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*.

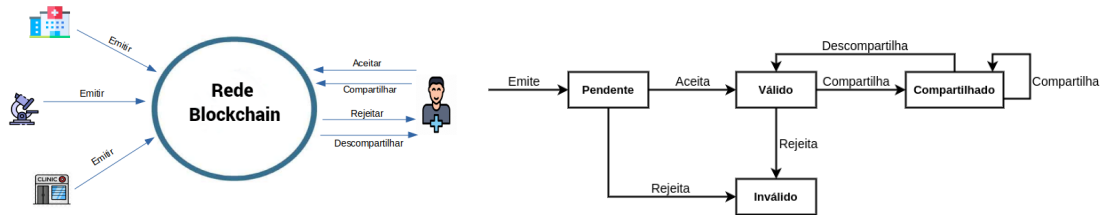
protocolo de consenso tolerante a falhas bizantinas (BFT). Esse protocolo garante a consistência da blockchain em todas as organizações, i.e., elas possuem cópias idênticas do *ledger* e cada objeto emitido possui o mesmo estado global [Androulaki and et al. 2018].

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

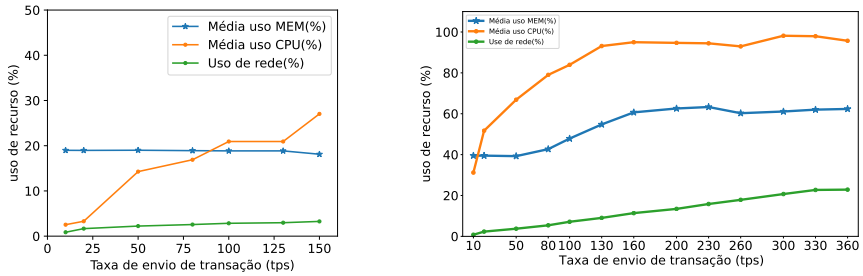
Tabela 1. Especificações dos nós que compõem cada tipo de infraestrutura: família AWS T2, processador Intel Xeon 3.0-3.3 GHz e disco SSD de 100 GB.

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.

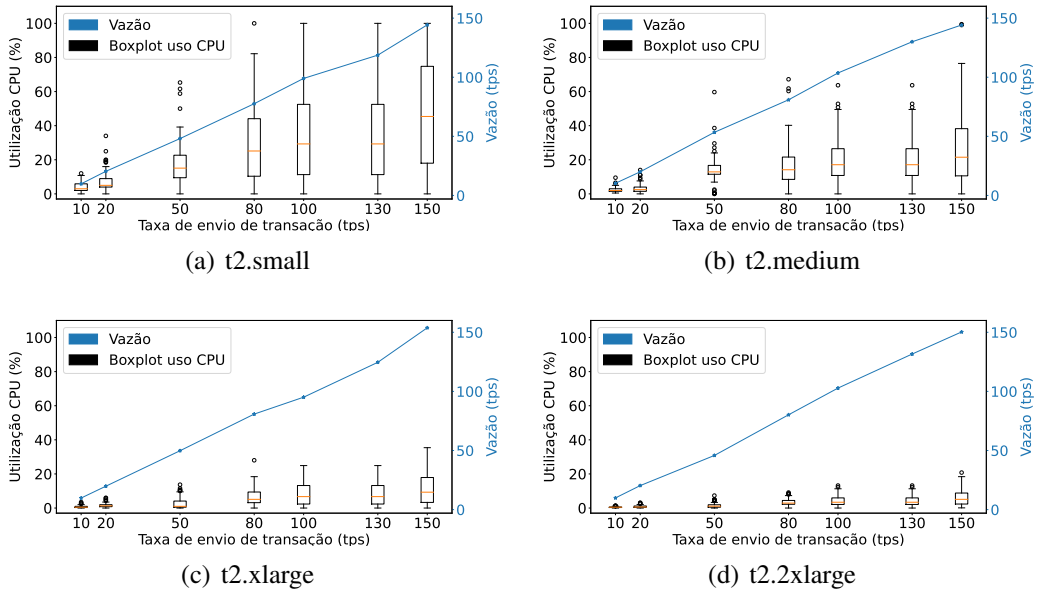
As Figuras 4 e 5 mostram a variação de uso de CPU e a vazão em função da carga de trabalho em transações por segundo (tps) para as medições observadas nas redes pública e permissionada respectivamente com os quatro tipos de infraestruturas. As figuras apresentam *boxplots* para sumarizar a distribuição 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



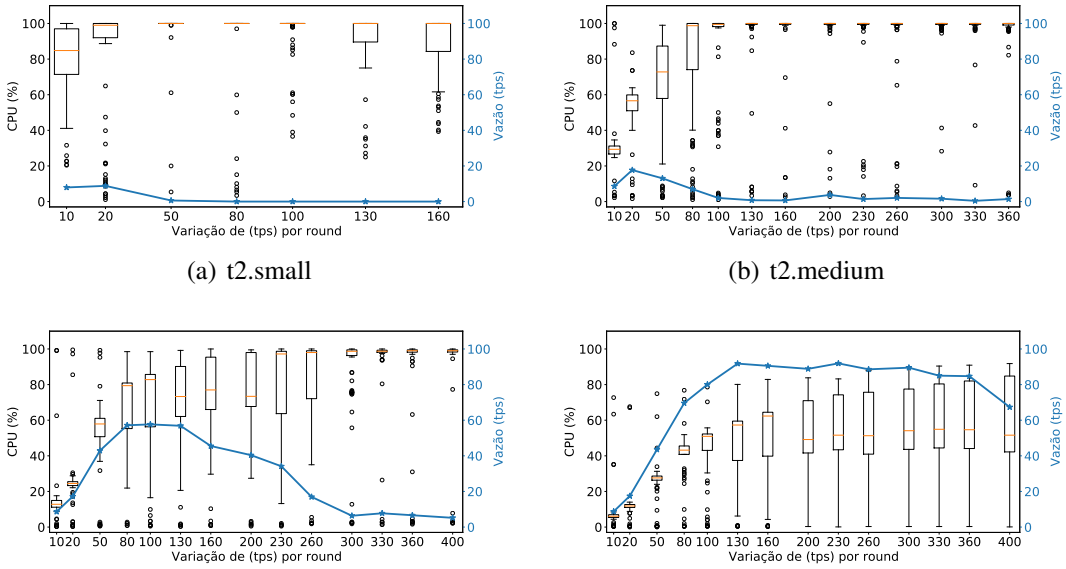
(a) t2.small (b) t2.medium

(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.



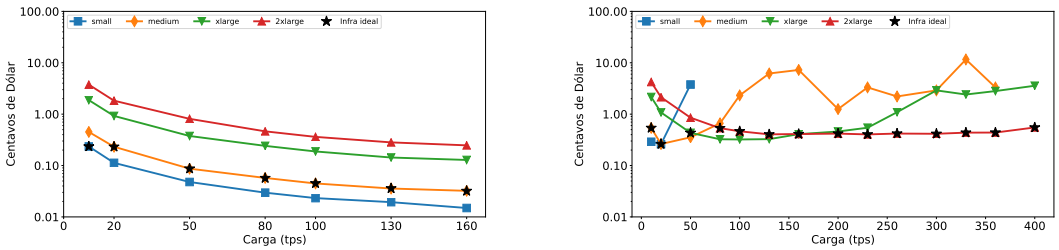
(a) t2.small (b) t2.medium

(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.