Lins, V.C., de Morais, A.M.
Revista Gest@o.org, V.19(2), 2021, p. 169-183
http://www.revista.ufpe.br/getaoorg
ISSN: 1679-1827

Simulação e Avaliação de Desempenho de uma *Blockchain* para Aplicações IoT

Blockchain Simulation and Performance Evaluation for IoT Applications

Vanessa Cordeiro Lins[1], Anderson Melo de Morais[2]

[1]*Universidade Federal Rural de Pernambuco, Pernambuco, Brasil.*
[2]*Universidade Federal de Pernambuco, Pernambuco, Brasil.*

INFO ARTIGO

Palavras-chave:
Blockchain,
Segurança da Informação,
Internet das Coisas.

RESUMO

A Internet das Coisas (IoT) consiste em um sistema de cooperação entre dispositivos inteligentes conectados. Os sistemas IoT têm acesso a diversos dados dos usuários, que precisam ser gerenciados de forma eficiente para evitar vulnerabilidades de segurança. Nesse cenário, a tecnologia Blockchain apresenta-se como uma opção promissora, pois permite o registro de dados de forma descentralizada, criptografada e imutável. Diante disso, este trabalho apresenta uma simulação de Blockchain utilizada para registros de dados da IoT e realiza uma avaliação de desempenho sobre ela, comparando com resultados da literatura. Foi realizada uma revisão bibliográfica, onde um trabalho foi escolhido como base para o comparativo de desempenho, em seguida foram definidas as métricas de avaliação, que foram vazão e tempo de resposta. Foram executados diferentes testes de carga sobre a Blockchain, variando sua quantidade de nós. Por fim, os resultados obtidos foram comparados com os dados do artigo de referência.

ARTICLE INFO

***Keywords*:**
Blockchain,
Information Security,
Internet of Things.

ABSTRACT

Internet of Things (IoT) is a system of cooperation between connected smart devices. IoT systems have access to diverse user data, which needs to be efficiently managed to avoid security vulnerabilities. In this scenario, Blockchain technology presents itself as a promising option, as it allows the recording of data in a decentralized, encrypted, and immutable way. Therefore, this work presents a Blockchain simulation used for IoT data records and performs a performance evaluation on it, comparing it with literature results. A literature review was carried out, where work was chosen as the basis for the performance comparison, then the evaluation metrics were defined, which were throughput and response time. Different load tests were performed on the Blockchain, varying its number of nodes. Finally, the results obtained were compared with data from the reference article.

DOI: doi.org/10.51359/1679-1827.2021.252657

Correspondência para autores:
vanecordelins@gmail.com (*Lins, V.C.*) (ORCID: 0000-0001-5388-5285),
amm6@cin.ufpe.br (*Morais, A.M.*) (ORCID: 0000-0001-7795-7183).

1. Introdução

Em uma sociedade permeada por diversas tecnologias, dados pessoais devem ser gerenciados com eficiência, para evitar que pessoas e/ou empresas com propósitos maliciosos o utilizem em benefício próprio. A preocupação em investir mais e melhor na segurança das informações tem sido um dos principais pontos discutidos no âmbito da computação.

A Internet das Coisas (IoT[1]) tem se tornado cada vez mais presente na vida das pessoas, seu principal objetivo é interconectar dispositivos do cotidiano, tornando-os inteligentes e autônomos (REYNA et al., 2018). A IoT pode ser aplicada em diversos contextos, como em cidades inteligentes; carros inteligentes, com diferentes sensores conectados à Internet; casas inteligentes; dispositivos de monitoramento da saúde, dentre muitas outras aplicações.

Os ambientes IoT têm acesso a diversos dados dos usuários, por isso é de fundamental importância que sejam aplicados mecanismos de segurança eficientes que garantam a confidencialidade, integridade e disponibilidade destes dados (CHICARINO et al., 2017). Técnicas de criptografia que auxiliam na proteção de dados sensíveis podem ser aplicadas a nível organizacional, institucional ou pessoal, protegendo dados armazenados localmente ou em transações na Internet (PILKINGTON, 2016).

Uma tecnologia que pode ser adotada para conferir segurança aos ambientes IoT é a *Blockchain*, que utiliza métodos criptográficos e o registro de dados descentralizados para estabelecer confiabilidade e segurança aos dados. Porém uma rede de dispositivos inteligentes gera e transmite grandes quantidades de dados, que precisam ser processados antes que sejam adicionados a cadeia de blocos. Dessa forma, é necessário avaliar a eficácia e o desempenho da tecnologia *Blockchain* integrada a um sistema IoT.

