura 2 apresenta o modelo de arquitetura da rede *Ethereum* com um nó minerador e um nó Validador, que provê acesso para as aplicações e a qual utilizamos.

O nó minerador é responsável pela mineração de transações e é quem gera os blocos que encadeiam e armazenam estas transações. A garantia da integridade e veracidade das

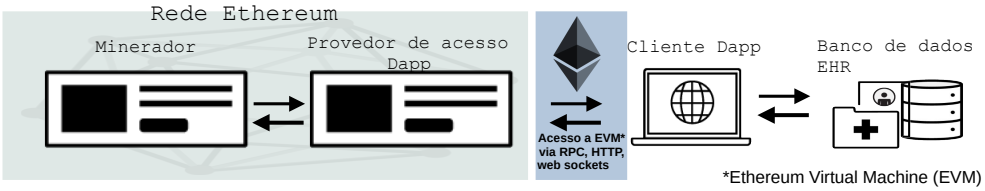


Figura 2 – Modelo de Blockchain privado.

informações também é realizada pelo nó minerador por meio do algoritmo de consenso nele implementado. Os blocos minerados serão então propagados para todos os nós pertencentes à rede. O nó Validador, por sua vez, mantém cópia de cada bloco minerado. Os nós Validadores expõem conexões via portas definidas por métodos e padrões *Remote Procedure Call* (RPC) para prover o acesso dos clientes da aplicação à rede.

2.4 Hyperledger Fabric

O *Hyperledger fabric* é uma implementação de *blockchain* que permite a criação de redes permissionadas, no qual permite que os participantes controlem quem possui acesso às suas transações (ANDROULAKI et al., 2018). Tal ferramenta foi desenvolvida pela *Linux foundation* com o propósito de ser utilizada em ambientes empresariais. Segundo (BALIGA et al., 2018), o *Hyperledger Fabric* se destaca pela sua flexibilidade, escalabilidade e segurança. Tais características permitem que a plataforma seja utilizada em diversas aplicações empresariais, como cadeia de suprimentos, sistemas financeiros, etc. Além disso, o *Hyperledger Fabric* fornece recursos para gerenciamento de identidades, deste modo permitindo que apenas participantes autorizados tenham acesso ao dados e transações dentro da rede.

Segundo (XU; WEBER; STAPLES, 2019), uma vantagem do *Hyperledger Fabric* é sua escabilidade. Pois a plataforma utiliza um modelo de consendo distribuído, no qual permite que a validação das transações seja feita após a aprovação de múltiplos participantes da rede. Deste modo, o *Hyperledger Fabric* pode suportar um grande número de transações por segundo, sendo algo muito importante para aplicações que exijam uma alta demanda de transações. Além disso, a plataforma fornece ferramentas para o desenvolvimento de contratos inteligentes, que podem ser desenvolvidos em linguagens de programação conhecidas como *Go*, *Java* e *JavaScript*.

2.4.1 Arquitetura Hyperledger Fabric

A implantação da rede *blockchain* permissionada segue as especificações da plataforma *Hyperledger Fabric* [1] e possui dois componentes físicos básicos: *nó pareador* e o *nó ordenador*. Cada nó pareador representa uma organização participante (P) da rede com

[1] *https://hyperledger-fabric.readthedocs.io/en/release-2.2/key_concepts.html*

as tarefas de emitir e validar objetos da *blockchain*. Para isso o nó pareador possui os módulos *ledger* (L), que registra transações; *CouchDB* que registra o estado global dos objetos (registro de ativo digital); *chaincode* (S) sendo o programa em que implementamos as transações e os estados dos objetos[2]; e o serviço de autenticação dos participantes (CA), que por padrão utiliza o mesmo protocolo de certificados digitais (X.509).

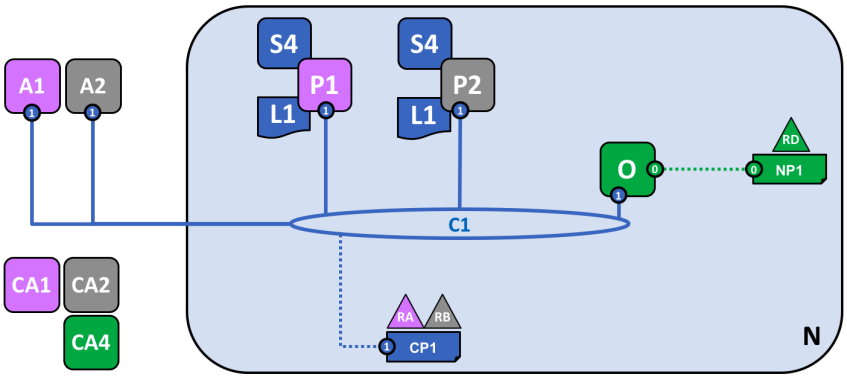


Figura 3 – Arquitetura do Hyperledger Fabric (Crédito: Hyperledger Fabric Documentation[3])

Por sua vez, o nó ordenador (O) é um membro neutro da rede, e deve ser mantido por todas as organizações participantes. Ele é responsável por receber transações dos nós pareadores, organizar as transações em blocos, e retransmitir esses blocos a todas as organizações participantes (nós pareadores) para validarem as transações, conforme programado no contrato inteligente. A plataforma *Hyperledger Fabric*, por padrão, utiliza o protocolo de consenso tolerante a falhas bizantinas (BFT). Esse protocolo garante a consistência da *blockchain* em todas as organizações, i.e., elas possuem cópias idênticas do *ledger* e cada objeto emitido possui o mesmo estado global.

[2] No Hyperledger Fabric os contratos inteligentes são denominados *chaincode*.

[3] Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/arch-deep-dive.html. Acesso em: 25 de março de 2023.

3 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados à avaliação de custos e desempenho de plataformas Blockchains.

O trabalho desenvolvido por Rimba et al. (2020) investigou a questão do custo monetário de utilizar uma plataforma *blockchain* em comparação com uma infraestrutura de armazenamento em nuvem. Por meio de modelos de custo para processos de negócios, eles compararam os custos na plataforma *Ethereum* e *Amazons Simple Workflow Service (SWF)*. Os resultados apontaram uma grande variação de custo entre as duas soluções. Sendo que o custo do *blockchain Ethereum* é, pelo menos, o dobro dos serviços tradicionais de nuvem fornecidos pelo Amazon SWF. Nosso trabalho desenvolveu um modelo de custo para *blockchains* públicas e permissionadas. Tal método foi aplicado em diferentes tipos de infraestruturas do serviço EC2 da AWS. Isso nos permitiu identificar estratégias específicas para melhorar o desempenho e reduzir custos em diferentes cenários.

(BALIGA et al., 2018; THAKKAR; NATHAN; VISWANATHAN, 2018; WANG; CHU, 2020) analisaram o desempenho da plataforma *Hyperledger Fabric*. A abordagem de Baliga et al. (2018) utilizou a ferramenta *Hyperledger Caliper* sob diferentes configurações para avaliar a latência e a taxa de transferência do *Hyperledger Fabric*. Avaliaram também o desempenho variando o número de *chaincodes*, *channels* e *peers*. Concluíram que a taxa de transferência é sensível às configurações e a latência é significativamente afetada pelo tamanho da carga experimentada. Thakkar, Nathan e Viswanathan (2018) testam duas abordagens para avaliação de desempenho, otimização de cache e configuração de políticas de endosso. Como contribuição, os autores descreveram orientações sobre a configuração de parâmetros da rede e também os principais gargalos de desempenho. Nos estudos de Wang e Chu (2020), os autores caracterizaram o desempenho de cada fase do ciclo de vida de uma transação, sendo que a fase de execução mostrou boa escalabilidade de desempenho em políticas de endosso específicas. A fase de validação obteve desempenho pior porque a carga de trabalho de computação do nó de validação é pesada. Os resultados mostraram que o principal fator de desempenho foi a política de endosso, ou seja, quantos pares tiveram que aprovar uma transação.

Os artigos Leal, Chis e González-Vélez (2020), Rouhani e Deters (2017), Zhang et al. (2020) fornecem avaliação de desempenho de redes blockchain privadas baseadas na plataforma *blockchain Ethereum* de código aberto. (LEAL; CHIS; GONZÁLEZ-VÉLEZ, 2020) avaliam o desempenho da rede utilizando um conjunto de dados para encontrar uma configuração ideal. Utilizaram diferentes custos, algoritmos de consenso, e número de nós de rede para determinar a configuração. Como contribuição, é fornecida uma forma para encontrar uma configuração ideal para um determinado número de transações exigidas por um caso de uso. O trabalho de Rouhani e Deters (2017) mostrou que o desempenho da rede

Ethereum depende, além da configuração da rede, da implementação do cliente utilizada. O estudo mostra que o cliente Parity obteve desempenho significativamente melhor do que o cliente Geth. Em Choi e Hong (2021), os autores utilizaram o *Hyperledger Caliper* para avaliar a rede Ethereum. Os resultados mostram que o desempenho das transações pode diferir de acordo com seu conteúdo e configuração da rede. Em Kim et al. (2021) é proposto uma solução para aumentar a eficiência e escabilidade da rede *blockchain*, sugerindo o uso do *Hyperledger Fabric* em conjunto com redes móveis 5G e comunicação *device-to-device (D2D)*. De acordo com Kim et al. (2021) a combinação destas tecnologias permitiria a criação de uma rede *blockchain* mais rápida e confiável, pois a tecnologia 5G permite aumentar a velocidade de transmissão de dados e a tecnologia D2D permite a comunicação direta entre dispositivos, deste modo eliminando redes de transmissão intermediárias.

Existem alguns estudos de análise de desempenho *blockchain*, que avaliam e comparam as plataformas *Hyperledger Fabric* e Ethereum. Em Monrat, Schelén e Andersson (2020) é realizada uma análise de desempenho e escalabilidade, variando as cargas de trabalho, das plataformas *Ethereum*, *Quorum*, *Corda* e *Hyperledger Fabric*. A conclusão geral do trabalho é que o *Hyperledger Fabric* tem um desempenho superior às demais plataformas porque atinge o consenso de forma mais eficiente. Em Malik et al. (2019) é realizada uma comparação do desempenho das plataformas *Ethereum* e *Hyperledger Fabric* utilizando uma aplicação de comércio de energia e *Hyperledger Caliper*. A conclusão é que o *Ethereum* fornece a melhor solução para a aplicação em pequena escala, mas, o *Hyperledger Fabric* pode ser mais adequado para aplicações de grande escala. Entretanto, estes trabalhos não analisaram ou avaliaram o custo de manter as aplicações em *blockchain*.

Trabalho	**Plataforma**	**Tipo de Rede**	**Método**
(RIMBA et al., 2020)	Ethereum, Amazon SWF	Pública, Nuvem	Modelo de Custo
(BALIGA et al., 2018))	Hyperledger Fabric	Privada	Avaliação de Desempenho
(THAKKAR; NATHAN; VISWANATHAN, 2018)	Hyperledger Fabric	Privada	Avaliação de Desempenho
(WANG; CHU, 2020)	Hyperledger Fabric	Privada	Avaliação de Desempenho
(LEAL; CHIS; GONZÁLEZ-VÉLEZ, 2020)	Ethereum	Privada	Avaliação de Desempenho
(ROUHANI; DETERS, 2017)	Ethereum	Privada	Avaliação de Desempenho
(CHOI; HONG, 2021)	Ethereum	Pública	Avaliação de Desempenho
(KIM et al., 2021)	Hyperledger Fabric, 5G, D2D	Pública	Proposta de Melhoria
Este Trabalho	Ethereum, Hyperledger fabric e AWS EC2	Pública e Privada	Modelo de Custo e avaliação de desempenho

Tabela 1 – Tabela Comparativa dos Trabalhos Relacionados

4 Análise de custo e desempenho

Para análise de custo é necessário identificar a vazão máxima suportada em redes *blockchain* com infraestruturas diferentes, especificamente, redes cujos nós tenham recursos computacionais de diferentes capacidades. Nesta seção discutimos a metodologia utilizada para determinar a vazão máxima empiricamente. Primeiramente, a aplicação *blockchain* típica para condução dos experimentos é apresentada e, a seguir, o ambiente experimental e ferramentas são descritos.

4.1 Custo por transação

A análise consiste em uma estimação do custo por transação considerando uma aplicação da tecnologia blockchain para inserção e consulta de registros em uma rede pública ou permissionada. Esta análise tem o objetivo de encontrar uma rede com uma infraestrutura com o menor custo possível ($custo_{ideal}$), mas que ainda atenda a demanda de uso prevista, considerando a vazão máxima (t_{ideal}) para a carga de trabalho avaliada. Nesse sentido, o formalizamos com as definições a seguir.

A quantidade de dados a serem registradas na rede é representada por w e seu valor é passado como uma carga de trabalho para ser processada pela rede. Cada carga consiste em um conjunto de dados emitidos em um determinado período de tempo, i.e., transações por segundo (tps). Também é informado um conjunto de tipos de recursos computacionais disponíveis. Este conjunto é definido por R e tem-se o tipo de recurso caracterizado por: $r_i = (cpu_i, memória_i, custo_i) \in R$. Considera-se uma rede blockchain B composta de nós com configuração uniforme: $B = r_i \in R$. A função $Max\_Vazão$ retorna o conjunto de todas as vazões máximas t_i para cada tipo de recurso r_i como nó $b \in B$. Onde $Max\_Vazão(R, w, B) = T$. Obtém-se o conjunto alvo A, em que a porcentagem de uso dos recursos computacionais está abaixo do limite L, definido em comum acordo pelos participantes da rede, $A = \{uso(r_i) \leq L | r_i \in T\}$. A função $Min\_Custo(A)$ retorna o recurso com menor custo para a carga w em A, onde r_{ideal} representa o recurso com $custo_{ideal} \in A$ e também a vazão máxima $t_{ideal} \in A$. Dada por:$Min\_Custo(A) = r_{ideal}$. Por fim, o custo de uma transação na blockchain B para a carga w considerando o conjunto de tipos de recursos computacionais R é dado pela Equação 4.1.

$$C_{trans} = \frac{custo_{ideal}}{t_{ideal}} \tag{4.1}$$

Por fim, a equação 4.1 é usada para calcular o custo por transação na rede blockchain. Ela divide o custo ideal $custo_{ideal}$ pelo valor da vazão máxima ideal t_{ideal}. Dessa forma,

quanto menor for o custo ideal e maior for a vazão máxima, menor será o custo por transação na rede blockchain.

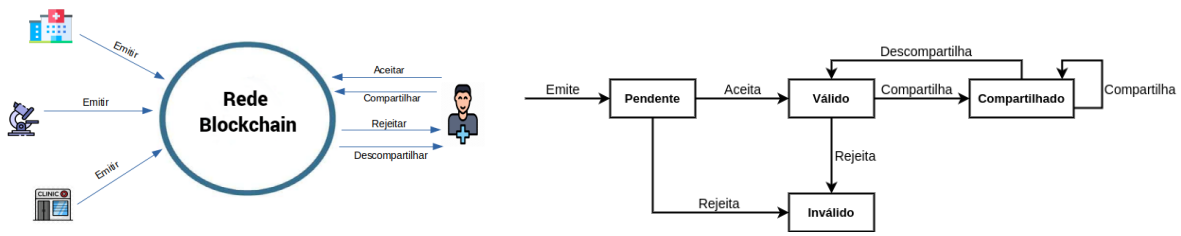
4.2 Aplicação Blockchain Típica

Neste trabalho, utilizamos uma aplicação *blockchain* típica, sendo o compartilhamento e gerenciamento de registros médicos eletrônicos (EMR), implementado em *Smart Contract* e *Chaincodes* para as plataformas *blockchain Ethereum* e *Hyperledger Fabric*. Esse modelo de aplicação pode ser utilizado em vários outros contextos pelos devidos aspectos: (i) armazenamento *offchain*, i.e., a *blockchain* armazena um resumo do registro no formato de um *hash* criptográfico para fins de rastreabilidade e auditabilidade, e (ii) dados completos dos registros são mantidos pelas organizações com permissões de acessos definidas pelos donos dos registros (e.g., pacientes). Dessa forma, exploramos *blockchain* como uma camada de conexão entre diferentes organizações, unificando aspectos comuns de redes *blockchains* públicas e permissionadas, i.e., baixo custo de armazenamento (dados *offchain*) e integração com sistemas já existentes.

