

Simulação e Avaliação de Desempenho de uma Rede Blockchain Utilizando Containers Docker

Anderson Melo de Moraes¹, Fernando Antonio Aires Lins¹,
Gustavo Rau de Almeida Callou¹

¹Programa de Pós-Graduação em Informática Aplicada (PPGIA)
Universidade Federal Rural de Pernambuco (UFRPE)
Rua Dom Manoel de Medeiros, s/n, Dois Irmãos, CEP 52171-900, Recife – PE – Brasil

{anderson.ufrpe, faires, gcallou}@gmail.com

Abstract. *With the development of new technologies, new challenges arise regarding information security. Given this, Blockchain technology is presented, which have a high level of security, as they keep data distributed and decentralized, and can be used in different contexts. In this article, a Blockchain simulation was performed using Docker containers. Then a methodology was proposed to evaluate the performance of the Blockchain and finally, a case study was carried out, applying the methodology in a series of tests on the application. Different load tests were performed, and the Blockchain flow rate and response time were evaluated, through the JMeter performance evaluation tool.*

Resumo. *Com o desenvolvimento de novas tecnologias surgem novos desafios em relação a segurança das informações. Diante disso apresentam-se a tecnologia Blockchain, que possuem um alto nível de segurança, pois mantêm os dados distribuídos e descentralizados, e podem ser utilizadas em diferentes contextos. Neste artigo, foi realizada uma simulação de uma Blockchain utilizando containers Docker. Em seguida foi proposta uma metodologia para avaliar o desempenho da Blockchain e por fim, realizou-se um estudo de caso, aplicando a metodologia em uma série de testes sobre a aplicação. Foram executados diferentes testes de carga, e avaliada a vazão e o tempo de resposta da Blockchain, através da ferramenta de avaliação de desempenho JMeter.*

1. Introdução

Blockchain consiste em um conceito tecnológico que foi apresentado em 2008 e tinha como principal propósito, inicialmente, dar suporte à criação da criptomoeda Bitcoin [Nakamoto, 2019]. Na época, muitos países se encontravam em meio a uma grave crise financeira, que gerava instabilidade econômica e uma grande desconfiança em empresários e investidores. Neste contexto, surgiu a proposta de levar as transações financeiras para a Internet e fazer com que acontecessem de forma descentralizada, sem o intermédio de bancos ou instituições reguladoras.

Para isso, fazia-se necessário a existência de uma tecnologia que garantisse segurança e confiabilidade às transações. A tecnologia Blockchain, também conhecida como protocolo de confiança, surgiu com o intuito de garantir a segurança descentralizando os dados. Esta apresenta-se como bases de registros de dados distribuídas e compartilhadas, que armazenam informações agrupadas em blocos sobre

todas as transações que ocorrem entre os usuários [Chicarino et al., 2017].

Cada computador conectado à rede, também chamado de nó, armazena uma cópia da base de dados onde se encontram os registros de todos os blocos da rede. Após um novo bloco ser gerado e validado ele é adicionado à cadeia, então todos os nós são atualizados para receber os novos dados e dessa forma, continuam todos a conter o mesmo conteúdo. Os blocos são armazenados de forma encadeada, cada um deles guarda uma referência para o seu anterior. Isso impossibilita que novos dados sejam inseridos, ou que blocos sejam modificados, sem que isso seja percebido por todos os demais nós da rede.

Devido ao alto nível de segurança apresentado pela tecnologia Blockchain, logo se percebeu que ela também poderia ser utilizada para diversos outros propósitos, como comunicações em cadeias de fornecimento, contratos inteligentes, gerenciamento de identidades digitais, registro de documentos, e em uma série de outras aplicações que demandam confiabilidade e registros de dados de forma segura e imutável [Pilkington, 2016].

No entanto, ao utilizar Blockchain para diferentes contextos de aplicações, faz-se necessário conhecer o comportamento da mesma frente a uma quantidade variável e possivelmente grande de usuário realizando requisições simultâneas. É importante garantir um bom desempenho da aplicação, alinhado à segurança proporcionada pela Blockchain. Assim, este trabalho propõe a análise de desempenho, via simulação de uma Blockchain, utilizando *containers Docker* [Singh e Singh, 2017]. É realizada uma avaliação de desempenho mediante a aplicação de diferentes cargas de requisições simultâneas, com o objetivo de analisar a sua performance em diferentes contextos de execução.

O artigo está organizando de acordo com as seções a seguir. A Seção 2 apresenta alguns trabalhos relevantes relacionados ao tema, e descrevem metodologias utilizadas para avaliação de desempenho de sistemas baseados em Blockchain. A Seção 3 apresenta os principais conceitos acerca da temática abordada para um melhor entendimento da pesquisa realizada. A Seção 4 descreve a metodologia utilizada para a realização deste trabalho. A Seção 5 apresenta um estudo de caso, onde é simulada uma Blockchain com 10 e 20 nós utilizando *containers Docker*. Por fim, a Seção 6 apresenta as conclusões do trabalho e indica possíveis estudos futuros.

2. Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados a avaliação de desempenho de sistemas baseados em Blockchain.

Pongnumkul, Siripanpornchana e Thajchayapong (2017), analisaram a performance e as limitações de duas plataformas de Blockchain privadas, a Hyperledger Fabric e a Ethereum [Androulaki et al., 2018]. Os autores aplicam diferentes quantidades de requisições simultâneas (1, 10, 100, 1000 e 10000) a ambas as redes para avaliar quesitos como tempo de execução, latência e taxa de transferência ao executar ações de criar conta e transferir dinheiro. Para tal avaliação, utilizou-se o serviço AWS EC2, implementando um nó do Blockchain e realizando a simulação das transações em grandes quantidades para avaliar o desempenho. Ao fim dos testes, o Hyperledger se mostrou mais eficiente em todos os quesitos analisados, que foram tempo de execução, latência e taxa de transferência.

Han, Gramoli e Xu (2018) avaliaram o desempenho de tecnologia Blockchain para registro de dados de diversos dispositivos de *IoT*. Realizaram a simulação de uma rede Blockchain com 32 máquinas, com sistema operacional Ubuntu 16.04 e Node.js 11.4 [Tilkov e Vinoski, 2010], que se trata de um interpretador, com código aberto, de código JavaScript. Os autores aplicaram testes de carga à rede, através do envio de diversas cargas diferentes para quantificar a latência, o tempo de resposta da rede, dentre outros parâmetros. O experimento teve como objetivo avaliar o desempenho de uma rede Blockchain para resolver o problema de consenso quando se tem uma grande quantidade de dispositivos de *IoT* tentando fazer uso da rede ao mesmo tempo.

Rouhani e Deters (2017) realizou uma avaliação de desempenho em uma rede Ethereum para diferentes quantidades de transações. Utilizando 2 nós de rede Ethereum, em máquinas i7-6700 com 24GB de RAM, foram aplicadas diferentes quantidades de requisições simultâneas, entre 1000 e 10000, com o objetivo de verificar o tempo médio de processamento das transações. Em seguida, foi realizada uma avaliação de desempenho na rede, que se mostrou 89,82% mais rápida para 1000 transações em comparação ao teste com 10000.

Zheng et al. (2018) mencionaram alguns problemas de performance apresentados por sistemas baseados em Blockchain e enfatizaram a necessidade de realizar monitoração de performance dessas plataformas. Em seguida, os autores propuseram a criação de um *framework* para avaliação de desempenho em sistemas de tempo real baseados em Blockchain. Este *framework* leva em consideração diferentes métricas, dentre elas tempo médio de resposta, tempo de processamento da CPU, taxa de utilização da memória RAM, etc. Para testar o *framework* foram analisadas as diferentes fases de execução de 1000 *Smart Contracts*, em 4 plataformas conhecidas de Blockchain. O resultado mostrou ser possível aplicar o *framework* para monitoramento de Blockchains e demonstra a eficiência deste.

Kim et al. (2018) trataram da necessidade de realizar avaliações de desempenho em sistemas baseados em Blockchain. Os autores realizaram uma avaliação das arquiteturas Hyperledger e Ethereum [Androulaki, et al., 2018], levando em consideração requisitos de modificabilidade, segurança e performance. Como resultado da avaliação a plataforma Hyperledger se mostrou mais robusta em relação a modificabilidade e performance, enquanto que a Ethereum apresentou um maior nível de segurança.

Mikkelsen et al. (2018) mencionam a respeito de ambientes de IoT que possuem um componente *marketplace* central, do qual dependem todos os componentes da rede. Devido ao fato deste ser centralizado, podem ocorrer vulnerabilidades de segurança. Os autores propuseram a utilização de Blockchain para implementar o *marketplace*, de forma distribuída e descentralizada, garantindo assim um maior nível de segurança e confiabilidade ao sistema. Para testar a teoria foi utilizada uma rede P2P executando uma Blockchain privada baseada em Ethereum, composta por um nó minerador, um provedor e um consumidor. Todos sendo executados através do sistema Ubuntu 16.04, implementados em Node.js 8.11. Foi realizada uma avaliação de desempenho da rede e observou-se que o *marketplace* baseado em Blockchain é eficiente em termos de segurança, podendo ser implementado em ambientes reais. Porém, ocorreram perdas de desempenho no sistema devido a necessidade de mineração dos blocos.

Na tabela 1 é possível visualizar um comparativo entre as características apresentadas pelos trabalhos mencionados e por este artigo. Dentre os trabalhos

analisados, apenas um deles realizou simulação, tal técnica é útil por permitir mensurar o comportamento do sistema antes mesmo de implementá-lo; todos realizaram avaliação de desempenho, porém somente alguns definiram objetivamente metodologias para isso; nenhum deles fez uso de *containers*, ou outra ferramenta de virtualização, que são extremamente úteis por proporcionarem economias de recursos computacionais. Considerando os trabalhos relacionados apresentados nesta seção, este trabalho propõe uma metodologia bem definida para avaliação de sistemas baseados em Blockchain. É utilizada também a tecnologia de *containers* para a simulação da Blockchain, devido à alta performance apresentada por esta.

Tabela 1. Comparação entre as características dos trabalhos relacionados

	Características Consideradas				
	Simulação	Medição	Avaliação de Desempenho	Utilização de Containers	Definição de Metodologia de Av. de Desempenho
Pongnumkul et al.	x	✓	✓	✓	x
Han et al.	✓	x	✓	x	x
Rouhani	x	✓	✓	x	x
Zheng et al.	x	✓	✓	x	✓
Kim et al.	x	✓	✓	x	x
Mikkelsen et al.	x	✓	✓	x	✓
Este Artigo	✓	✓	✓	✓	✓

3. Conceitos e Definições

Esta seção apresenta os principais conceitos e terminologias necessárias para a compreensão deste trabalho. Explica brevemente o que é uma rede Blockchain, como se dá o seu funcionamento e como a sua estrutura é organizada. Apresenta ainda uma breve descrição sobre *containers* e avaliação de desempenho.

3.1. Blockchain

Também conhecido como protocolo de confiança, visa garantir a segurança através da descentralização de dados, ou seja, são bases de registros e dados distribuídos e compartilhados que armazenam informações sobre todas as transações que ocorrem em uma determinada rede [Chicarino et al., 2017]. Cada nó na rede guarda as mesmas informações que os demais, se um novo bloco é inserido todos os nós são atualizados para receber os novos dados e dessa forma, voltarem a conter o mesmo conteúdo.

Cada bloco guarda uma referência para o seu anterior. Dessa forma, para que as informações armazenadas em um bloco fossem alteradas seria necessário gerar novamente todos os blocos posteriores a ele, o que em uma rede de grandes proporções se tornaria inviável do ponto de vista computacional. O primeiro bloco da cadeia, comumente chamado de bloco gênese, é codificado pelo software no momento em que a rede é criada e serve como o estado inicial do sistema. Ele contém informações sobre as regras ou instruções que os demais blocos deverão obedecer. A figura 1 apresenta o encadeamento dos blocos em uma Blockchain.

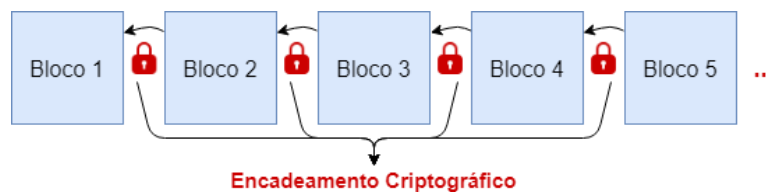


Figura 1. Estrutura de organização da Blockchain.

Um bloco é composto por duas partes principais que são o cabeçalho e as transações. As transações consistem no agrupamento dos dados que são armazenados no bloco. O cabeçalho, por sua vez, possui diversos campos, sendo os principais: o *hash*¹ do bloco anterior e o *nonce*. Além destes há também outros três conceitos importantes: altura do bloco, *hash* do cabeçalho e *timestamp*. A seguir são apresentados cada um destes conceitos [Chicarino et al., 2017].

- **Transações:** consistem no conjunto de dados que são gravados nos blocos. Quando um nó cria uma transação, ele a envia aos seus vizinhos e estes, por sua vez, reenviam aos demais, até que alcance todos os nós da rede. Quando um bloco for validado e incluído na cadeia, as transações nele contidas se tornam públicas e inalteráveis.
- **Hash do bloco anterior:** é a existência deste campo, presente no cabeçalho, que permite o encadeamento dos blocos, ligando o bloco atual ao seu anterior e assim sucessivamente. Dessa forma é possível percorrer toda a cadeia até alcançar o bloco gênese, que por sua vez, possui o campo *hash* do bloco anterior preenchido com zero, por inexistir blocos anteriores a ele.
- **Nonce:** consiste em um número usado como variável para alterar o resultado gerado pelo cabeçalho. É utilizado para provar que um bloco foi validado e atende aos critérios estabelecidos pela rede.
- **Hash do cabeçalho:** é o principal identificador do bloco dentro da cadeia. Após todas as informações terem sido validadas e incluídas no cabeçalho, o *hash* do cabeçalho é gerado. É ele que é incluído no bloco posterior para garantir o encadeamento dos blocos.
- **Altura do bloco:** os blocos são incluídos na cadeia de forma sequencial. A diferença entre a posição de um bloco e o bloco gênese da cadeia é denominada altura do bloco.
- **Timestamp:** junto a cada bloco é armazenado o momento em que ele foi gerado. Este registro se dá através de um número que representa a data e hora da criação do bloco.

A figura 2 apresenta uma representação mais detalhada da estrutura dos blocos e dos principais campos contidos neles. No retângulo superior de cada bloco está representado o seu cabeçalho, com os campos descritos acima, e no retângulo inferior as transações que o bloco armazena.

¹ Cadeias de caracteres que servem como identificadores de dados que se encontram armazenados em um determinado local.