O diagrama da Figura 4(a) mostra os dois tipos de participantes modelados na aplicação. Na esquerda temos as organizações do ecossistema de saúde como hospitais, clínicas e laboratórios, e na direita temos o paciente que utiliza os serviços dessas organizações. Cada relacionamento entre paciente e organização gera um EMR armazenado em sistemas usuais das organizações de saúde. Na rede, o EMR também se torna um *objeto* a ser registrado na *blockchain* na forma de resumo criptográfico (*hash*).[1] Além do *hash*, o objeto EMR contém os campos: ID da organização emissora do EMR, ID do paciente, marca de tempo, compartilhamento e localização. O ID é a chave pública do participante que compõe a sua credencial na rede (código alfanumérico) juntamente à chave privada, essa última mantida secretamente pelo participante apenas para autenticações. O compartilhamento consiste em uma lista de pares (ID, expiração), que representa a organização que tem acesso ao objeto e a data de expiração do acesso. A localização, por sua vez, consiste em um endereço (e.g., link) onde o EMR pode ser acessado via as credenciais dos participantes com tal permissão.

A Figura 4(a) também ilustra as transações que podem ser realizadas pelos participantes da rede. Nesse caso, a organização emite o EMR, ao passo que o paciente o aceita ou rejeita, e adicionalmente compartilha ou descompartilha o EMR com outras organizações via autenticação com sua chave privada para cada transação. Por sua vez, a Figura 4(b) ilustra o estado do EMR após cada transação. Na aplicação, a transação *compartilha* se aplica apenas a objetos no estado *válido*, enquanto a transação *descompartilha* limpa a lista de compartilhamentos e retorna o objeto para o estado *válido*. Por sua vez, o ciclo

[1] Utilizamos o algoritmo *SHA256* para gerar o *hash*, mas outros algoritmos também podem ser utilizados.



(a) Participantes da rede e suas transações (b) Estados do objeto após transação

Figura 4 – Visão geral da aplicação blockchain.

de vida de um objeto finaliza quando o paciente rejeita a organização emissora indo para o estado *inválido* a partir dos estados *pendente* ou *válido*, o que significa desautorizar a organização a utilizar o EMR para qualquer finalidade. A Figura 4(b) ilustra também a modificação no estado dos objetos a partir das transações. Sistemas baseados em *blockchain*, tipicamente, mantém o estado global dos objetos e os valores de seus respectivos campos, dado a última transação realizada, em bancos de dados auxiliares (e.g., CouchDB, LevelDB) para aumentar a velocidade de acesso. Contudo, cada transação sobre esse objeto é registrada na *blockchain* para fins de auditabilidade e inviolabilidade dos dados.

É importante ainda observar que a aplicação armazena metadados de EMRs (dados *offchain*), que são passíveis de serem comprovadas sua autenticidade por todos os participantes. Logo, a *blockchain* é explorada para estabelecer a inviolabilidade dos registros e o não repúdio da posse desses por parte das organizações que os possuem ou compartilham. A *blockchain* oferece provas digitais auditáveis para garantir o compartilhamento de dados entre organizações sem confiança mútua (e.g., concorrentes), e a judicialização entre as partes pelo vazamento ou uso indevido de EMRs.

4.3 Ambiente Experimental e Métricas

Cargas sintéticas para a aplicação *blockchain* típica apresentada foram geradas com foco na transação de emissão de EMR, i.e., inserção de registros, a qual é usualmente a operação com maior uso de recursos computacionais e atrasos em *blockchains* como já observado em trabalhos anteriores (SPENGLER; SOUZA, 2021). Nesse sentido, a ferramenta de aferição *Caliper* (CALIPER, 2019) foi utilizada para gerar cargas com emissão de EMRs. Diferentes cargas de trabalho foram submetidas às redes, onde cada carga representa um conjunto de registros emitidos por segundo, i.e., transações por segundo (tps), de forma fixa em um dado período de tempo aqui chamado por rodada. O valor em tps das cargas de trabalho foram aumentadas gradativamente até ser atingido o ponto de saturação da rede em que todas as transações submetidas falham.

Quatro tipos de recursos computacionais foram utilizados para executar os experimen-

tos nas redes blockchain pública e permissionada. Esses tipos são máquinas virtuais (VMs) do serviço *Amazon Elastic Cloud Computing* (EC2) para compor os nós de cada rede, e aumentamos gradualmente o poder computacional desses nós para analisar o desempenho da rede em função do aumento de carga. Nesse sentido, foram utilizadas as VMs T2 do tipo *small, medium, xlarge* e *2xlarge*, cujas respectivas especificações são apresentadas na Tabela 2.

A plataforma *Hyperledger Fabric* (rede permissionada) foi configurada com o *Minifabric*, uma ferramenta para implementação dessa rede. Configuramos a rede com quatro nós pareadores e um nó ordenador, sendo que o *Minifabric* inicia a rede com um nó ordenador e dois nós pareadores em uma única VM. As cargas foram submetidas por dois clientes *Caliper*, cada cliente utilizando um nó pareador em VMs separadas. Para a plataforma *Ethereum* (rede pública) foi configurado um nó minerador em uma VM exclusiva, um nó validador para prover acesso à rede em outra VM, e um cliente *Caliper* em outra VM que realizou a submissão de transações.

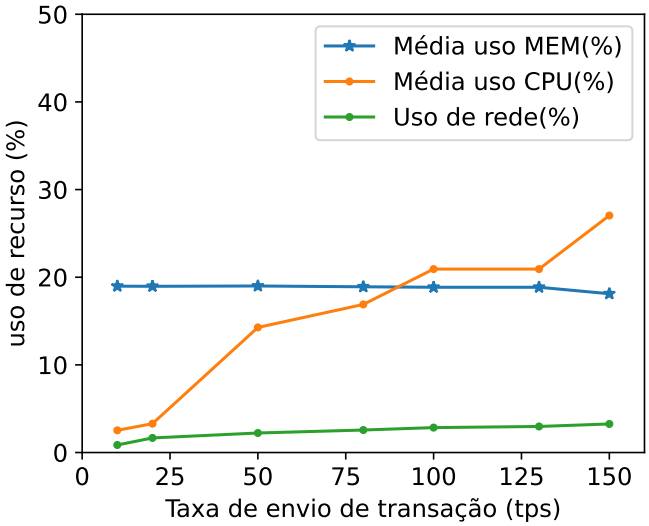
	Small	**Medium**	**xLarge**	**2xLarge**
vCPUs	1	2	4	8
Memória (GB)	2	4	16	32
Custo/hora (USD)	0,0230	0,0464	0,1856	0,3712

Tabela 2 – Especificações dos nós que compõem cada tipo de infraestrutura: família AWS T2, processador Intel Xeon 3.0-3.3 GHz e disco SSD de 100 GB.

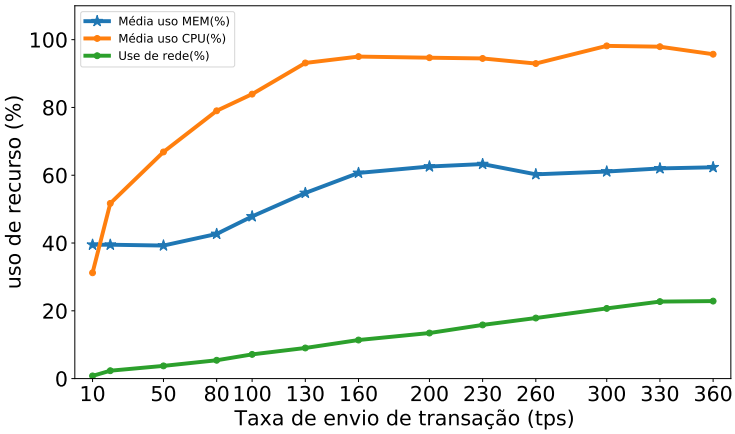
Para cada carga de trabalho executada foram medidos a vazão da rede em tps e o atraso da transação, além da medição do uso dos recursos processamento (CPU), memória, disco e rede para os nós da rede. O *Caliper* registra o instante de envio e de confirmação (sucesso ou falha) para cada transação. Assim, a vazão é calculada pela taxa de total de transações com sucesso sobre o período total da carga aplicada, i.e., a diferença entre o instante da última confirmação e o instante da primeira submissão. Por sua vez, o uso dos recursos computacionais foram coletados em granularidade de segundos via a biblioteca *Psutil versão 5.9.0*. Esta biblioteca é multiplataforma e tem como finalidade o monitoramento de processos e sistemas em Python. Desenvolvemos um script utilizando a biblioteca *Psutil* e instalamos em cada nó da rede para coletar os dados referentes aos recursos monitorados.

No método de custo apresentado (Seção 4), é necessário identificar a vazão máxima suportada em redes blockchain com recursos computacionais diferentes, especificamente, redes cujos nós tenham as capacidades apresentadas na Tabela 2. Intuitivamente, o crescimento da vazão está associado ao aumento do consumo de recursos computacionais, assim como a super utilização desses recursos pode levar à limitação da vazão. Nesse sentido, foi examinado quais recursos do nó são mais consumidos com o aumento da carga na rede blockchain, indicando a vazão máxima que pode ser alcançada nessa rede por contenção desses recursos.

A Figura 5 (a) e (b) mostra o consumo médio de CPU, memória e rede[2] para cargas sintéticas submetidas sobre as redes Ethereum e Hyperledger Fabric construídas com nós do tipo *medium* com a finalidade de observar quais desses recursos são mais requisitados, preliminarmente ao início dos experimentos. Como pode ser observado, CPU é o recurso com o uso mais impactado com os aumentos de carga, i.e., a taxa do envio de transações, ao passo que o uso de memória permanece estáveis e o uso da rede (entrada e saída) cresce em relação à capacidade máxima (1 Gbps) mas não tão significativamente quanto CPU. Portanto, o foco deste trabalho é no uso de CPU para identificar a vazão máxima nos quatro tipos de infraestruturas para as redes blockchain, e estabelecemos o limite de 100% de uso de CPU para o conjunto de infraestrutura alvo.



(a) Ethereum



(b) Hyperledger Fabric

Figura 5 – Uso de recursos CPU, memória e rede.

[2] Disco foi omitido dessa análise visto que a aplicação típica proposta para a avaliação foca no armazenamento *offchain*, como descrito na seção anterior.

Durante nossos experimentos, verificamos que a demanda por memória nos dois tipos de rede utilizados foi relativamente baixa. Na rede pública *Ethereum*, o uso de memória permaneceu em torno de 20% em média, enquanto na rede permissionada *Hyperledger Fabric*, o uso médio de memória chegou a cerca de 60%. É importante mencionar que esses resultados foram obtidos em uma máquina com 4GB de memória RAM. Quanto ao uso de rede, em ambas as redes, não foi observado um consumo superior a 20%. Em relação à CPU, notamos que o uso aumenta à medida que a carga de trabalho aumenta. Esse comportamento pode ser claramente observado na Figura 5(b), que indica que o uso de CPU chega a 100% ao se injetar altas cargas de trabalho.

4.4 Resultados

Nesta seção apresentamos os resultados. Primeiramente serão apresentados os melhores desempenhos alcançados pelas diferentes infraestruturas avaliadas para a aplicação nas redes pública e permissionada. A seguir, será incluído o fator custo, analisando a melhor relação entre custo e desempenho observada para as infraestruturas avaliadas.

4.4.1 Avaliação de Desempenho

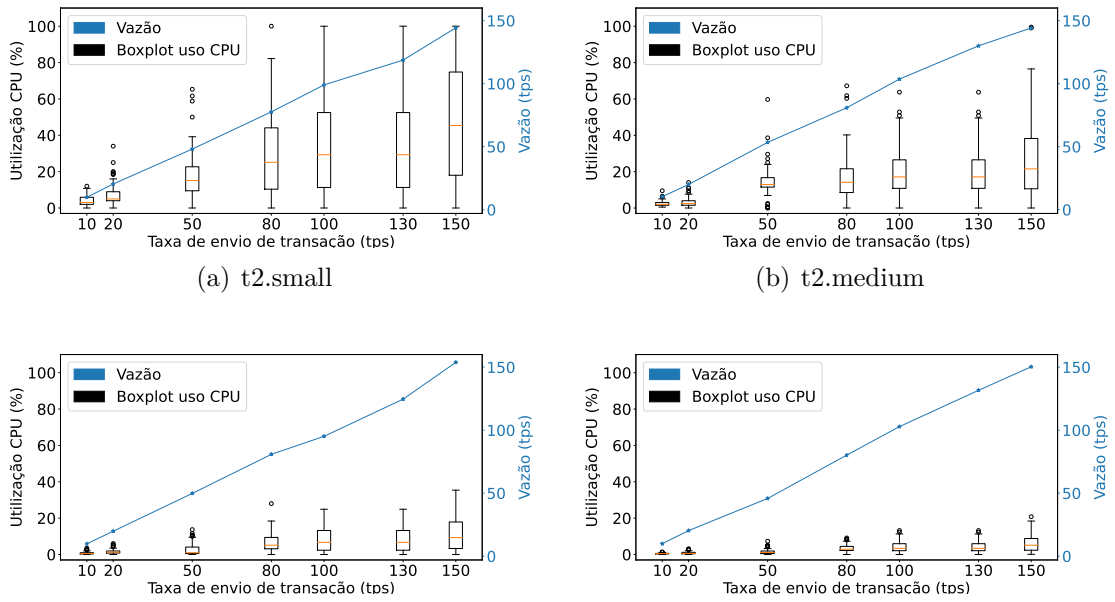
Foram executados diversos experimentos com redes *blockchains* pública (*Ethereum*) e permissionada (*Hyperledger Fabric*) implantadas em nós com crescimento gradativo da infraestrutura computacional, representada por CPU, e também sob cargas de trabalho crescentes, conforme a metodologia descrita na seção anterior.

As Figuras 6 e 7 mostram a variação de uso de CPU e a vazão em função da carga de trabalho em transações por segundo (tps) para as medições observadas nas redes pública e permissionada respectivamente com os quatro tipos de infraestruturas. As figuras apresentam *boxplots* para sumarizar a distribuição dos usos de CPU no eixo y principal da seguinte forma: o retângulo central se expande entre o primeiro e terceiro quartil, o segmento interior é a mediana, enquanto os indicadores abaixo e acima do retângulo representam o 10^{o} e 90^{o} percentis. Por sua vez, as curvas em azul mostram a evolução da vazão em tps no eixo y secundário.

A Figura 6 apresenta resultados observados para a rede *blockchain* pública, i.e., a aplicação na plataforma *Ethereum*. De modo geral, nota-se que a variação do uso de CPU cresce com o aumento da carga de trabalho, visto pelas expansões consecutivas dos boxplots entre o 10^{o} e 90^{o} percentis, que correspondem a 80% das medições. A vazão também cresce com o aumento da carga de trabalho. As medições foram limitadas até a carga de 150 tps, sendo o valor máximo suportado pelo cliente *Ethereum* utilizado sem perdas de transações. O foco dos experimentos está na avaliação de desempenho e na infraestrutura ideal para a aplicação cliente. Logo, a rede *blockchain Ethereum* foi construída com um nó minerador, de modo a não limitar a vazão pelo mecanismo de

consenso distribuído entre vários mineradores, como ocorre na rede *Ethereum* principal (*mainnet*). Dessa forma pode-se observar o impacto da infraestrutura computacional, i.e., o uso de CPU, na vazão da aplicação cliente.