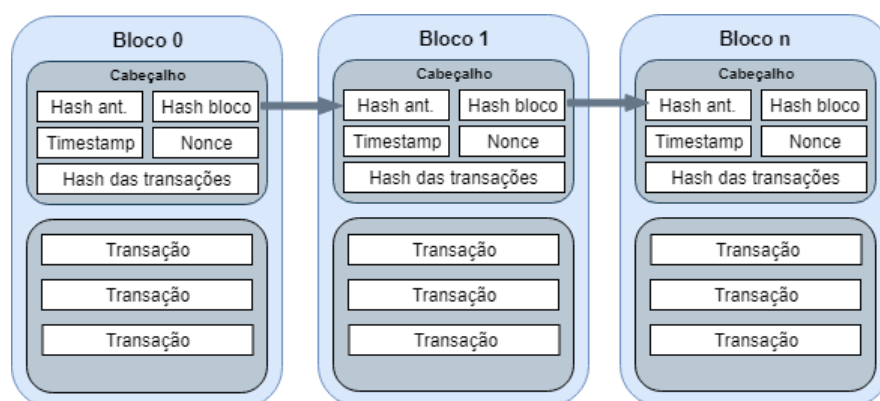


Figura 2. Estruturas dos blocos da Blockchain.

3.2. Containers

Os *containers* consistem em uma tecnologia de empacotamento de código, bibliotecas e dependências em um único objeto [Singh e Singh, 2017]. Compartilham um mesmo sistema operacional e são executados como processos isolados, o que possibilita a realização de implementações rápidas, confiáveis e consistentes, independentemente do ambiente.

Existem algumas tecnologias para o gerenciamento de *containers*, sendo a principal delas o *Docker*, que cria imagens (cópias completas dos *containers*) e as disponibiliza para *download* de forma simples e rápida. Devido à natureza distribuída dos sistemas baseados em Blockchain, faz-se necessário a utilização de tecnologias que ofereçam uma boa performance e economia de recursos computacionais [Yadav, 2018], por isso, neste trabalho foi feito uso do *Docker* para simular uma rede Blockchain, criando os nós virtuais através de *containers*.

3.3. Avaliação de Desempenho de Sistemas

Para realizar a avaliação de desempenho de um sistema, é possível utilizar três diferentes técnicas [Yadav, Sousa e Callou, 2018; Jain, 1991]:

- **Medição:** faz a análise diretamente sobre o sistema real, aplicando cargas de trabalhos para mensurar o desempenho deste através das métricas coletadas. Tem como objetivo conhecer o comportamento do sistema em diferentes cenários de trabalho.
- **Modelagem:** realiza o uso de modelos matemáticos, como redes de Petri, Cadeias de Markov, etc, para representar sistemas do mundo real e, desta forma, poder analisar o seu comportamento diante da aplicação de diferentes cenários de trabalho. São utilizados em situações onde o sistema real ainda não está implementado ou que não se tem acesso direto a ele.
- **Simulação:** esta técnica permite projetar um modelo computacional de um sistema real e, a partir dele, conduzir experimentos, com o propósito de entender seu comportamento e/ou avaliar estratégias para sua operação [Pegden, Sadowski e Shannon, 1995].

Para realizar a avaliação de desempenho de uma aplicação, costuma-se realizar a aplicação de diferentes cargas de trabalho sobre ela [Pongnumkul et al., 2017] para criar

um estresse computacional no sistema e verificar o seu comportamento em diferentes situações. Para isso, utilizam-se ferramentas de *benchmarks*, que permitem ao pesquisador a definição de parâmetros, como número de usuários simultâneos, entre outras coisas, e assim aproximar a simulação de uma situação do mundo real.

4. Metodologia

Esta seção descreve a metodologia proposta que tem como objetivo avaliar o desempenho de uma rede Blockchain. Esta metodologia é descrita como uma sequência de etapas que permitem conduzir o estudo desde a modelagem do problema até as conclusões. A figura 3 mostra uma representação diagramática dos passos proposto na metodologia deste trabalho.

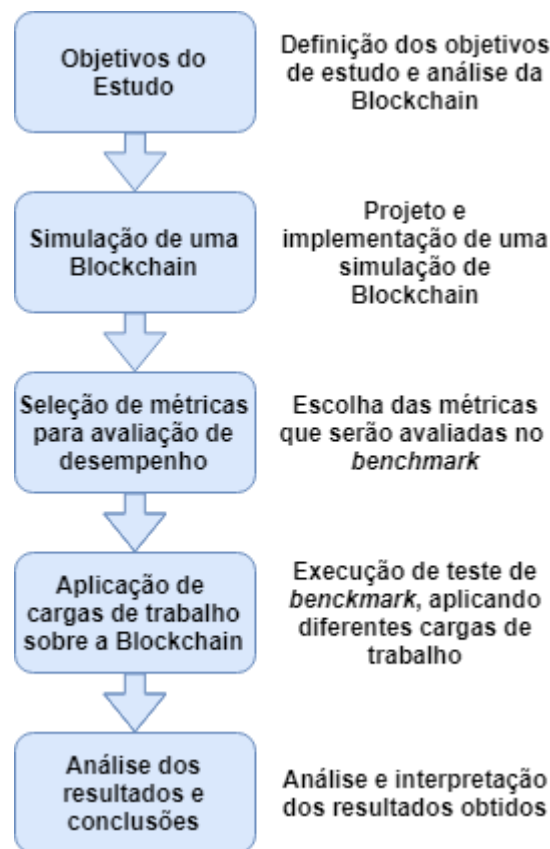


Figura 3. Metodologia utilizada para a Avaliação de Desempenho de uma rede Blockchain

- **Objetivos do estudo:** inicialmente é preciso definir os objetivos de estudos, entender como se dá o funcionamento de uma Blockchain e quais parâmetros deverão ser levados em consideração no momento da avaliação.
- **Projeto e implementação de simulação em Blockchain:** esta atividade permite projetar uma rede Blockchain, para simular o seu comportamento e definir ferramentas de *benchmarks*, para realizar a avaliação de desempenho durante a execução dos experimentos.
- **Seleção de métricas para avaliação de desempenho:** nesta etapa é possível definir quais métricas serão adotadas para a avaliação de desempenho, como por exemplo, tempo de resposta, que representará a rapidez com que a Blockchain

reage à uma requisição; tempo na fila, que indica o tempo que uma requisição aguarda na fila até ser processada pela Blockchain; taxa de utilização de recursos, que está relacionada ao nível de ociosidade de um recurso; tempos de execução, que representam o tempo de atendimento total para uma requisição, dentre outras.

- **Aplicação de cargas de trabalho:** nesta etapa é realizada efetivamente a simulação, mediante a aplicação de diferentes cargas de trabalho sobre a Blockchain. É realizada a execução dos testes de *benchmarks* na simulação e a coleta dos resultados das métricas.
- **Análise dos resultados e conclusões:** por fim, nesta etapa, os resultados das métricas obtidos nos experimentos são interpretados com o objetivo de obter conclusões sobre o problema de pesquisa.

5. Estudo de Caso

Esta seção apresenta um estudo de caso que foi realizado com o objetivo de ilustrar e avaliar a metodologia proposta, realizando uma simulação de uma rede Blockchain com *containers Docker*. A seguir, são descritas as atividades realizadas durante o estudo, de acordo com a metodologia apresentada.

Dentre as inúmeras aplicações que podem fazer uso de registro em Blockchain, está o registro de diplomas digitais. De acordo com Morais (2019), instituições de ensino podem realizar a emissão de diplomas e certificados no formato digital e, para assegurar a autenticidade destes documentos, estes poderiam ser registrados em uma Blockchain. Para fazer tal registro bastaria gerar um identificador único para cada documento. Uma vez que este identificador se encontrasse registrado na Blockchain, ele poderia ser consultado sempre que necessário para comprovar a existência do documento original.

Objetivos do estudo: no início deste trabalho buscou-se compreender como se dá o funcionamento de uma Blockchain e como os blocos são encadeados. Em seguida buscou-se realizar a simulação de uma Blockchain, utilizando *containers Docker*. Esta tecnologia foi escolhida, pois de acordo com Yadav (2018) os *containers* apresentam uma melhor performance e uma maior economia de recursos computacionais, em comparação com outras tecnologias como as máquinas virtuais. Também foi avaliado o desempenho das Blockchains simuladas, mediante a aplicação de diferentes cargas de requisições simultâneas, para analisar a performance em diferentes contextos de execução.

Projeto e implementação de simulação em Blockchain: nesta etapa realizou-se a simulação de uma Blockchain. Optou-se pelo uso de simulação, pois ela permite entender e avaliar o comportamento de um sistema e realizar experimentos sobre ele. Neste trabalho é realizada a simulação de uma Blockchain local, com uma quantidade de nós definida, por isso a necessidade e a importância de avaliar o possível comportamento da aplicação antes da sua implementação real.

A simulação, que foi implementada em Node.js, ao ser executada cria o bloco gênese da cadeia e instancia os demais nós da Blockchain em *containers*, através do *Docker*. Cada *container* possui uma imagem *Linux*, que armazena uma cópia dos registros da cadeia de blocos. Após criados, os nós começam então a monitorar se os novos blocos adicionados são válidos e se podem ser acrescentados a rede.

Neste estudo a quantidade de nós a ser instanciada é definida a critério do pesquisador. Foram considerados inicialmente uma simulação com 10 nós,

representando uma rede de pequenas proporções, em seguida este número foi aumentado para 20, com o intuito de observar o comportamento da rede com o dobro de nós. Ao ser executada, a aplicação cria apenas o bloco gênese, que é o bloco inicial da cadeia e o envia para todos os nós, que a partir de então começam a monitorar se os novos blocos adicionados são válidos e se podem ser acrescentados a cadeia.

Os testes foram executados em um sistema operacional Linux Mint 19.1 de 64 bits. A figura 4 mostra uma representação visual da rede Blockchain gerada pela aplicação, contendo apenas o bloco gênese da cadeia, o *timestamp* com o momento em que este foi gerado e o *hash* de identificação do bloco.