Ao observar os quatro tipos de infraestruturas mostrados na Figura 6, nota-se que o tipo *small* sofre a maior variação de uso CPU em relação aos tipos *medium, large* e *2xlarge*. Logo, o cliente *Ethereum*, em infraestrutura do tipo *small*, pode enfrentar instabilidades que comprometam a vazão para cargas superiores a 100 tps. Isso porque uma parcela relevante das medições tiveram 100% do uso de CPU como indicada a marca do 90º percentil, i.e., 10% das medições. Por outro lado, os outros três clientes com maior poder computacional alcançam cargas de até 150 tps com estabilidade, i.e., menor variação, do uso de CPU, e raramente alcançam 100% de uso de CPU. Nesses casos, foi observado apenas uma amostra de medição para o cliente do tipo *medium* com 100% de uso de CPU em carga com 150 tps.



(a) t2.small (b) t2.medium

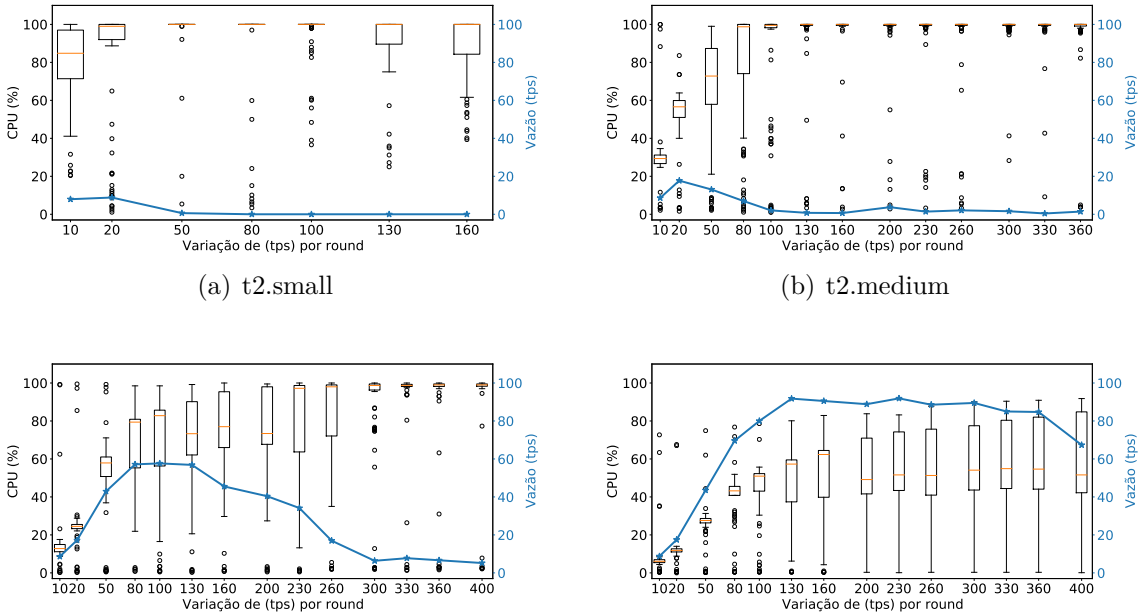
(c) t2.xlarge (d) t2.2xlarge

Figura 6 – Uso de CPU e vazão em rede pública Ethereum.

Agora discutimos os resultados observados para a rede *blockchain* permissionada, i.e., a aplicação na plataforma *Hyperledger Fabric*, mostrados na Figura 7. É notável o maior uso de CPU no nó *Hyperledger Fabric*, o que leva a maior variabilidade e saturação desse recurso para cargas bem menores ao observado anteriormente. Por exemplo, uma carga de 10 tps já leva o nó do tipo *small* a alcançar 100% de processamento em cerca de 10% das medições, como indica a marca do 90º percentil. Isso ocorre porque o nó da rede permissionada atua não apenas como um cliente recebendo transações dos usuários, mas também validando as transações dos demais nós da rede.

A vazão medida na rede permissionada foca nas transações submetidas por nó (visão

local) e não o total de transações da rede. Contudo, o nó usa recursos computacionais para validar transações de toda a rede o que levou a vazões menores que as observadas na rede pública. Em nossos experimentos, submetemos cargas de até 400 tps para a rede construída com nós do tipo *large* e *2xlarge*, mostrados respectivamente nas Figuras 7 (c) e (d). Observamos nesses casos, desempenhos satisfatórios com perdas zero ou inferiores a 1% do total de transações e vazões com comportamento ligeiramente linear para cargas de trabalho até 80 tps. Por outro lado em cargas superiores a essa, observa-se que o desempenho das redes alcançam um estágio de perda (i.e., decaimento da vazão). Essas perdas coincidem com a alta utilização de CPU em infraestruturas do tipo *small, medium e 2xlarge*, que visivelmente demonstram a saturação de suas CPUs dado certos graus de aumento de carga. Nas infraestruturas do tipo *2xlarge*, diferentemente, as perdas de desempenho decorrem da comunicação entre os nós da rede para validar transações, que segue o consenso BFT, usual nas redes *blockchain* permissionadas.



(a) t2.small (b) t2.medium

(c) t2.xlarge (d) t2.2xlarge

Figura 7 – Uso de CPU e vazão em rede permissionada Hyperledger Fabric.

Ao observar os quatro tipos de infraestruturas mostrados na Figura 7, nota-se que o tipo *small* não seria adequado para nós de uma rede permissionada *Hyperledger Fabric* como já discutido acima. Nos resta então analisar os demais tipos *medium, large e 2xlarge*. Seguindo o mesmo critério de escolha da infraestrutura adequada (i.e., 100% de uso de CPU abaixo do 90o. percentil), concluímos que o nó *Hyperledger Fabric* pode enfrentar instabilidades que comprometam a vazão para cargas superiores a 20 tps em infraestrutura do tipo *medium* e cargas a partir de 80 tps para o tipo *xlarge*. Por sua vez, na infraestrutura do tipo *2xlarge*, não foram observadas instabilidades devido aos recursos computacionais. Logo, conjecturamos que o aumento de vazão nesse caso estaria mais relacionado ao

protocolo de consenso distribuído adotado pela rede permissionada, cuja avaliação está fora do escopo deste trabalho.

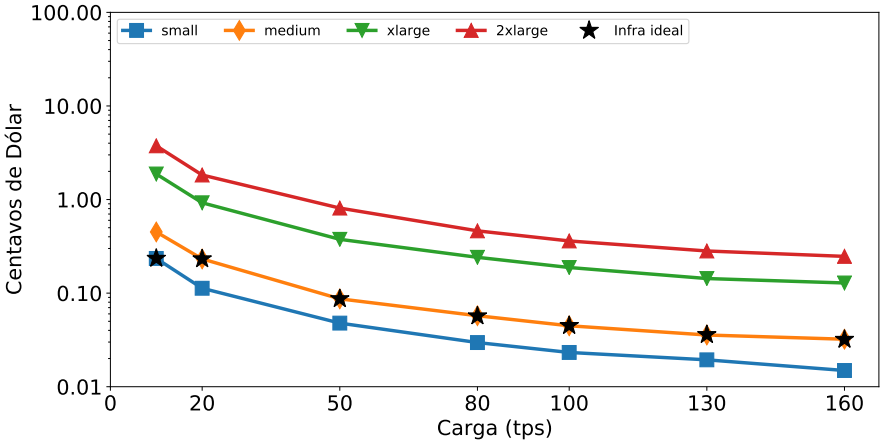
4.4.2 Compromisso entre Custo e Desempenho

Agora incluímos o fator custo para os desempenhos das redes para os quatro tipos de infraestruturas analisadas na seção anterior. A Figura 8 (a) e (b) mostra o custo por transação da aplicação típica nas redes pública (*Ethereum*) e permissionada (*Hyperledger Fabric*) em função da carga de entrada dada em tps. O custo por transação representa a relação entre o custo da infraestrutura por hora e a vazão da rede para a carga aplicada. Para melhor visualização, as figuras mostram o custo por transação em centavos de dólar (e.g., US$ 0,01 tem valor unitário 1,0 no eixo y) em escala logarítmica. Adicionalmente, foi incluída a marca (estrela) para recomendar a infraestrutura ideal, i.e., o compromisso entre custo e desempenho mais adequado segundo o método proposto na Seção 4. Em outras palavras, a recomendação foca primeiramente no uso adequado dos recursos computacionais do nó, mostrado na seção anterior, e a seguir, foca no menor custo. Logo, o tipo de infraestrutura com menor custo não é sempre recomendada nessa análise.

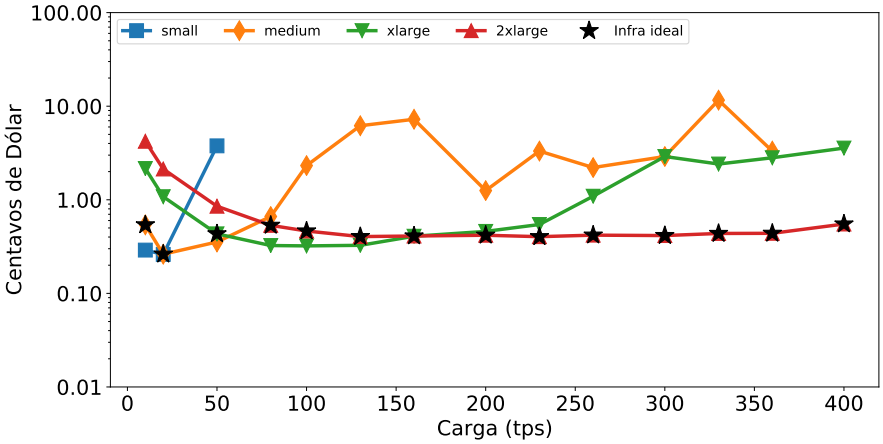
A Figura 8(a) mostra uma tendência de redução do custo por transação na rede pública para as quatro infraestruturas à medida que se aumenta a carga. Essa tendência reflete o bom desempenho observado para a aplicação típica na rede *Ethereum*. É importante observar que essa aplicação obteve uma vazão próxima à carga nos experimentos (Figura 6). No entanto, cargas altas são impraticáveis na rede pública principal do *Ethereum* com o protocolo de consenso atual, que alcança vazão em torno de 13 tps[3] independente da carga na rede. As recomendações de infraestrutura para o cliente *Ethereum* que executa a aplicação inicia com o custo por transação em 0,23 e alcança 0,03 centavos de dólar para nó do *small* e se mantém nessa faixa com nó do tipo *medium*. Considerando os experimentos até 20 tps, que é equivalente ao cenário atual, o custo da transação na rede pública se aproxima ao observado para a rede permissionada, que será discutida a seguir.

A Figura 8(b) apresenta o custo da transação na rede permissionada. Notavelmente, esse custo é maior ao observado na rede pública dado que o nó que executa a aplicação *Hyperledger Fabric* também valida transações de outros nós, i.e., o participa do consenso distribuído BFT adotado na rede permissionada. Logo, o consumo de recursos computacionais dos nós é maior nessa rede e, adicionalmente, há comunicação e espera entre os nós na realização do consenso. Em consequência, só foi possível calcular o custo de transação para as cargas submetidas na rede com nós *small* e *medium* até 50 e 350 tps, respectivamente. Todos esses aspectos contribuem para o decaimento da vazão em função da carga observada nos experimentos (Figura 7). Portanto, há uma tendência de aumento do custo da transação, como mostram as curvas representando cada tipo de infraestrutura na Figura 8(b). Nesse caso, a recomendação de infraestrutura ideal é importante ao

[3] Vazão média da rede *Ethereum* medida pelo serviço http://etherscan.io em fevereiro de 2022.



(a) Ethereum



(b) Hyperledger Fabric

Figura 8 – Custo por transação para cada tipo de infraestrutura por hora de uso: asteriscos indicam a recomendação de infraestrutura ideal considerando o compromisso entre custo e desempenho.

mostrar que aumentar o poder computacional dos nós face ao aumento de carga mantém o custo por transação razoavelmente estável. Observe na figura que a rede foi iniciada com nós do tipo *medium*, modificada para nós *xlarge* em cargas de 80 tps e, novamente, modificada para nós *2xlarge* em cargas a partir de 100 tps. Ao longo dessas modificações, o custo por transação foi mantido entre 0,54 e 0,55 centavos de dólar do início ao fim dos experimentos, respectivamente.

5 Conclusão

Neste trabalho foi proposto uma avaliação da infraestrutura *blockchain* necessário para que aplicações acessem e interajam com a rede. Para isso, uma comparação de desempenho e custo foi realizada entre as plataformas *Ethereum* e *Hyperledger Fabric*. Avaliamos por meio de um método de custo por transação para aplicações em redes *blockchain* pública e permissionada, considerando simultaneamente o desempenho máximo em função da infraestrutura e carga de trabalho imposta. Realizamos um experimento com a implementação de aplicações nas duas plataformas para aplicarmos o método em diferentes tipos de infraestrutura. Como resultado, fornecemos uma metodologia capaz de estimar o custo da infraestrutura por transação confirmada na *blockchain*, considerando redes públicas e permissionadas. A partir do método proposto, nossos resultados mostraram os limites de escalabilidade dessas redes e os compromissos entre custo e desempenho para aplicações *blockchain*.

Durante este trabalho tivemos alguns problemas em buscar e achar ferramentas para realizar a fase experimental de ambas as plataformas. Nesta fase foi usado a ferramenta de aferição *Hyperledger Fabric*, mas notamos que esta ferramenta ainda está em fase de melhorias pois em determinados momentos notamos alguns problemas em relação à precisão dos resultados retornados. Por isso, tivemos uma fase do trabalho somente para analisar tais resultados, e em alguns casos fazer o cálculo para obter os resultados de vazão de forma manual.

Ao longo deste trabalho foi possível aprender mais a fundo sobre a tecnologia *blockchain* e suas aplicações. Nenhuma plataforma apresentada neste trabalho é melhor que outras, ambas possuem modelos de negócio diferentes, portanto, a aplicação de cada uma vai depender do modelo de negócio da aplicação na qual serão implementadas. Basicamente, o *Ethereum* é mais adequado para aplicações em que a transparência e descentralização são mais importantes e valorizadas, como, por exemplo, finanças descentralizadas (DeFi) e tokenização de ativos. Já o *Hyperledger Fabric* é mais adequado para soluções empresariais, onde a privacidade e confiabilidade são características mais importantes, como setores governamentais e serviços financeiros.

Para trabalhos futuros, seria interessante o desenvolvimento de ferramentas para a aplicação do método proposto deste trabalho, com o intuito de facilitar a aplicação em diferentes tipos de redes *blockchain*. Além disso, aplicar este modelo em diversos cenários de uso, com o objetivo de verificar sua aplicabilidade em em diferentes contextos.

6 Publicações

Artigo submetido para o Workshop em *blockchain*: teoria, tecnologias e aplicações (WBLOCKCHAIN)

MENDONÇA, Ronan Dutra; DANTAS, Pedro Hércules; GONÇALVES, Glauber Dias; VIEIRA, Alex Borges; NACIF, José A. M.. Análise de Custo de Infraestrutura em Redes Blockchain Públicas e Permissionadas. In: WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES (WBLOCKCHAIN), 5. , 2022, Fortaleza. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022 . p. 26-39.

Artigo submetido para o XIV Encontro Unificado de Computação do Piauí (ENUCOMPI) e XI Simpósio de Sistemas de Informação (SINFO)

DANTAS, Pedro Hércules; GONÇALVES, Glauber Dias; VIEIRA, Alex Borges. B-Drive: em Direção a Redes para Compartilhamento de Registros Médicos Eletrônicos via Tecnologia Blockchain. In: ENCONTRO UNIFICADO DE COMPUTAÇÃO DO PIAUÍ (ENUCOMPI), 14. , 2021, Picos. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021 . p. 160-167.