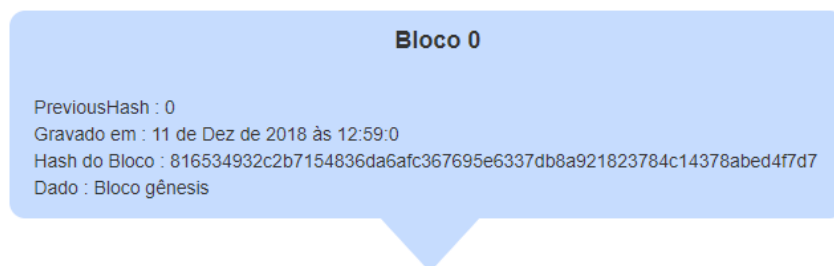


Figura 4. Representação gráfica do primeiro nó da Blockchain simulada.

Seleção de métricas para avaliação de desempenho: Os parâmetros escolhidos para análise foram a vazão ou *throughput*, que corresponde a taxa na qual as requisições são atendidas pelo sistema, e o tempo de resposta, que é o tempo decorrido entre o início e a conclusão de um serviço [Menasce, Dowdy, e Almeida, 2004].

Aplicação de cargas de trabalho: para obter os valores da vazão e do tempo de resposta, foram realizados 30 experimentos. Com este número de repetições o experimento terá um intervalo de confiança alto, ou seja, os resultados se aproximarão mais de um cenário real [Brown e Berthouex, 2002]. O desvio padrão dos dados utilizados no experimento foi de 1,18. Foram aplicadas cargas diferentes de trabalho, que simulam diferentes quantidades de usuários realizando acessos simultâneos à aplicação. As cargas aplicadas foram de 1, 5, 10, 50, 100, 500 e 1000 acessos simultâneos.

Inicialmente foram adicionados 10 nós a Blockchain e aplicadas as diferentes cargas de trabalho sobre a mesma, simulando acessos simultâneos a rede. Os testes foram realizados em uma máquina com processador Intel Core i5-10210U de 1,60GHZ, com 8GB de memória RAM.

A ferramenta JMeter² permite definir a quantidade de acesso simultâneos que se deseja simular. Neste experimento, cada um dos acessos realiza o envio, via POST, de um dado no formato JSON para a aplicação, que no mundo real representaria o registro de um diploma digital na cadeia de blocos.

Análise dos resultados e conclusões: a primeira métrica considerada na avaliação foi a vazão. A figura 5 apresenta os resultados obtidos para cada uma das diferentes cargas aplicadas. Pelo gráfico é possível perceber que conforme o número de acessos simultâneos aumenta, o valor da vazão tende a se estabilizar. Isso ocorre por volta de 23 requisições por milissegundos, o que indica que este é o limite de vazão da aplicação,

² Software de código aberto, projetado para a execução de testes de carga e estresse e que nos permite medir o desempenho de diversos tipos de aplicações.

quando esta contém apenas 10 nós.



Figura 5. Vazão da Blockchain com 10 nós para diferentes cargas de trabalho.

A segunda métrica considerada foi a de tempo de resposta. A figura 6 apresenta os resultados obtidos para o teste com 10 nós, como é possível perceber pelo gráfico, conforme o número de usuários simultâneos aumenta, cresce também o tempo de resposta da aplicação. Para o exemplo contendo 1000 acessos, o tempo total de resposta foi de 12845 milissegundos.



Figura 6. Tempo de resposta da Blockchain com 10 nós para diferentes cargas de trabalho.

Em seguida foi realizada uma simulação da Blockchain contendo 20 nós, com o intuito de avaliar o seu comportamento ao dobrar a quantidade de máquinas conectadas. Uma rede com um número maior de nós, apresentará um nível maior de segurança, pois os dados estarão distribuídos em mais lugares. Para que um indivíduo malicioso consiga atacar e alterar os dados de uma rede Blockchain seria necessário que este conseguisse alterar mais de 51% da rede [Ye et al., 2018].

Neste estudo, buscou-se analisar o que acontece com o desempenho da Blockchain, em termos de vazão e tempo de resposta ao aumentarmos a quantidade de nós conectados. Para isso, foi realizado o mesmo experimento com 20 nós, aplicando as mesmas cargas de trabalho. Na figura 7 são apresentados os resultados obtidos para a vazão da aplicação com 20 nós. É possível perceber que conforme o número de requisições simultâneas aumenta, o valor da vazão tende a se estabilizar por volta de 23

requisições por milissegundos.



Figura 7. Vazão da Blockchain com 20 nós para diferentes cargas de trabalho.

Realizou-se também, a avaliação do tempo de resposta da Blockchain com 20 nós, para as mesmas cargas de trabalho consideradas anteriormente. A figura 8 apresenta os resultados obtidos, onde é possível perceber que houve um aumento considerável nos tempos de repostas para todas os casos testados.



Figura 8. Tempo de resposta da Blockchain com 20 nós para diferentes cargas de trabalho.