Prêmio de melhor artigo no V Workshop Blockchain: Teoria, Tecnologia e Aplicações (WBlockchain) do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos para o artigo *Análise de Custo de Infraestrutura em Redes Blockchain Públicas e Permissionadas*.

Referências

ANDROULAKI, E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the thirteenth EuroSys conference*. [S.l.: s.n.], 2018. p. 1–15. Citado 2 vezes nas páginas 17 e 18.

BALIGA, A. et al. Performance characterization of hyperledger fabric. In: IEEE. *2018 Crypto Valley conference on blockchain technology (CVCBT)*. [S.l.], 2018. p. 65–74. Citado 4 vezes nas páginas 13, 18, 20 e 22.

BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, v. 3, n. 37, p. 2–1, 2014. Citado 3 vezes nas páginas 13, 16 e 17.

CALIPER, H. *Caliper*. 2019. Https://hyperledger.github.io/caliper. (Accessed on 09/23/2021). Citado na página 25.

CHOI, W.; HONG, J. W.-K. Performance evaluation of ethereum private and testnet networks using hyperledger caliper. In: IEEE. *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*. [S.l.], 2021. p. 325–329. Citado 2 vezes nas páginas 21 e 22.

GREVE, F. G. et al. Blockchain e a revolução do consenso sob demanda. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos*, 2018. Citado 3 vezes nas páginas 13, 15 e 17.

KIM, R. H. et al. Quick block transport system for scalable hyperledger fabric blockchain over d2d-assisted 5g networks. *IEEE Transactions on Network and Service Management*, IEEE, v. 19, n. 2, p. 1176–1190, 2021. Citado 2 vezes nas páginas 21 e 22.

LEAL, F.; CHIS, A. E.; GONZÁLEZ-VÉLEZ, H. Performance evaluation of private ethereum networks. *SN Computer Science*, Springer, v. 1, n. 5, p. 1–17, 2020. Citado 3 vezes nas páginas 13, 20 e 22.

MALIK, H. et al. Performance analysis of blockchain based smart grids with ethereum and hyperledger implementations. In: IEEE. *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. [S.l.], 2019. p. 1–5. Citado 3 vezes nas páginas 13, 17 e 21.

MONRAT, A. A.; SCHELÉN, O.; ANDERSSON, K. Performance evaluation of permissioned blockchain platforms. In: IEEE. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. [S.l.], 2020. p. 1–8. Citado 3 vezes nas páginas 13, 17 e 21.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260, 2008. Citado 3 vezes nas páginas 13, 15 e 16.

RIMBA, P. et al. Quantifying the cost of distrust: Comparing blockchain and cloud services for business process execution. *Information Systems Frontiers*, Springer, v. 22, p. 489–507, 2020. Citado 2 vezes nas páginas 20 e 22.

ROUHANI, S.; DETERS, R. Performance analysis of ethereum transactions in private blockchain. In: IEEE. *2017 8th IEEE international conference on software engineering and service science (ICSESS)*. [S.l.], 2017. p. 70–74. Citado 3 vezes nas páginas 13, 20 e 22.

SPENGLER, A. C.; SOUZA, P. S. Avaliação de desempenho do hyperledger fabric com banco de dados para o armazenamento de grandes volumes de dados médicos. In: *Proc. of WPerformance*. [S.l.: s.n.], 2021. ISSN 2595-6167. Citado na página 25.

THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: IEEE. *2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS)*. [S.l.], 2018. p. 264–276. Citado 3 vezes nas páginas 13, 20 e 22.

WANG, C.; CHU, X. Performance characterization and bottleneck analysis of hyperledger fabric. In: IEEE. *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. [S.l.], 2020. p. 1281–1286. Citado 3 vezes nas páginas 13, 20 e 22.

WOOD, G. et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, v. 151, n. 2014, p. 1–32, 2014. Citado na página 17.

XU, X. et al. Latency performance modeling and analysis for hyperledger fabric blockchain network. *Information Processing & Management*, Elsevier, v. 58, n. 1, p. 102436, 2021. Citado na página 13.

XU, X.; WEBER, I.; STAPLES, M. *Architecture for blockchain applications*. [S.l.]: Springer, 2019. Citado 2 vezes nas páginas 13 e 18.

XU, X. et al. A taxonomy of blockchain-based systems for architecture design. In: IEEE. *2017 IEEE international conference on software architecture (ICSA)*. [S.l.], 2017. p. 243–252. Citado 2 vezes nas páginas 14 e 15.

ZHANG, L. et al. Ethereum transaction performance evaluation using test-nets. In: SPRINGER. *European Conference on Parallel Processing*. [S.l.], 2020. p. 179–190. Citado 2 vezes nas páginas 13 e 20.

Apêndices

APÊNDICE A – Apêndice

Artigo submetido para o Workshop em *blockchain*: teoria, tecnologias e aplicações (WBLOCKCHAIN) em 2022.

Análise de Custo de Infraestrutura em Redes Blockchain Públicas e Permissionadas*

Ronan Dutra Mendonça[1], Pedro Hércules Dantas[2]
Glauber Dias Gonçalves[2], Alex Borges Vieira[3], José A. M. Nacif[1]

[1]Universidade Federal de Viçosa (UFV) – Florestal, MG – Brasil
[2]Universidade Federal do Piaui (UFPI) – Picos, PI – Brasil
[3]Universidade Federal de Juiz de Fora (UFJF) – Juiz de Fora, MG – Brasil

{ronan.dutra,jnacif}@ufv.br,{pedrohercules,ggoncalves}@ufpi.edu.br

alex.borges@ufjf.edu.br

Resumo. *Blockchain é uma tecnologia disruptiva que oferece recursos para aumentar a segurança nas relações entre organizações via o registro auditável e descentralizado de transações. Existe um crescente interesse por aplicações dessa tecnologia, mas o seu uso requer a escolha de uma rede pública ou permissionada. O tipo de rede impacta nas qualidades não funcionais das aplicações, em especial desempenho e custo. Neste artigo, investigamos esse impacto com foco na infraestrutura das redes pública e permissionada para uma aplicação blockchain típica. Modelamos o custo monetário da infraestrutura para a aplicação obter a vazão máxima em função da carga esperada em transações por segundo. Nossos resultados mostram os limites de escalabilidade dessas redes e os seus compromissos entre custo e desempenho no projeto de aplicações baseadas em blockchain.*

Abstract. *Blockchain is a disruptive technology that offers resources to increase security in relationships between organizations via the auditable and decentralized record of transactions. There is a growing interest in applications of this technology, but its use requires the choice of a public or permissioned network. The network type impacts the non-functional qualities of applications, especially performance and cost. In this paper, we investigated this impact focusing on the infrastructure of public and permissioned networks for a typical blockchain application. We model the monetary cost of the infrastructure for the application to obtain the maximum throughput as a function of the expected workload in transactions per second. The results show the scalability limits of these networks and trade-offs between the cost and performance in blockchain application design.*

1. Introdução

Blockchain é uma tecnologia disruptiva com impactos nas relações entre pessoas, consumo e produção de bens e serviços [Xu et al. 2019]. Essa tecnologia possibilita o registro seguro e descentralizado de dados ou transações entre entidades (pessoas e/ou organizações) que podem não se conhecer, e assim não terem confiança mútua.

*Essa pesquisa é financiada por CNPq/Amazon AWS (Processo 440069/2020-3) e PIBITI UFPI.

Logo, os dados e transações entre essas entidades são registradas de forma imutável, com acesso público ou privado para fins de verificação de autenticidade e derivação de novas transações. Isso se tornou possível a partir da evolução e unificação de outras tecnologias, em especial, criptografia assimétrica e protocolos de consenso distribuído via comunicação par a par, que são a essência de blockchains [Greve et al. 2018].

Existe um crescente interesse por novas aplicações dessa tecnologia no meio corporativo e nos serviços públicos, além das já conhecidas aplicações para cripto ativos Bitcoin e Ethereum [Nakamoto 2008, Wood 2014]. Os recursos da tecnologia blockchain como os *contratos inteligentes* estendem o seu uso em diferentes domínios de aplicação corporativas [Xu et al. 2019]. Contudo, essa tecnologia encontra-se ainda em fase de amadurecimento e necessita de ferramentas para gerenciamento de custos e recursos computacionais (i.e., infraestrutura) que permitirão a sua adoção por organizações nos setores da indústria, serviços e governos. Atualmente os modelos de infraestrutura mais adotadas para a tecnologia blockchain são *redes públicas* e as *redes permissionadas*, sendo que o desempenho e o custo associados são questões essenciais para a definição de qual modelo blockchain utilizar.

As redes blockchain públicas foram as primeiras a serem desenvolvidas e são ainda as mais utilizadas. Plataformas populares como Ethereum permitem o desenvolvimento e execução de contratos inteligentes, sem restrição ao acesso ou uso desses recursos e constituem um intricado ecossistema de aplicações descentralizadas (DApps). Contudo, transações nessas redes podem levar minutos para serem confirmadas dado o grande número de usuários que as submetem e o consenso distribuído realizado pelos nós mantenedores da rede para validar transações[1]. Esses nós têm direito de gerar novos ativos (ou moeda) e adquiri-los (mineração), assim como cobrar tarifa aos usuários por transação confirmada. Uma aplicação em rede pública requer um nó provedor de acesso para encaminhar transações requisitadas pelos seus usuários aos nós mantenedores. Existem provedores de acesso tais como a AWS[2] e Infura[3], que oferecem o recurso de blockchain com um serviço, porém o custo pode não ser apropriado para os requisitos da aplicação. Logo, o custo da aplicação consiste primordialmente no recurso computacional do nó provedor, ao passo que o usuário geralmente arca com a tarifa da transação.

Por sua vez, uma rede blockchain permissionada [Androulaki and et al. 2018] é uma alternativa atrativa para organizações que possuem infraestrutura e corpo técnico próprios, visando escapar de questões de custos (tarifação) e desempenho instáveis das redes blockchains públicas como Ethereum e Bitcoin [Sousa et al. 2021]. Hyperledger Fabric é uma das plataformas para blockchains permissionadas mais populares atualmente[4] com recursos para a implantação de uma infraestrutura de rede privada entre organizações e desenvolvimento de aplicações no topo dessa rede. Nesse caso, os participantes da rede formam um consórcio e arcam com o custo da infraestrutura, supondo que haveria ganhos no compromisso entre custo e desempenho em relação às redes blockchain públicas.

Nesse contexto, modelos que permitam analisar benefícios e custo das infraestruturas computacionais necessárias para implantação e o funcionamento de uma aplicação

[1]Desempenho da rede Ethereum em tempo real: https://etherscan.io

[2]https://docs.aws.amazon.com/blockchain-templates/

[3]https://infura.io

[4]https://www.ibm.com/topics/hyperledger

blockchain são essenciais para orientar o corpo técnico e executivo das organizações a planejarem uma possível adoção da tecnologia blockchain. Esses atores necessitam avaliar as opções de rede pública ou privada e o problema em questão é entender o impacto desses dois modelos no consumo de recursos computacionais e por conseguinte identificar a infraestrutura com melhor compromisso entre desempenho e custo para a aplicação blockchain.

A maioria das propostas da literatura que lidam com essa questão focam na aplicação para rede pública [Leal et al. 2020, Rouhani and Deters 2017, Zhang et al. 2020] ou rede permissionada [Baliga et al. 2018, Thakkar et al. 2018, Wang and Chu 2020, Xu et al. 2021]. Poucos trabalhos ainda focam na análise de uma aplicação típica para ambas as redes [Monrat et al. 2020, Malik et al. 2019]. Contudo, nenhuma desses propostas buscam identificar a infraestrutura que leva ao melhor desempenho, considerando ao mesmo tempo o fator custo para redes públicas e permissionadas.

Neste artigo buscamos preencher essa lacuna, propondo um modelo para estimar o custo da infraestrutura por transação confirmada na blockchain, considerando redes públicas e permissionadas. Para isso, analisamos a relação entre o custo monetário do recurso computacional necessário para executar uma aplicação blockchain típica e a vazão máxima obtida por esse recurso em transações por segundo. Desenvolvemos uma aplicação para inserção e consultas de registros em blockchain seguindo padrões de projeto gerais que atendem à plataforma Ethereum e Hyperledger Fabric simultaneamente [Xu et al. 2017]. Em seguida, conduzimos experimentos realistas para avaliações quantitativas sob o modelo proposto aumentando gradativamente o poder dos recursos computacionais e a carga de trabalho imposta à aplicação. Dessa forma exploramos o melhor compromisso entre custo e desempenho para várias infraestruturas executarem aplicações blockchain em redes públicas ou permissionadas via uma única métrica que é o custo por transação.

Nossos resultados experimentais, apresentados na Seção 4, foram baseados no modelo e metodologia aqui propostos. Eles mostram que o processamento, isto é, uso de CPU é o recurso mais crítico e que necessita ser cuidadosamente administrado na infraestrutura computacional para blockchains. Por sua vez, os valores obtidos nos resultados demonstraram a variação do uso de CPU e vazão em função do aumento da carga de trabalho. Por exemplo, quando o uso de CPU alcança valores próximos ou iguais a 100%, independente da infraestrutura utilizada, temos uma baixa vazão. Sendo que estes valores foram observados para cargas de trabalho maior. Do ponto de vista de modelagem, pudemos demonstrar o compromisso entre custo e desempenho mais adequado para escolha da infraestrutura.

Em suma, esse artigo traz duas contribuições relevantes: (i) um modelo de custo por transação para aplicações em redes blockchain pública e permissionada, considerando simultaneamente o desempenho máximo em função da infraestrutura e carga de trabalho imposta, e (ii) uma avaliação experimental que aplica esse modelo em diferentes tipos de infraestrutura e evidencia a melhor compromisso entre custos e benefícios para aplicações Ethereum e Hyperledger Fabric, respectivamente as redes públicas e permissionadas mais populares atualmente.

As próximas seções desse artigo têm a seguinte organização. Na Seção 2, apresen-

tamos os trabalhos relacionados ao uso de blockchain para aplicações médicas. Descrevemos o nosso modelo para analisar custo por transação em blockchain pública e permissionada na Seção 3. Na Seção 4 mostramos nossa metodologia e conduzimos avaliações experimentais considerando o modelo proposto. Discutimos nossos resultados na Seção 5 e apresentamos nossas considerações finais na na Seção 6.

2. Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados à avaliação de custos e desempenho de plataformas Blockchains.

O trabalho desenvolvido por [Rimba et al. 2020] investigou a questão do custo monetário de utilizar uma plataforma blockchain em comparação com uma infraestrutura de armazenamento em nuvem. Por meio de modelos de custo para processos de negócios eles compararam os custos na plataforma Ethereum e Amazons Simple Workflow Service (SWF). Os resultados apontaram uma grande variação de custo entre as duas soluções. Sendo que o custo do blockchain Ethereum é, pelo menos, o dobro dos serviços tradicionais de nuvem fornecidos pelo Amazon SWF. Nosso trabalho se diferencia ao apresentar um modelo de custo para comparação da infraestrutura necessária para manter o provimento da plataforma blockchain, sendo ela pública ou permissionada.

[Baliga et al. 2018, Thakkar et al. 2018, Wang and Chu 2020] analisaram o desempenho da plataforma Hyperledger Fabric. A abordagem de [Baliga et al. 2018] utilizou a ferramenta Hyperledger Caliper sob diferentes configurações para avaliar a latência e a taxa de transferência do hyperledger fabric. Avaliaram também o desempenho variando o número de *chaincodes*, *channels* e *peers*. Concluíram que a taxa de transferência é sensível às configurações e que a latência é significativamente afetada pelo tamanho da carga experimentada. [Thakkar et al. 2018] testou duas abordagens para avaliação de desempenho, otimização de cache e configuração de políticas de endosso. Como contribuição, os autores descreveram orientações sobre a configuração de parâmetros da rede e também os principais gargalos de desempenho. Nos estudos de [Wang and Chu 2020], os autores caracterizaram o desempenho de cada fase do ciclo de vida de uma transação, sendo que a fase de execução mostrou boa escalabilidade de desempenho em políticas de endosso específicas. A fase de validação obteve desempenho pior porque a carga de trabalho de computação do nó de validação é pesada. Os resultados mostraram que o principal fator de desempenho foi a política de endosso, ou seja, quantos pares tiveram que aprovar uma transação.