Com o intuito de compreender o porquê da vazão se estabilizar em valores próximos a 23 requisições por 12845 milissegundos, observou-se os percentuais de uso de CPU e de memória RAM durante a execução dos testes para 1000 requisições simultâneas. Para isso, foi utilizado o *plugin* do Perfmon³ adicionado ao JMeter, com ele é possível observar estas métricas.

³ Ferramenta de monitoramento de desempenho disponível em sistemas operacionais Windows. Permite monitorar diferentes métricas, como uso de CPU, memória RAM, taxa de leitura e escrita em disco, taxa de uso de rede, dentre outras coisas.

(a) Uso de CPU e Memória - 10 nós



(b) Uso de CPU e Memória - 20 nós

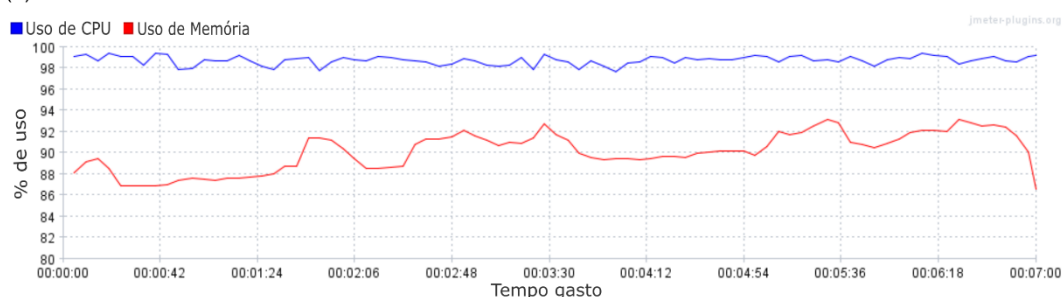


Figura 9. (a) Percentual de uso de CPU, representado pela linha azul, e memória, linha vermelha, durante a realização do experimento para 10 nós. (b) Percentual de uso de CPU, linha azul, e memória, linha vermelha, durante a realização do experimento para 20 nós.

Pela figura 9 (a) é possível perceber que durante a realização do experimento para a Blockchain com 10 nós o percentual de uso de CPU, representado pela linha azul, estava próximo a 100% e a taxa de utilização da memória RAM, representada pela linha vermelha, estava alcançando valores próximos aos 90%. O mesmo é possível verificar na figura 9 (b), onde são mostradas as taxas de utilização de CPU e memória, linhas azul e vermelha respectivamente, para a Blockchain com 20 nós. Também nesse caso, o uso de CPU se aproxima de 100% e o de memória oscila entre 85 e 95%. Esta é, possivelmente, a causa do valor da vazão se estabilizar a medida em que o número de requisições simultâneas aumenta. É possível presumir que para alcançar uma taxa de vazão mais alta, seria necessário a utilização de um *hardware* com configurações superiores.

A tabela 2 mostra um comparativo entre os tempos (em milissegundos) de execução para ambos os testes, juntamente com os percentuais de aumento.

Tabela 2. Percentual de aumento do tempo de resposta

Carga	1	5	10	50	100	500	1000
10 nós	17	43,5	81	961	1531	7688	12845
20 nós	20	57	197	1631	3189	11219	22022
Aumento	17%	31%	143%	70%	108%	45,9%	71,4%

No total houve um aumento médio de 70% no tempo de resposta para o teste com 20 nós em comparação ao teste anterior, com apenas 10. Em alguns casos houve um impacto de quase 10s a mais (carga de 1000 requisições simultâneas), o que gera um impacto significativo no tempo de resposta final, que consequentemente será percebido pelo usuário. Por isso, ao se projetar uma rede Blockchain, se faz necessário analisar a viabilidade de adicionar uma quantidade maior de nós. Especialmente considerando que

com uma quantidade menor de nós, já é possível obter um nível de segurança satisfatório para aplicações mais simples.

Logo, é possível realizar o uso de Blockchain para a implementação de diversas aplicações que requerem um alto nível de segurança e imutabilidade dos dados. Porém, como é possível constatar pela análise realizada, ao aumentar o número de nós da rede tem-se uma considerável perda de desempenho, logo é necessário levar em consideração o *trade-off* entre desempenho e segurança, para que assim, seja possível a implantação de sistemas altamente seguros e eficientes.

6. Considerações Finais

Este artigo realizou uma simulação de uma rede Blockchain utilizando *containers* em *Docker* e propôs uma metodologia com etapas bem definidas para a avaliação de desempenho de sistemas que utilizam Blockchain como base de registro. Foi realizado um estudo variando a quantidade de nós (10 e 20 nós) na Blockchain, com o objetivo de avaliar o desempenho mediante a aplicação de diferentes cargas de trabalho. Para a realização dos testes foi utilizada a ferramenta JMeter, levando em consideração as métricas de vazão e tempo de resposta. Ao final constatou-se que a Blockchain com 20 nós apresentou um tempo de resposta 70% maior que a anterior, isso aponta que apesar do uso de Blockchain oferecer um maior nível de segurança, pode haver um comprometimento no desempenho da aplicação. Assim nota-se a necessidade de fazer um balanceamento entre segurança e desempenho ao se projetar um sistema baseado em Blockchain. O uso de simulação permite avaliar o comportamento da aplicação antes da sua implementação, e assim analisar o seu desempenho.