Os artigos [Leal et al. 2020, Rouhani and Deters 2017, Zhang et al. 2020] fornecem avaliação de desempenho de redes blockchain privadas baseadas na plataforma blockchain Ethereum de código aberto. [Leal et al. 2020] avaliam o desempenho da rede utilizando um conjunto de dados para encontrar uma configuração ideal. Utilizaram diferentes custos, algoritmos de consenso, e número de nós de rede para determinar a configuração. Como contribuição é fornecida uma forma para encontrar uma configuração ideal para um determinado número de transações exigidas por um caso de uso. O trabalho de [Rouhani and Deters 2017] mostrou que o desempenho da rede Ethereum depende, além da configuração da rede, da implementação do cliente utilizada. O estudo mostra que o cliente Parity obteve desempenho significativamente melhor do que o cliente Geth.

Em [Choi and Hong 2021], os autores utilizaram o Hyperledger Caliper para avaliar a rede Ethereum. Os resultados mostram que o desempenho das transações pode diferir de acordo com seu conteúdo e configuração da rede.

Existem alguns estudos de análise de desempenho Blockchain, que avaliam e comparam as plataformas Hyperledger Fabric e Ethereum. Em [Monrat et al. 2020] é realizada uma análise de desempenho e escalabilidade, variando as cargas de trabalho, das plataformas Ethereum, Quorum, Corda e Hyperledger Fabric. A conclusão geral do trabalho é que o Hyperledger Fabric tem um desempenho superior às demais plataformas porque atinge o consenso de forma mais eficiente. Em [Malik et al. 2019] é realizada uma comparação do desempenho das plataformas Ethereum e Hyperledger Fabric utilizando uma aplicação de comércio de energia e Hyperledger Caliper. A conclusão é que o Ethereum fornece a melhor solução para a aplicação em pequena escala, mas, o Hyperledger Fabric pode ser mais adequado para aplicações de grande escala.

3. Modelo de custo por transação

Nesta seção serão apresentados o modelo de custo por transação e a as arquiteturas de redes públicas e permissionadas.

3.1. Custo por Transação

Propomos um modelo que estima o custo por transação considerando uma aplicação da tecnologia blockchain típica para inserção e consulta de registros em uma rede pública ou permissionada. Esse modelo tem o objetivo de encontrar uma rede com uma infraestrutura de custo mínimo ($custo_{ideal}$) que alcança a vazão máxima (t_{ideal}) para a carga de trabalho avaliada. Nesse sentido, formalizamos o modelo com as definições a seguir.

A carga da rede é definida por w e ser valor é informado no modelo como as cargas de trabalho submetidas às redes, onde cada carga representa um conjunto de registros emitidos por um determinado tempo, i.e., transações por segundo (tps). Também é informado um conjunto de tipos de recursos computacionais disponíveis. Este conjunto é definido por R e tem-se o tipo de recurso caracterizado por: $r_i = (cpu_i, memória_i, custo_i) \in R$. Considera-se uma rede blockchain B composta de nós com configuração uniforme: $B = r_i \in R$. A função $Max\_Vazão$ retorna o conjunto de todas as vazões máximas t_i para cada tipo de recurso r_i como nó $b \in B$. Onde $Max\_Vazão(R, w, B) = T$. Obtém-se o conjunto alvo A, em que a porcentagem de uso dos recursos computacionais está abaixo do limite L, definido em comum acordo pelos participantes da rede. $A = \{uso(r_i) \leq L | r_i \in T\}$ A função $Min\_Custo(A)$ retorna o recurso com menor custo para a carga w em A, onde r_{ideal} representa o recurso com $custo_{ideal} \in A$ e também a vazão máxima $t_{ideal} \in A$. Dada por:$Min\_Custo(A) = r_{ideal}$. Por fim, o custo de uma transação na blockchain B para a carga w considerando o conjunto de tipos de recursos computacionais R é dado pela Equação 1.

$$C_{trans} = \frac{custo_{ideal}}{t_{ideal}} \tag{1}$$

3.2. Arquiteturas Blockchain Pública e Permissionada

Nesta seção descrevemos dois padrões de arquiteturas utilizadas nesse artigo representativas para redes blockchain pública e permissionadas. Primeiramente, mostramos a arquitetura do Ethereum, que atualmente se destaca como a segunda maior rede blockchain pública mundial em captação de recursos financeiros e número de contratos inteligentes. A seguir, mostramos a arquitetura da plataforma Hyperledger Fabric, que vem se destacando como um dos maiores projetos de código fonte aberto para desenvolvimento de redes blockchain permissionadas.

Ethereum : A arquitetura que empregamos para avaliação de custos da rede pública utiliza nós privados Ethereum. Estes nós são configurados a partir do *Geth*, que é a implementação oficial do protocolo da rede Ethereum. Assim, pode ser criada uma instância da rede Ethereum com múltiplos nós sem conexão com a rede principal ou com redes de teste para execução de experimentos ou utilização de forma privada. A Figura 1 apresenta o modelo de arquitetura da rede Ethereum com um nó minerador e um nó Validador, que provê acesso para as aplicações e a qual utilizamos.

Figura 1. Modelo de Blockchain privado.

O nó minerador é responsável pela mineração de transações e é quem gera os blocos que encadeiam e armazenam estas transações. A garantia da integridade e veracidade das informações também é realizada pelo nó minerador por meio do algoritmo de consenso nele implementado. Os blocos minerados serão então propagados para todos os nós pertencentes à rede. O nó Validador, por sua vez, mantém cópia de cada bloco minerado. Os nós Validadores expõem conexões através de portas definidas por métodos e padrões *Remote Procedure Call* (RPC) para prover o acesso dos clientes da aplicação à rede.

Hyperledger Fabric : A implantação da rede blockchain permissionada segue as especificações da plataforma Hyperledger Fabric[5] e possui dois componentes físicos básicos: *nó pareador* e o *nó ordenador*. Cada nó pareador representa uma organização participante da rede com as tarefas de emitir e validar objetos da blockchain. Para isso o nó pareador possui os módulos *ledger*, que registra transações; *CouchDB* que registra o estado global dos objetos (registro de ativo digital); contrato inteligente que é o programa em que implementamos as transações e os estados dos objetos[6]; e o serviço de autenticação dos participantes, que por padrão utiliza o mesmo protocolo de certificados digitais (X.509).

Por sua vez, o nó ordenador é um membro neutro da rede, e deve ser mantido por todas as organizações participantes. Ele é responsável por receber transações dos nós pareadores, organizar as transações em blocos, e retransmitir esses blocos a todas as organizações participantes (nós pareadores) para validarem as transações, conforme programado no contrato inteligente. A plataforma Hyperleger Fabric, por padrão, utiliza o

[5] *https://hyperledger-fabric.readthedocs.io/en/release-2.2/key_concepts.html*

[6] No Hyperledger Fabric os contratos inteligentes são denominados *chaincode*.

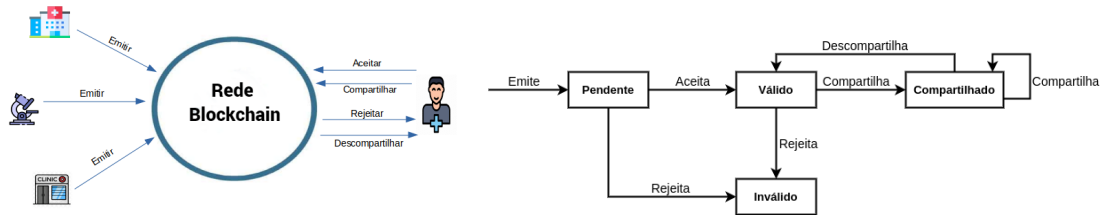
protocolo de consenso tolerante a falhas bizantinas (BFT). Esse protocolo garante a consistência da blockchain em todas as organizações, i.e., elas possuem cópias idênticas do *ledger* e cada objeto emitido possui o mesmo estado global [Androulaki and et al. 2018].

4. Metodologia e Experimentos

No modelo de custo apresentado, é necessário identificar a vazão máxima suportada em redes blockchain com infraestruturas diferentes, especificamente, redes cujos nós tenham recursos computacionais de diferentes capacidades. Nesta seção discutimos a metodologia utilizada para determinar a vazão máxima empiricamente. Primeiramente, a aplicação blockchain típica para condução dos experimentos é apresentada e, a seguir, o ambiente experimental e ferramentas são descritos.

4.1. Aplicação Blockchain Típica

Neste trabalho, utilizamos uma aplicação blockchain típica, que é o compartilhamento e gerenciamento de registros médicos eletrônicos (EMR), implementado em *Smart Contract* e *Chaincodes* para as plataformas blockchain Ethereum e Hyperledger Fabric. Esse modelo de aplicação pode ser utilizado em vários outros contextos pelos devidos aspectos: (i) armazenamento *offchain*, i.e., a blockchain armazena um resumo do registro no formato de um *hash* criptográfico para fins de rastreabilidade e auditabilidade, e (ii) dados completos dos registros são mantidos pelas organizações com permissões de acessos definidas pelos donos dos registros (e.g., pacientes). Dessa forma exploramos blockchain como uma camada de conexão entre diferentes organizações, unificando aspectos comuns de redes blockchains públicas e permissionadas, i.e., baixo custo de armazenamento (dados *offchain*) e integração com sistemas já existentes [Xu et al. 2017].



(a) Participantes da rede e suas transações (b) Estados do objeto após transação

Figura 2. Visão geral da aplicação blockchain.

O diagrama da Figura 2(a) mostra alguns participantes modelados em nossa aplicação. Cada relacionamento entre paciente e uma organização gera um EMR que é armazenado em sistemas usuais das organizações de saúde. Na solução proposta, o EMR se torna um *objeto* registrado na blockchain como um resumo criptográfico na forma de *hash*.[7] Por sua vez, os *hashes* de EMRs na blockchain são passíveis de comprovação da sua autenticidade por todos os participantes via as propriedades de segurança da blockchain [Greve et al. 2018].

A Figura 2(b) ilustra a modificação no estado dos *objetos* a partir das transações da aplicação. Para registrar um EMR na blockchain a organização armazena o EMR completo na sua base de dados local, em seguida, o *hash* do EMR é armazenado na blockchain,

[7]O algoritmo *SHA256* foi utilizado para gerar o *hash*, mas outros algoritmos podem ser utilizados.

assumindo o estado *pendente*, ou seja, esperando a confirmação do paciente. Neste estado, o EMR não pode ser acessado por outras organizações da rede. A seguir, o paciente é notificado do registro na blockchain e deve responder, confirmando ou rejeitando tal transação. Após a confirmação do paciente, o estado do EMR é atualizado na blockchain, caso seja confirmado outras organizações podem requisitar o acesso ao EMR do paciente, o contrário se o estado for rejeitado.

4.2. Ambiente Experimental e Métricas

Cargas sintéticas para a aplicação blockchain típica apresentada foram geradas com foco na transação de emissão de EMR, i.e., inserção de registros, que é usualmente a operação com maior uso de recursos computacionais e atrasos em blockchains como já observado em trabalhos anteriores [Spengler and Souza 2021]. Nesse sentido, a ferramenta de aferição *Caliper* [Caliper 2019] foi utilizada para gerar cargas com emissão de EMRs. Diferentes cargas de trabalho foram submetidas às redes, onde cada carga representa um conjunto de registros emitidos por segundo, i.e., transações por segundo (tps), de forma fixa em um dado período de tempo aqui chamado por rodada. O valor em tps das cargas de trabalho foram aumentadas gradativamente até ser atingido o ponto de saturação da rede em que todas as transações submetidas falham.

Quatro tipos de recursos computacionais foram utilizados para executar os experimentos nas redes blockchain pública e permissionada. Esses tipos são máquinas virtuais (VMs) do serviço *Amazon Elastic Cloud Computing* (EC2) para compor os nós de cada rede, e aumentamos gradualmente o poder computacional desses nós para analisar o desempenho da rede em função do aumento de carga. Nesse sentido, foram utilizadas as VMs T2 do tipo *small, medium, xlarge* e *2xlarge*, cujas respectivas especificações são apresentadas na Tabela 1. A plataforma Hyperledger Fabric (rede permissionada) foi configurada com o *Minifabric*, uma ferramenta para implementação dessa rede. Configuramos a rede com quatro nós pareadores e um nó ordenador, sendo que o *Minifabric* inicia a rede com um nó ordenador e dois nós pareadores em uma única VM. As cargas foram submetidas por dois clientes Caliper, cada cliente utilizando um nó pareador em VMs separadas. Para a plataforma Ethereum (rede pública) foi configurado um nó minerador em uma VM exclusiva, um nó validador para prover acesso à rede em outra VM, e um cliente Caliper em outra VM que realizou a submissão de transações.

	Small	**Medium**	**xLarge**	**2xLarge**
vCPUs	1	2	4	8
Memória (GB)	2	4	16	32
Custo/hora (USD)	0,0230	0,0464	0,1856	0,3712

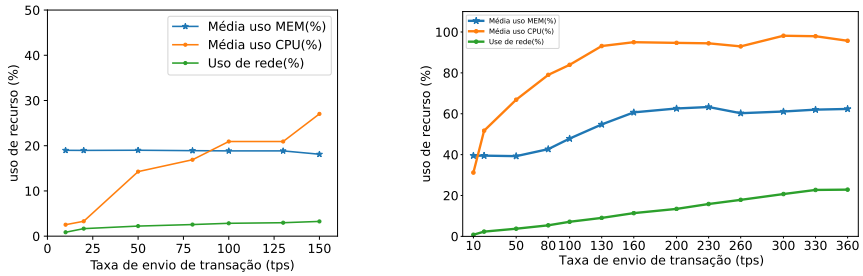
Tabela 1. Especificações dos nós que compõem cada tipo de infraestrutura: família AWS T2, processador Intel Xeon 3.0-3.3 GHz e disco SSD de 100 GB.

Para cada carga de trabalho executada foram medidos a vazão da rede em tps e o atraso da transação, além da medição do uso dos recursos processamento (CPU), memória, disco e rede para os nós da rede. O Caliper registra o instante de envio e de confirmação (sucesso ou falha) para cada transação. Assim, a vazão é calculada pela taxa de total de transações com sucesso sobre o período total da carga aplicada, i.e., a diferença entre o instante da última confirmação e o instante da primeira submissão. Por sua vez, o uso dos recursos computacionais foram coletados em granularidade de segundos via a

biblioteca *Psutil) versão 5.9.0*. Está biblioteca é multiplataforma e tem como finalidade o monitoramento de processos e sistemas em Python. Desenvolvemos um script utilizando a biblioteca *Psutil)* e instalamos em cada nó da rede para coletar os dados referentes aos recursos monitorados.

No modelo de custo apresentado (Seção 3), é necessário identificar a vazão máxima suportada em redes blockchain com recursos computacionais diferentes, especificamente, redes cujos nós tenham as capacidades apresentadas na Tabela 1. Intuitivamente o crescimento da vazão está associado ao aumento do consumo de recursos computacionais, assim como a super utilização desses recursos pode levar à limitação da vazão. Nesse sentido, foi examinado quais recursos do nó são mais consumidos com o aumento da carga na rede blockchain, indicando a vazão máxima que pode ser alcançada nessa rede por contenção desses recursos.

A Figura 3 (a) e (b) mostra o consumo médio de CPU, memória e rede[8] para cargas sintéticas submetidas sobre as redes Ethereum e Hyperledger Fabric construídas com nós do tipo *medium* com a finalidade de observar quais desses recursos são mais requisitados, preliminarmente ao início dos experimentos. Como pode ser observado, CPU é o recurso que tem o uso mais impactado com os aumentos de carga, i.e., a taxa do envio de transações, ao passo que o uso de memória permanece estáveis e o uso da rede (entrada e saída) cresce em relação à sua capacidade máxima (1 Gbps) mas não tão significativamente quanto CPU. Portanto, o foco deste trabalho é no uso de CPU para identificar a vazão máxima nos quatro tipos de infraestruturas para as redes blockchain, e estabelecemos o limite de 100% de uso de CPU para o conjunto de infraestrutura alvo.



(a) Ethereum (b) Hyperledger Fabric

Figura 3. Uso de recursos CPU, memória e rede.

5. Resultados

Nesta seção apresentamos os resultados. Primeiramente serão apresentados os melhores desempenhos alcançados pelas diferentes infraestruturas avaliadas para a aplicação nas redes pública e permissionada. A seguir, será incluído o fator custo, analisando a melhor relação entre custo e desempenho observada para as infraestruturas avaliadas.

[8]Disco foi omitido dessa análise visto que a aplicação típica proposta para a avaliação foca no armazenamento *offchain*, como descrito na seção anterior.

5.1. Avaliação de Desempenho

Foram executados diversos experimentos com redes blockchains pública (Ethreum) e permissionada (Hyperledger Fabric) implantadas em nós com crescimento gradativo da infraestrutura computacional, representada por CPU, e também sob cargas de trabalho crescentes, conforme a metodologia descrita na seção anterior.

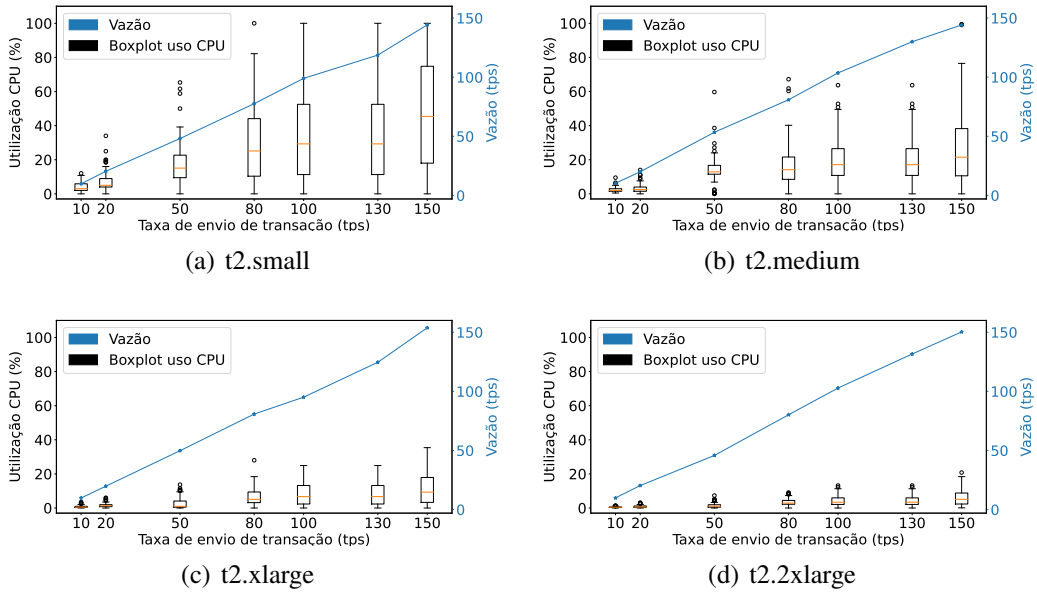
As Figuras 4 e 5 mostram a variação de uso de CPU e a vazão em função da carga de trabalho em transações por segundo (tps) para as medições observadas nas redes pública e permissionada respectivamente com os quatro tipos de infraestruturas. As figuras apresentam *boxplots* para sumarizar a distribuição dos usos de CPU no eixo y principal da seguinte forma: o retângulo central se expande entre o primeiro e terceiro quartil, o segmento interior é a mediana, enquanto os indicadores abaixo e acima do retângulo representam o 10^{o} e 90^{o} percentis. Por sua vez, as curvas em azul mostram a evolução da vazão em tps no eixo y secundário.

A Figura 4 apresenta resultados observados para a rede blockchain pública, i.e., a aplicação na plataforma Ethereum. De modo geral, nota-se que a variação do uso de CPU cresce com o aumento da carga de trabalho, visto pelas expansões consecutivas dos boxplots entre o 10^{o} e 90^{o} percentis, que correspondem a 80% das medições. A vazão também cresce com o aumento da carga de trabalho. As medições foram limitadas até a carga de 150 tps, que é o valor máximo suportado pelo cliente Ethereum utilizado sem perdas de transações. O foco dos experimentos está na avaliação de desempenho e na infraestrutura ideal para a aplicação cliente. Logo, a rede blockchain Ethereum foi construída com um nó minerador, de modo a não limitar a vazão pelo mecanismo de consenso distribuído entre vários mineradores, como ocorre na rede Ethereum principal (*mainnet*). Dessa forma pode-se observar o impacto da infraestrutura computacional, i.e., o uso de CPU, na vazão da aplicação cliente.

Ao observar os quatro tipos de infraestruturas mostrados na Figura 4, nota-se que o tipo *small* sofre a maior variação de uso CPU em relação aos tipos *medium, large* e *2xlarge*. Logo, o cliente Ethereum, em infraestrutura do tipo *small*, pode enfrentar instabilidades que comprometam a vazão para cargas superiores a 100 tps. Isso porque uma parcela relevante das medições tiveram 100% do uso de CPU como indicada a marca do 90^{o} percentil, i.e., 10% das medições. Por outro lado, os outros três clientes com maior poder computacional alcançam cargas de até 150 tps com estabilidade, i.e., menor variação, do uso de CPU, e raramente alcançam 100% de uso de CPU. Nesses casos, foi observado apenas uma amostra de medição para o cliente do tipo *medium* com 100% de uso de CPU em carga com 150 tps.

Agora discutimos os resultados observados para a rede blockchain permissionada, i.e., a aplicação na plataforma Hyperledger Fabric, mostrados na Figura 5. É notável o maior uso de CPU no nó Hyperledger Fabric, o que leva a maior variabilidade e saturação desse recurso para cargas bem menores ao observado anteriormente. Por exemplo, uma carga de 10 tps já leva o nó do tipo *small* a alcançar 100% de processamento em cerca de 10% das medições, como indica a marca do 90^{o} percentil. Isso ocorre porque o nó da rede permissionada atua não apenas como um cliente recebendo transações dos usuários, mas também validando as transações dos demais nós da rede.

A vazão medida na rede permissionada foca nas transações submetidas por nó



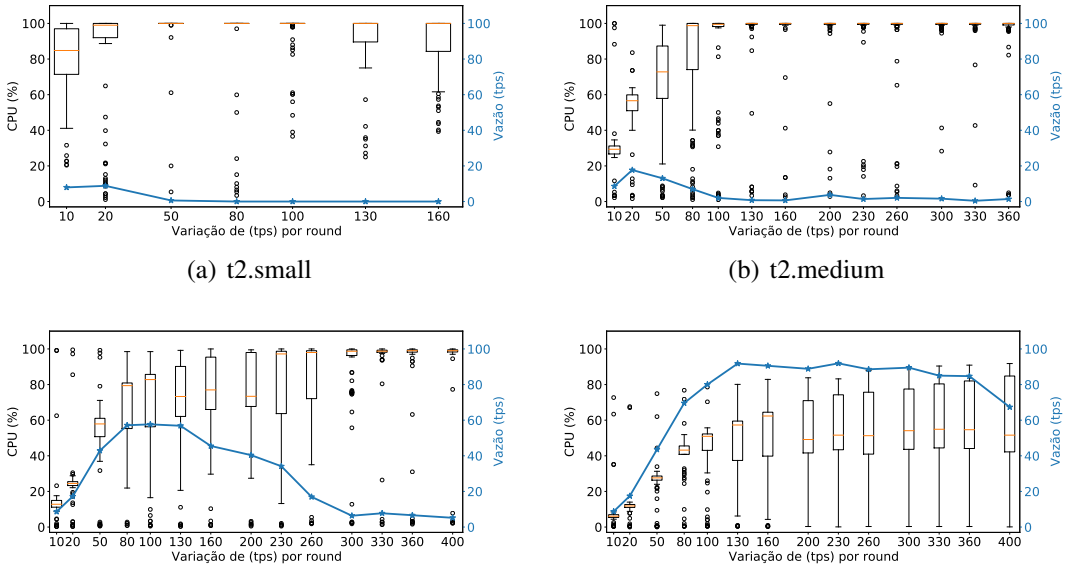
(a) t2.small (b) t2.medium

(c) t2.xlarge (d) t2.2xlarge

Figura 4. Uso de CPU e vazão em rede pública Ethereum.

(visão local) e não o total de transações da rede. Contudo, o nó usa recursos computacionais para validar transações de toda a rede o que levou a vazões menores que as observadas na rede pública. Em nossos experimentos, submetemos cargas de até 400 tps para a rede construída com nós do tipo *large* e *2xlarge*, mostrados respectivamente nas Figuras 5 (c) e (d). Observamos nesses casos, desempenhos satisfatórios com perdas zero ou inferiores a 1% do total de transações e vazões com comportamento ligeiramente linear para cargas de trabalho até 80 tps. Por outro lado em cargas superiores a essa, observa-se que o desempenho das redes alcançam um estágio de perda (i.e., decaimento da vazão). Essas perdas coincidem com a alta utilização de CPU em infraestruturas do tipo *small, medium e 2xlarge*, que visivelmente demonstram a saturação de suas CPUs dado certos graus de aumento de carga. Nas infraestruturas do tipo *2xlarge*, diferentemente, as perdas de desempenho decorrem da comunicação entre os nós da rede para validar transações, que segue o consenso BFT, usual nas redes blockchain permissionadas.

Ao observar os quatro tipos de infraestruturas mostrados na Figura 5, nota-se que o tipo *small* não seria adequado para nós de uma rede permissionada Hyperledger Fabric como já discutido acima. Nos resta então analisar os demais tipos *medium, large e 2xlarge*. Seguindo o mesmo critério de escolha da infraestrutura adequada (i.e., 100% de uso de CPU abaixo do 90o. percentil), concluímos que o nó Hyperledger Fabric pode enfrentar instabilidades que comprometam a vazão para cargas superiores a 20 tps em infraestrutura do tipo *medium* e cargas a partir de 80 tps para o tipo *xlarge*. Por sua vez, na infraestrutura do tipo *2xlarge*, não foram observadas instabilidades devido recursos computacionais. Logo, conjecturamos que o aumento de vazão nesse caso estaria mais relacionado ao protocolo de consenso distribuído adotado pela rede permissionada, cuja avaliação está fora do escopo desse trabalho.



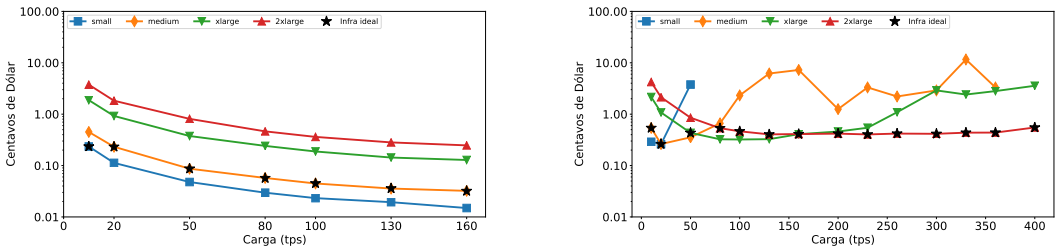
(a) t2.small (b) t2.medium

(c) t2.xlarge (d) t2.2xlarge

Figura 5. Uso de CPU e vazão em rede permissionada Hyperledger Fabric.

5.2. Compromisso entre Custo e Desempenho

Agora incluímos o fator custo para os desempenhos das redes para os quatro tipos de infraestruturas analisadas na seção anterior. A Figura 6 (a) e (b) mostra o custo por transação da aplicação típica nas redes pública (Ethereum) e permissionada (Hyperledger Fabric) em função da carga de entrada dada em tps. O custo por transação representa a relação entre o custo da infraestrutura por hora e a vazão da rede para a carga aplicada. Para melhor visualização as figuras mostram o custo por transação em centavos de dólar (e.g., US$ 0,01 tem valor unitário 1,0 no eixo y) em escala logarítmica. Adicionalmente, foi incluída a marca (estrela) para recomendar a infraestrutura ideal, i.e., o compromisso entre custo e desempenho mais adequado de acordo com o modelo proposto na Seção 3. Em outras palavras, a recomendação foca primeiramente no uso adequado dos recursos computacionais do nó, mostrado na seção anterior, e a seguir, foca no menor custo. Logo, o tipo de infraestrutura com menor custo não é sempre recomendada nessa análise.



(a) Ethereum (b) Hyperledger Fabric

Figura 6. Custo por transação para cada tipo de infraestrutura por hora de uso: asteriscos indicam a recomendação de infraestrutura ideal considerando o compromisso entre custo e desempenho.

A Figura 6(a) mostra uma tendência de redução do custo por transação na rede pública para as quatro infraestruturas à medida em que se aumenta a carga. Essa tendência reflete o bom desempenho observado para a aplicação típica na rede Ethereum. É importante observar que essa aplicação obteve uma vazão próxima à carga nos experimentos (Figura 4). No entanto, cargas altas são impraticáveis na rede pública principal do Ethereum com o protocolo de consenso atual, que alcança vazão em torno de 13 tps[9] independente da carga na rede. As recomendações de infraestrutura para o cliente Ethereum que executa a aplicação inicia com o custo por transação em 0,23 e alcança 0,03 centavos de dólar para nó do *small* e se mantém nessa faixa com nó do tipo *medium*. Considerando os experimentos até 20 tps, que é equivalente ao cenário atual, o custo da transação na rede pública se aproxima ao observado para a rede permissionada, que será discutida a seguir.

A Figura 6(b) apresenta o custo da transação na rede permissionada. Notavelmente, esse custo é maior ao observado na rede pública dado que o nó que executa a aplicação Hyperledger Fabric também valida transações de outros nós, i.e., o participa do consenso distribuído BFT adotado na rede permissionada. Logo, o consumo de recursos computacionais dos nós é maior nessa rede e, adicionalmente, há comunicação e espera entre os nós na realização do consenso. Em consequência, só foi possível calcular o custo de transação para as cargas submetidas na rede com nós *small* e *medium* até 50 e 350 tps, respectivamente. Todos esses aspectos contribuem para o decaimento da vazão em função da carga observada nos experimentos (Figura 5). Portanto, há uma tendência de aumento do custo da transação, como mostram as curvas representando cada tipo de infraestrutura na Figura 6(b). Nesse caso, a recomendação de infraestrutura ideal é importante, pois mostra que aumentar o poder computacional dos nós face ao aumento de carga mantém o custo por transação razoavelmente estável. Observe na figura que a rede foi iniciada com nós do tipo *medium*, modificada para nós *xlarge* em cargas de 80 tps e, novamente, modificada para nós *2xlarge* em cargas a partir de 100 tps. Ao longo dessas modificações o custo por transação foi mantido entre 0,54 e 0,55 centavos de dólar do início ao fim dos experimentos, respectivamente.

6. Conclusão

Neste artigo, propusemos uma avaliação da infraestrutura blockchain, necessária para prover acesso de aplicações à rede, traçando uma comparação de desempenho entre as plataformas Ethereum e Hyperledger Fabric. Avaliamos por meio de um modelo de custo por transação para aplicações em redes blockchain pública e permissionada, considerando simultaneamente o desempenho máximo em função da infraestrutura e carga de trabalho imposta. Realizamos um experimento com a implementação de aplicações nas duas plataformas para aplicarmos o modelo em diferentes tipos de infraestrutura. Como resultado, fornecemos um modelo capaz de estimar o custo da infraestrutura por transação confirmada na blockchain, considerando redes públicas e permissionadas. A partir do modelo proposto, nossos resultados mostraram os limites de escalabilidade dessas redes e os compromissos entre custo e desempenho para aplicações blockchain.