Como trabalhos futuros é possível a realização de um número maior de experimentos, variando a quantidade de nós e o número de requisições simultâneas aplicadas, para assim, analisar o comportamento do sistema em outras circunstâncias. Pode-se realizar testes de segurança na rede Blockchain, através da simulação de ataques, considerando diferentes quantidades de nós, com o objetivo de fazer um comparativo mais detalhado entre a relação de segurança vs desempenho existente nesse tipo de rede. É possível ainda, modelar o fluxo de requisições através de redes de Petri com o intuito de simular uma rede Blockchain atendendo diversas requisições causadas por cargas de trabalho controladas. Dessa forma é possível avaliar outras métricas como, tempo médio na fila, tamanho da fila, e latência, sendo métricas importantes para a qualidade de sistemas computacionais. É possível ainda, realizar estimativas de cenários que não seriam facilmente avaliados, devido ao alto custo computacional.

Referências

- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & Muralidharan, S. (2018, April). Hyperledger fabric: a distributed operating system for permissioned Blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).
- Brown, L. and Berthouex, P. (2002). *Statistics for Environmental Engineers, Second Edition*. Taylor & Francis.
- Han, R., Gramoli, V., & Xu, X. (2018). Evaluating Blockchains for IoT. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018-Janua*, 1–5. <https://doi.org/10.1109/NTMS.2018.8328736>

- Jain, R. (1991). *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley, Nova York, 1th edition.
- Kim, J., Kang, S., Ahn, H., Keum, C., & Lee, C. G. (2018). Poster: Architecture reconstruction and evaluation of blockchain open source platform. *Proceedings - International Conference on Software Engineering*, 2, 185–186. <https://doi.org/10.1145/3183440.3195088>
- L Chicarino, V. R., Ferreira Jesus, E., N de Albuquerque, C. V., & de A Rocha, A. A. (2017). Uso de Blockchain para Privacidade e Segurança em Internet das Coisas. *Minicursos Do XVII Simpósio Brasileiro Em Segurança Da Informação e de Sistemas Computacionais - SBSeg2017*, (November), 51.
- Menasce, D. A., Dowdy, L. W., and Almeida, V. A. (2004). *Performance by Design: Computer Capacity Planning By Example*. Prentice Hall, 1th edition.
- Mikkelsen, L., Mortensen, K., Rasmussen, H., Schwefel, H. P., & Madsen, T. (2018). Realization and Evaluation of Marketplace Functionalities Using Ethereum Blockchain. *2018 International Conference on Internet of Things, Embedded Systems and Communications, IINTEC 2018 - Proceedings*, 47–52. <https://doi.org/10.1109/IINTEC.2018.8695307>
- Morais, A. M. de. (2019). *Controle de Emissão e Validação de Diplomas Digitais Utilizando Blockchain*. 66. Retrieved from http://www.repository.ufrpe.br/bitstream/123456789/1062/1/tcc_andersonmelodemoais.pdf
- Nakamoto, S. (2019). Bitcoin: a peer-to-peer electronic cash system, October 2008. *Cited On*, 53.
- Pegden, C. D., Sadowski, R. P., and Shannon, R. E. (1995). *Introduction to Simulation Using SIMAN*. McGraw-Hill, Inc., New York, NY, USA, 2nd edition.
- Pilkington, M. (n.d.). Blockchain technology: principles and applications. *Research Handbook on Digital Transformations*, 225–253. <https://doi.org/10.4337/9781784717766.00019>
- Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017). Performance analysis of private Blockchain platforms in varying workloads. *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*. <https://doi.org/10.1109/ICCCN.2017.8038517>
- Rouhani, S., & Deters, R. (2017). Performance analysis of Ethereum transactions in private Blockchain. *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2017-Novem, 70–74. <https://doi.org/10.1109/ICSESS.2017.8342866>
- Singh, S., & Singh, N. (2017). Containers & Docker: Emerging roles & future of Cloud technology. *Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, ICATccT 2016*, 804–807. <https://doi.org/10.1109/ICATCCT.2016.7912109>
- Tilkov, S., & Vinoski, S. (2010). Node.js: Using JavaScript to build high-performance network programs. *IEEE Internet Computing*, 14(6), 80-83.

- Yadav, R. R., Sousa, E. T. G., & Callou, G. R. A. (2018). Performance comparison between virtual machines and Docker containers. *IEEE Latin America Transactions*, 16(8), 2282–2288. <https://doi.org/10.1109/TLA.2018.8528247>
- Ye, C., Li, G., Cai, H., Gu, Y., and Fukuda, A. (2018). *Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting*.
- Zheng, P., Zheng, Z., Luo, X., Chen, X., & Liu, X. (2018). A detailed and real-time performance-monitoring framework for blockchain systems. *Proceedings - International Conference on Software Engineering*, 134–143. <https://doi.org/10.1145/3183519.3183546>