[9] Vazão média da rede Ethereum medida pelo serviço http://etherscan.io em fevereiro de 2022.

Referências

Androulaki, E. and et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proc. of the EuroSys Conference*.

Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., and Chatterjee, S. (2018). Performance characterization of hyperledger fabric. *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, pages 65–74.

Caliper, H. (2019). Caliper. https://hyperledger.github.io/caliper. (Accessed on 09/23/2021).

Choi, W. and Hong, J. W. K. (2021). Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper. *22nd APNOMS 2021*, pages 325–329.

Greve, F., Sampaio, L., Abijaude, J., Coutinho, A. A., Brito, I., and Queiroz, S. (2018). Blockchain e a Revolução do Consenso sob Demanda. In *Proc. of SBRC Minicursos*.

Leal, F., Chis, A. E., and González–Vélez, H. (2020). Performance Evaluation of Private Ethereum Networks. *SN Computer Science*, 1(5):1–17.

Malik, H., Manzoor, A., Ylianttila, M., and Liyanage, M. (2019). Performance Analysis of Blockchain based SG with Ethereum and Hyperledger Implementations. *IEEE International Conference on ANTS*.

Monrat, A. A., Schelen, O., and Andersson, K. (2020). Performance Evaluation of Permissioned Blockchain Platforms. *IEEE, CSDE 2020*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Rimba, P., Tran, A. B., Weber, I., Staples, M., Ponomarev, A., and Xu, X. (2020). Quantifying the Cost of Distrust: Comparing Blockchain and Cloud Services for Business Process Execution. *Information Systems Frontiers*, 22(2):489–507.

Rouhani, S. and Deters, R. (2017). Performance analysis of ethereum transactions in private blockchain. In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*. IEEE.

Sousa, J. E. d. A., Oliveira, V., Valadares, J., Dias Goncalves, G., Moraes Villela, S., Soares Bernardino, H., and Borges Vieira, A. (2021). An analysis of the fees and pending time correlation in ethereum. *International Journal of Network Management*.

Spengler, A. C. and Souza, P. S. (2021). Avaliação de desempenho do hyperledger fabric com banco de dados para o armazenamento de grandes volumes de dados médicos. In *Proc. of WPerformance*.

Thakkar, P., Nathan, S., and Viswanathan, B. (2018). Performance benchmarking and optimizing hyperledger fabric blockchain platform. *Proceedings - IEEE, MASCOTS 2018*, pages 264–276.

Wang, C. and Chu, X. (2020). Performance characterization and bottleneck analysis of hyperledger fabric. *Proceedings - International Conference on Distributed Computing Systems*, 2020-Novem:1281–1286.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32.

Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., and Vasilakos, A. V. (2021). Latency performance modeling and analysis for hyperledger fabric blockchain network. *Information Processing and Management*, 58(1).

Xu, X., Weber, I., and Staples, M. (2019). *Architecture for blockchain applications*. Springer.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)*, pages 243–252. IEEE.

Zhang, L., Lee, B., Ye, Y., and Qiao, Y. (2020). Ethereum transaction performance evaluation using testnets. In *Euro-Par 2019: Parallel Processing Workshops*, Cham. Springer International Publishing.

Artigo submetido para o XIV Encontro Unificado de Computação do Piauí (ENUCOMPI) e XI Simpósio de Sistemas de Informação (SINFO) em 2021.

B-Drive: em Direção a Redes para Compartilhamento de Registros Médicos Eletrônicos via Tecnologia Blockchain*

Pedro Hércules Dantas[1], **Glauber Dias Gonçalves**[1], **Alex Borges Vieira**[2]

[1]Universidade Federal do Piauí - CSHNB

[2]Universidade Federal de Juiz de Fora - DCC

{pedrohercules, ggoncalves}@ufpi.edu.br, alex.borges@ufjf.edu.br

Abstract. *Blockchain is a disruptive technology that offers resources to reduce costs and bureaucracy in relationships between organizations, considering public, auditable and decentralized data records. There is a growing interest in new applications of this technology, in particular, for the control and sharing of electronic medical records (EMR). In this work, we propose B-Drive, a blockchain-based network infrastructure model for sharing EMRs between patients and various healthcare organizations. Different from existing approaches, our proposal considers a model of a permissioned network, patient-defined shares and integration of systems and infrastructures that already exist in organizations to deploy the blockchain network. Our results based on realistic experiments show the feasibility and minimum requirements for deploying a blockchain consortium for sharing EMRs.*

Resumo. *Blockchain é uma tecnologia disruptiva que oferece recursos para redução de custos e burocracia nos relacionamentos entre organizações, em especial no registro público, auditável e descentralizado de dados. Existe um crescente interesse por novas aplicações dessa tecnologia, em particular, para o controle de compartilhamentos de registros médicos eletrônicos (EMR). Nesse trabalho, propomos B-drive, um modelo de infraestrutura de redes baseado em blockchain para o compartilhamento de EMRs entre pacientes e as diversas organizações da área de saúde. Diferente das abordagens existentes, a nossa proposta considera um modelo de rede permissionada, compartilhamentos definidos por pacientes e integração dos sistemas e infraestruturas já existentes nas organizações para construção da rede blockchain. Nossos resultados baseados em experimentos realistas mostram a viabilidade e requisitos mínimos para implantação de uma rede blockchain para compartilhamento de EMRs.*

1. Introdução

Um registro médico eletrônico ou EMR (*electronic medical record)* é a versão digitalizada do tradicional prontuário médico, que inclui os principais dados clínicos administrativos relevantes para o cuidado do paciente, como medicamentos, progressos e exames [CMS 2012]. Para gerenciar diferentes tipos de dados em EMRs, existem padrões que especificam como os dados clínicos devem ser armazenados e tratados [OpenEHR 2003, HL7 2014]. Tais padrões possibilitam a interoperabilidade entre

*Essa pesquisa é financiada por CNPq/Amazon AWS (Processo 440069/2020-3) e PIBITI UFPI.

diferentes sistemas de informação em saúde. Um exemplo da utilização de tais padrões é a Rede Nacional de Dados em Saúde [RNDS 2020] mantida pelo governo federal, que adota o padrão FHIR para realizar a interoperabilidade de EMRs entre todas as unidades do sistema único de saúde (SUS).

Dado a existência de padrões bem estabelecidos para EMRs, uma questão pertinente é o desenvolvimento de ferramentas para controle, auditoria e compartilhamento desses dados. O armazenamento de EMRs de pacientes é um serviço crítico que pode gerar conflitos entre políticas de acessibilidade e privacidade desses registros. Geralmente, os pacientes precisam de cuidados de diferentes médicos em diferentes instituições que podem demandar compartilhamentos do histórico de EMRs. Todavia, esses dados nem sempre estão acessíveis para permitir troca de informações e interoperabilidade entre as organizações e seus especialistas como ocorre no SUS, que é centralizado no governo federal. No caso da rede privada de saúde pode haver conflito de interesses entre organizações concorrentes, além do receio das questões legais que envolvem o compartilhamento de dados sensíveis de pacientes. Logo, são necessárias ferramentas que garantam a inviolabilidade dos dados, a rastreabilidade de permissões para compartilhamentos e a integração entre sistemas de diferentes organizações.

Vários pesquisadores apontam blockchain como a tecnologia adequada para lidar com as questões de autenticidade, consistência e acessibilidade em sistemas de EMR [Azaria et al. 2016, Conceicao et al. 2018, Spengler and Souza 2021, Mendonça et al. 2021]. De forma simples, blockchain é um arcabouço para armazenar registros de forma imutável e verificável entre participantes de uma rede par-a-par (P2P) [Greve et al. 2018]. Nesse caso, uma estrutura de dados chamada *ledger* é utilizada para encadear blocos de registros via resumos criptográficos (*hashes*), o que permite fácil verificação de violabilidade. Por sua vez um mecanismo de consenso é utilizado para replicar os blocos do *ledger* de forma consistente entre todos os participantes da rede P2P.

A maioria das propostas da literatura para o gerenciamento de EMRs via blockchain [Azaria et al. 2016, Conceicao et al. 2018, Mendonça et al. 2021], como discutimos na Seção 2, utilizam o modelo da criptomoeda Ethereum, i.e., uma infraestrutura blockchain pública. Nesse modelo as organizações não têm a autonomia para integrar seus sistemas EMRs e reutilizar suas infraestruturas computacionais, havendo ainda a necessidade de pagar tarifas em Ether para registrar dados na blockchain, o que pode ser um custo inviável para pacientes e organizações. Visando escapar dessas questões, redes blockchains permissionada como a plataforma Hyperledger Fabric [Androulaki and et al. 2018] é uma alternativa atrativa para organizações que já investiram em infraestrutura, corpo técnico e sistemas de EMRs próprios. Contudo, modelar e implementar uma rede blockchain permissionada é uma tarefa complexa. De um lado há a modelagem do sistema de outro lado há a infraestrutura de rede. Poucos estudos debruçam sobre esse tema [Spengler and Souza 2021] e existem questões a serem investigadas em especial quanto ao desempenho da rede.

Neste artigo propomos um modelo de redes blockchain permissionadas para o compartilhamento de EMRs entre pacientes e várias organizações da área de saúde. Nossa proposta descrita na Seção 3 se diferencia das existentes em dois aspectos chave: (i) utilizamos o armazenamento *offchain*, i.e., a blockchain armazena metadados dos EMRs no formato de um resumo criptográfico (*hash*) para fins de rastreabilidade e auditabilidade de

compartilhamentos, e (ii) EMRs reais são mantidos pelas organizações com permissões de acessos definidas pelos pacientes. Dessa forma exploramos a tecnologia blockchain como uma camada de conexão entre os participantes de uma rede, i.e., um consórcio de organizações de saúde. Nossa abordagem une os aspectos positivos de redes blockchains públicas, i.e., baixo custo de armazenamento e transferência de dados e as redes permissionadas, i.e., utilização de infraestrutura própria e sistemas EMRs existentes.

Nossos resultados experimentais (Seção 4), baseados na implementação dessa rede na plataforma Hyperledger Fabric, mostram que o processamento (uso de CPU) é o recurso crítico que necessita ser cuidadosamente administrado. Por sua vez, recursos de memória, armazenamento e comunicação foram pouco exigidos dado a nossa proposta de dados *offchain*. Por exemplo, menos de 4GB de memória, 42 MBytes de disco e 250 Kbps foram o suficiente para emitir 400 EMRs por segundo sem perdas na blockchain. Do ponto de vista de modelagem, propomos o compartilhamento de EMRs via blockchain com um modelo simples mas ajustável a diferentes organizações, onde o EMR é um objeto com apenas cinco transações que modificam o seu estado global.

Em suma, esse artigo tem as seguintes contribuições: (i) um modelo baseado em blockchain que permite pacientes e organizações de saúde compartilharem EMRs sob permissões definidas pelos pacientes, e (ii) uma avaliação experimental para medir desempenho e custos da infraestrutura da rede blockchain.

2. Trabalhos Relacionados

MedRec [Azaria et al. 2016] é um trabalho seminal, dado que é uma das propostas pioneiras de sistema de gerenciamento de EMRs baseado em blockchain. Os autores propõem uma arquitetura onde pacientes e organizações da área médica armazenam registros médicos de forma imutável e acessível por ambas as partes na blockchain pública da plataforma Ethereum. Contudo, ao optar por essa plataforma as organizações não têm a possibilidade de configurar a blockchain da forma que lhes seria mais viável, especialmente quanto aos desempenho, componentes e protocolos da rede blockchain. Além disso, é necessário pagar tarifas para o processamento de transações em plataformas de blockchain públicas) o que pode ser um custo inviável para pacientes e organizações.

Em [Conceicao et al. 2018] foi proposto diretrizes gerais de sistemas de gerenciamento de EMRs baseados em blockchain com garantias de permissões a dados pessoais sensíveis compartilhados sob permissão do paciente. Estendendo MedRec, essa proposta possibilita que dados privados de pacientes estejam disponíveis a autoridades de saúde pública para lidar com epidemias e problemas de saúde pública. Nessa mesma linha, em [Mendonça et al. 2021] foi proposto uma estrutura para a utilização de blockchain no controle de acesso e compartilhamento de EMRs com foco em manter o controle de posse dos dados do paciente por meio de autorização e revogação de acessos às organizações. Os autores estendem o sistema Medrec com simplificações da arquitetura baseada em blockchain pública, e sua eficiência foi demonstrada via prototipação em laboratório. Por se basearem em infraestrutura pública, ambas as propostas estão sujeitas às mesmas questões acima mencionadas ao sistema Medrec [Azaria et al. 2016].

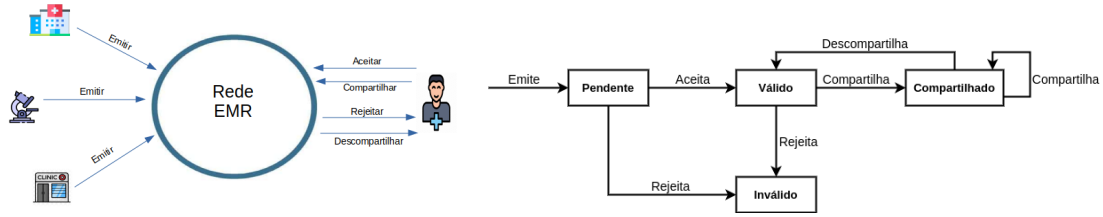
Mais relacionado ao nosso trabalho é o estudo recente [Spengler and Souza 2021], onde os autores propuseram um sistema de gerenciamento de EMRs baseado em redes

blockchain permissionadas com a plataforma Hyperledger Fabric. Nessa proposta, EMRs são armazenados na blockchain, o que pode levar riscos de perda de privacidade e violação de integridade caso seja necessário remover registros questões legais (e.g., lei geral de proteção de dados). Adicionalmente submissão de registros grandes ou sem padrões de tamanhos ocasionam perda de desempenho (latência e vazão), aumento do volume de armazenamento compartilhado entre os participantes da rede (i.e., custo). Nosso modelo de rede permissionada também usa Hyperledger Fabric, mas diferentemente dessa, exploramos o armazenamento *offchain* e integramos organizações via o compartilhamento de EMRs mantidos localmente com permissões de acessos definidas pelos pacientes.

3. Arquitetura da Rede EMR

Nesta seção descrevemos a nossa proposta de rede blockchain permissionada. Primeiramente mostramos a visão geral em termos de transações e objetos registrados na blockchain. A seguir, descrevemos a infraestrutura que permite a implementação da rede.

3.1. Visão Geral



(a) Participantes da rede e suas transações (b) Estados do objeto EMR após transação

Figura 1. Visão geral da rede EMR.

O diagrama da Figura 1(a) mostra os dois tipos de participantes modelados em nossa proposta. Na esquerda temos as organizações do ecossistema de saúde como hospitais, clínicas e laboratórios, e na direita temos o paciente que utiliza os serviços dessas organizações. Cada relacionamento entre paciente e organização gera um EMR que é armazenado em sistemas usuais das organizações de saúde. Em nossa rede, o EMR também se torna um *objeto* a ser registrado na blockchain na forma de resumo criptográfico (*hash*).[1] Além do *hash*, o objeto EMR contém os campos: ID da organização emissora do EMR, ID do paciente, marca de tempo, compartilhamento, e localização. O ID é a chave pública do participante que compõe a sua credencial na rede (código alfanumérico) juntamente à chave privada, essa última mantida secretamente pelo participante apenas para autenticações. O compartilhamento consiste em uma lista de pares (ID, expiração), que representa a organização que tem acesso ao objeto e a data de expiração do acesso. A localização, por sua vez, consiste em um endereço (e.g., link) onde o EMR pode ser acessado via as credenciais dos participantes com tal permissão.

A Figura 1(a) também ilustra as transações que podem ser realizadas pelos participantes da rede. Nesse caso, a organização emite o EMR, ao passo que o paciente

[1] Utilizamos o algoritmo *SHA256* para gerar o *hash*, mas outros algoritmos também podem ser utilizados.

o aceita ou rejeita, e adicionalmente compartilha ou descompartilha o EMR com outras organizações via autenticação com sua chave privada para cada transação. Por sua vez, a Figura 1 ilustra o estado do EMR após cada transação. Em nossa proposta, a transação *compartilha* se aplica apenas a objetos no estado *válido*, enquanto a transação *descompartilha* limpa a lista de compartilhamentos e retorna o objeto para o estado *válido*. Por sua vez, o ciclo de vida de um objeto finaliza quando o paciente rejeita a organização emissora indo para o estado *inválido* a partir dos estados *pendente* ou *válido*, o que significa desautorizar a organização a utilizar o EMR para qualquer finalidade.

A Figura 1(b) ilustra também a modificação no estado dos objetos a partir das transações. Sistemas baseados em blockchain, tipicamente, mantém o estado global dos objetos e os valores de seus respectivos campos, dado a última transação reliazada, em bancos de dados auxiliares (e.g., CouchDB, LevelDB) para aumentar a velocidade de acesso. Contudo, cada transação sobre esse objeto é registrada na blockchain para fins de auditabilidade e inviolabilidade dos dados [Greve et al. 2018].

É importante ainda observar que nossa proposta armazena metadados de EMRs (dados *offchain*), que são passíveis de serem comprovadas sua autenticidade por todos os participantes. Logo, exploramos a blockchain para estabelecer a inviolabilidade dos registros e o não repúdio da posse desses por parte das organizações que os possuem ou compartilham. A blockchain oferece provas digitais auditáveis para garantir o compartilhamento de dados entre organizações sem confiança mútua (e.g., concorrentes), e a judicialização entre as partes pelo vazamento ou uso indevido de EMRs.

3.2. Infraestrutura de Rede

Nossa implementação da rede blockchain permissionada segue as especificações da plataforma Hyperledger Fabric[2] e possui dois componentes físicos básicos: *nós pareadores* e o *nó ordenador*. Cada nó pareador representa uma organização participante da rede com as tarefas de emitir e validar objetos da blockchain. Para isso o nó pareador possui os módulos *ledger*, que registra transações; *CouchDB* que registra o estado global dos objetos; contrato inteligente que é o programa em que implementamos as transações e os estados dos objetos[3]; e o serviço de autenticação dos participantes, que por padrão utiliza o mesmo protocolo de certificados digitais (X.509).

Por sua vez, o ordenador é um membro neutro da rede, e deve ser mantido por todas as organizações participantes. Ele é responsável por receber transações dos nós pareadores, organizar as transações em blocos, e retransmitir esses blocos a todas as organizações participantes (nós pareadores) para validarem as transações, conforme programado no contrato inteligente. A plataforma Hyperleger Fabric, por padrão, utiliza o protocolo de consenso tolerante a falhas bizantinas (BFT). Esse protocolo garante a consistência da blockchain em todas as organizações, i.e., elas possuem cópias idênticas do *ledger* e cada objeto emitido possui o mesmo estado global [Androulaki and et al. 2018].

[2] *https://hyperledger-fabric.readthedocs.io/en/release-2.2/key_concepts.html*

[3] No Hyperledger Fabric os programas são chamados de *chaincode*.

4. Avaliação Experimental

Nessa seção descrevemos a avaliação da rede proposta. Primeiro descrevemos o seu funcionamento por meio de uma atividade entre paciente e organização típica que gera um EMR. A seguir, realizamos testes de carga na rede baseado nessa atividade para mostrar nossos resultados quanto ao uso de recursos computacionais e o seu desempenho.

4.1. Atividade Paciente-Organização Típica

Cada organização de saúde possui seu sistema proprietário para o gerenciamento de EMRs com banco de dados local para o armazenamento e uma interface de rede para acesso externo aos mesmos.[4] Por sua vez, o paciente pode utilizar um dispositivo pessoal *pendrive, smartphone* ou computador para autenticar na rede e gerenciar seus EMRs. Cada dispositivo é identificado por um par de chaves pública e privada, que são utilizados para autenticação assimétrica de registros médicos. Um participante ou organização pode ter vários dispositivos, ficando responsável pelas chaves de seus respectivos dispositivos.

Para armazenar um EMR na blockchain são seguidos alguns passos.[5] Primeiramente, a organização armazena o EMR completo na sua base de dados local. Em seguida, os metadados do EMR serão armazenados na blockchain, assumindo o estado *pendente*, ou seja, esperando a confirmação do paciente. Neste estado, o EMR não pode ser acessado por outras organizações da rede. A seguir, o paciente é notificado do registro na blockchain e deve respondê-la, confirmando ou rejeitando tal transação com o seu dispositivo fisicamente nas dependências da organização ou remotamente via aplicação em dispositivo móvel ou desktop. Após o retorno do paciente o estado do EMR será atualizado na blockchain, caso seja *confirmado* outras organizações podem requisitar o acesso ao EMR do paciente, o contrário se o estado for *rejeitado*.

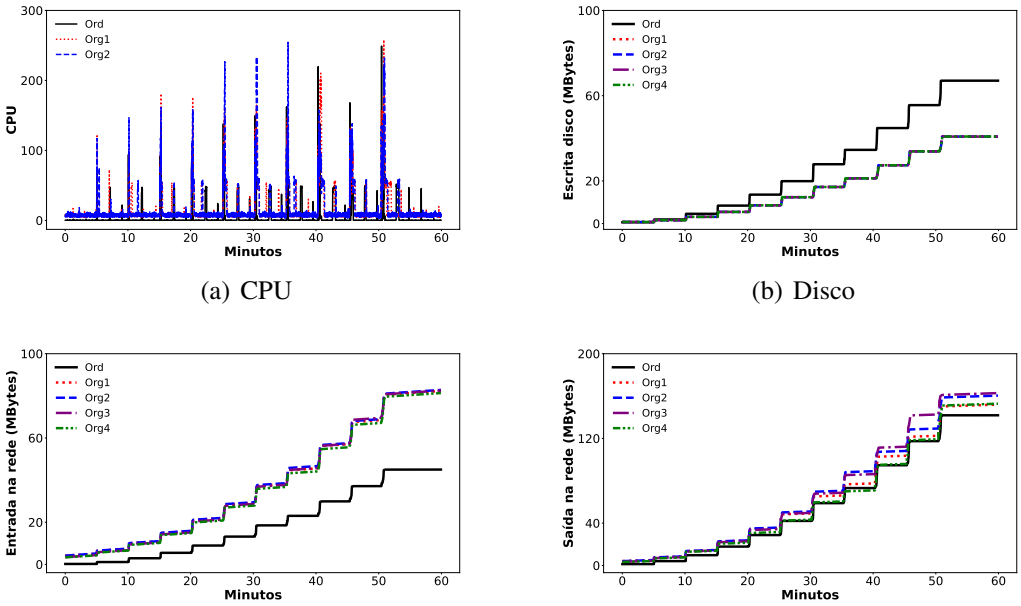
4.2. Resultados

Realizamos testes de carga na rede proposta, considerando quatro organizações participantes e emissão de vários EMRs, baseado na atividade acima, para observarmos o uso de recursos computacionais e o seu desempenho. Nesse sentido, planejamos um conjunto de dez cargas de trabalho submetidas à rede entre intervalos de cinco minutos. As cargas representam EMRs emitidos por segundo, i.e., transações por segundo (tps), que aumentamos gradativamente entre 100 até 1000 tps, ao passo de 100. Então medimos uso de processamento (CPU), memória, disco e rede em cada organização. Adicionalmente medimos a porcentagem de perda de transações para encontrar o ponto de saturação da rede, considerando a configuração padrão do Hyperledger Fabric. Conduzimos esses testes em um computador 4 CPUs Intel Xeon de 3.0 Ghz e 16 GB de memória RAM, considerando um nó ordenador e quatro nós pareadores, cada nó instalado em um *container docker*, e medimos o uso de recursos computacionais separadamente por *container*.

A Figura 2(a) mostra picos de processamento a cada carga de trabalho com um padrão nítido: um pico maior para a emissões de EMRs, i.e., inserções na blockchain e picos menores devido autenticações dos participantes na rede. Imediatamente, o pico de inserções ultrapassa 100% de processamento, cresce gradativamente e diminui a partir de 40 minutos, o que indica saturação da rede, i.e., perdas de inserções. O uso de memória,

[4]Código experimental: *https://github.com/PedroHercules/Fabric_EMR*.

[5]Diagrama: *https://github.com/PedroHercules/Fabric_EMR/blob/main/emissaoEmr.png*.



(a) CPU (b) Disco

(c) Rede Entrada (d) Rede Saída

Figura 2. Consumo de recursos computacionais e perdas de transações.

por sua vez, é baixo, e não ultrapassa 4% em todos os participantes (figura omitida por questão de espaço), ao passo que o uso de disco aumenta de forma cumulativa proporcionalmente à intensidade da carga (Figura 2(b)). Logo, observamos que memória e disco não são recursos críticos dado a nossa proposta de dados *offchain*. Disco, em particular, terá algum impacto nos custos da infraestrutura a longo prazo (e.g., mais de um ano) quando acumulado vários EMRs, cujos volumes pequenos e padronizados do seus *hashes* torna o armazenamento da blockchain em cada organização baixo e previsível. Observamos em nossos experimentos que mais de 1000 EMRs ocupou cerca de 42 MBytes por organização, e possivelmente, um milhão de EMRs ocuparia menos de 50 GBytes.

O uso da rede mostrado na Figuras 2(c) e 2(d) também não é um recurso crítico. O uso desse recurso se comporta assim como o uso de disco. No entanto, o custo com o uso da rede não é cumulativo ao longo do tempo, mas é fixo por período de tempo (e.g., custo fixo por mês) considerando a carga média da rede. Por exemplo, ao observar o uso de rede por participante, nossos experimentos de uma hora consumiram até 150 MBytes de saída, o que requer uma conexão de 350 Kbps para *upload*, e até 86 MBytes de entrada, o que requer uma conexão de 200 Kbps para *download*.

Ao longo das inserções, observamos perdas de transações, devido à contenção de recursos (cpu) dos participantes. Especificamente, ao pico de CPU em 25 minutos, i.e., a carga de 500 tps, iniciam perdas que variam entre 1 e 4% nas organizações, e essas perdas alcançam o maior ponto de saturação ao pico de 45 minutos, com perdas de pelo menos 50% em algumas organizações. As perdas observadas são severas e demandam mais estudos para descoberta do recurso computacional ideal para evitá-la ou otimizações na configuração padrão da plataforma que são os alvos seguintes dessa pesquisa.

5. Conclusões

Neste artigo propomos um modelo de redes blockchain permissionadas para o compartilhamento de EMRs entre pacientes e organizações da área de saúde. Modelamos um EMR como um objeto com cinco transações básicas realizadas por participantes de um sistema de saúde típico: emitir, aceitar, rejeitar, compartilhar e descompartihar EMRs. Codificamos esse modelo na plataforma Hyperledger Fabric via seus recursos de contratos inteligentes. Uma organização que adere à rede necessita apenas instalar nosso cliente Hyperledger para conectar seus sistemas particulares de EMR à rede blockchain. Pacientes e profissionais dessa organização passam a fazer parte da rede blockchain com suas devidas credenciais para realizar as transações mencionadas. Nossos resultados experimentais mostram que a rede blockchain proposta é robusta e aceita até 400 transações por segundo, considerando computadores básicos e recursos de comunicação e armazenamento mínimos das organizações participantes. Contudo, observamos que o desafio na gerência da rede concerne o processamento das transações, i.e., o uso de CPU, que é um recurso crítico que necessita ser cuidadosamente administrado para obter taxas superiores a 400 transações por segundo. Trabalhos futuros consistem em desenvolver rotinas para automatizar o cliente da rede em diferentes sistemas de saúde e desenvolver ferramentas para gerência de consumo e custos de recursos computacionais na rede blockchain.

Referências

Androulaki, E. and et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proc. of the EuroSys Conference*.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In *Proc. of OBD Conference*.

CMS (2012). Center for Medicare and Medicaid Services: Electronic Health Records. https://www.cms.gov/Medicare/E-Health/EHealthRecords. Accessed: 2021-08-27.

Conceicao, A. F., da Silva, F. S. C., Rocha, V., Locoro, A., and Barguil, J. M. M. (2018). Eletronic Health Records Using Blockchain Technology. In *Proc. of WBlockchain*.

Greve, F., Sampaio, L., Abijaude, J., Coutinho, A. A., Brito, I., and Queiroz, S. (2018). Blockchain e a Revolução do Consenso sob Demanda. In *Proc. of SBRC Minicursos*.

HL7 (2014). HL7 Fast Healthcare Interoperability Resources. https://ecqi.healthit.gov/fhir. Accessed: 2021-08-27.

Mendonça, R., Gomes, O., Vieira, A. B., and Nacif, J. A. N. (2021). Tratamento de Concessão e Revogação de Acesso a Registros Eletrônicos de Saúde em Blockchain. In *Proc. of WBlockchain*.

OpenEHR (2003). Open Industry Specifications, Models and Software for E-Health. https://www.openehr.org/. Accessed: 2021-08-27.

RNDS (2020). Rede Nacional de Dados em Saúde: Ecossistema FHIR. https://rnds-guia.saude.gov.br/docs/rnds/tecnologias. Accessed: 2020-06-14.

Spengler, A. C. and Souza, P. S. (2021). Avaliação de desempenho do hyperledger fabric com banco de dados para o armazenamento de grandes volumes de dados médicos. In *Proc. of WPerformance*.

Prêmio de melhor artigo no V Workshop Blockchain: Teoria, Tecnologia e Aplicações (WBlockchain) do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos em 2022.

FORTALEZA - CE

SBRC

XL SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS

Certificado

Certificamos que o artigo intitulado **"Análise de Custo de Infraestrutura em Redes Blockchain Públicas e Permissionadas"** dos autores **Ronan Dutra Mendonça, Pedro Hércules Dantas, Glauber Dias Gonçalves, Alex Borges Vieira e José A. M. Nacif** recebeu o prêmio de Melhor Artigo no V Workshop Blockchain: Teoria, Tecnologia e Aplicações (WBlockchain) do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, que ocorreu no período de 23 a 27 de maio de 2022.

Fortaleza, 27 de Maio de 2022.

Rafael Lopes Gomes
Coordenador Geral do SBRC 2022

Rossana Maria de Castro Andrade
Coordenadora Geral do SBRC 2022

ORGANIZAÇÃO: REALIZAÇÃO: SECRETARIA EXECUTIVA::

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DIGITAL NA BIBLIOTECA "JOSÉ ALBANO DE MACEDO"

Identificação do Tipo de Documento

( ) Tese

( ) Dissertação

(x) Monografia

( ) Artigo

Eu, **Pedro Hércules de Sousa Dantas**, autorizo com base na Lei Federal nº 9.610 de 19 de Fevereiro de 1998 e na Lei nº 10.973 de 02 de dezembro de 2004, a biblioteca da Universidade Federal do Piauí a divulgar, gratuitamente, sem ressarcimento de direitos autorais, o texto integral da publicação Análise de Custo e Desempenho de Aplicações Baseadas na Tecnologia Blockchain de minha autoria, em formato PDF, para fins de leitura e/ou impressão, pela internet a título de divulgação da produção científica gerada pela Universidade.

Picos-PI 28 de Março de 2023.

Pedro Hercules de Sousa Dantas

Assinatura

_____

Assinatura