Diante disto, este trabalho propõe uma simulação de uma *Blockchain* e realiza uma avaliação de desempenho, alterando o tamanho da rede, com o objetivo de analisar o seu comportamento em diferentes situações. Inicialmente foi realizado um estudo bibliográfico com a finalidade de construir a fundamentação teórica do trabalho. Em seguida, utilizou-se a metodologia de avaliação de desempenho de *Blockchain* proposta por Morais, Lins e Callou (2020). Optou-se pelo uso de simulação, pois ela permite entender e avaliar o comportamento de um sistema e realizar experimentos sobre ele.

Para a escolha das métricas de avaliação utilizou-se a proposta de Zheng et al. (2018), onde foram selecionadas as métricas de Vazão e Tempo de Resposta. Foram aplicadas tais métricas na *Blockchain* simulada, visando validar a utilização de tal tecnologia em sistemas IoT e, posteriormente, foram discutidos e apresentados os resultados.

O artigo está organizando de acordo com as seguintes seções. A Seção II apresenta alguns trabalhos relevantes relacionados ao uso de *Blockchain* para IoT; A Seção III apresenta os principais conceitos sobre a temática abordada. A Seção IV apresenta a metodologia utilizada para o desenvolvimento deste trabalho. A Seção V descreve uma simulação e avaliação de desempenho de uma *Blockchain*, comparando-a a resultados

[1] *Internet of Things* (IoT): em português Internet das Coisas, rede de dispositivos físicos do cotidiano, conectados à Internet, com eletrônica e software embarcados

da literatura. Por fim, a Seção VI apresenta as considerações finais do trabalho e indica possíveis estudos futuros.

2. Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relevantes, referentes a temática abordada neste trabalho, a respeito do uso de *Blockchain* em ambientes IoT.

Giannoutakis et al. (2020) apresentam uma solução baseada em *Blockchain* para melhorar os mecanismos de segurança de casas inteligentes, com foco no registro dos usuários e dispositivos que constituem tais ambientes. A metodologia proposta utiliza *Smart Contracts*[1] para o registro dos elementos da casa inteligente. A solução foi implantada utilizando uma rede *Blockchain Ethereum*, para demonstrar a aplicabilidade e eficiência da implementação proposta em hardwares leves que são usados para gerenciar os dispositivos IoT. Porém os autores não avaliam a solução proposta, para verificar a sua eficiência em termos de desempenho.

Han, Gramoli e Xu (2018) avaliaram o desempenho de uma *Blockchain* para registro de dados IoT. Os autores realizaram uma simulação de *Blockchain* contendo 32 nós, cada um executando um sistema operacional Ubuntu 16.04. Para a avaliação são realizados diferentes testes de carga, para quantificar a latência, o tempo de resposta, dentre outros parâmetros. O experimento teve como objetivo avaliar o desempenho da *Blockchain* em um cenário onde uma grande quantidade de dispositivos IoT tentando fazer uso da rede ao mesmo tempo. No entanto o trabalho não apresenta resultados para cenários de *Blockchain* com outras quantidades de nós.

Mikkelsen et al. (2018) descrevem ambientes IoT que possuem um componente de gerenciamento central, do qual dependem todos os demais componentes da rede, devido a este fato podem ocorrer vulnerabilidades de segurança que comprometerão todo a ambiente. Diante disso propõem a utilização de *Blockchain* como mecanismo de gerenciamento distribuído e descentralizado, garantindo assim um maior nível de segurança e confiabilidade ao sistema. Para testar a solução proposta, utilizam uma *Blockchain* privada baseada em *Ethereum*. Foi realizada uma avaliação de desempenho e observou-se que a solução 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.

Morais, Lins e Callou (2020) realizam uma simulação de *Blockchain* utilizando *containers Docker*[2]. Em seguida apresentam 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. Os autores executados diferentes testes de carga, e avaliaram a vazão e o tempo de resposta da *Blockchain*, através da ferramenta de avaliação de desempenho *JMeter*. No entanto não foram realizadas variações no número de nós da *Blockchain*.

Zheng et al. (2018) propõe em seu trabalho métricas gerais para avaliação de desempenho, que podem ser utilizadas em diferentes estágios da *Blockchain*. Tais avaliações visam resolver o problema de desempenho da rede que, com as características de descentralização, em muitos casos não possui monitoramento de desempenho padrão. Essa abordagem pode se adaptar automaticamente a diferentes sistemas, fornecendo informações detalhadas e de desempenho em tempo real.

[1] Os *Smart Contracts* consistem em códigos computacionais criados com o propósito de facilitar a execução e o cumprimento de um acordo, através de uma *Blockchain*, de forma automática e segura (SZABO, 1996).
[2] Docker é uma plataforma que usa virtualização para criar software em pacotes chamados *containers*. Os *containers* são isolados uns dos outros e agrupam seus próprios *softwares*, bibliotecas e arquivos de configuração.

Nos trabalhos relacionados encontrados atualmente na literatura, é possível perceber que a tecnologia *Blockchain* pode ser utilizada com o propósito de conferir mais segurança e confiabilidade aos ambientes IoT. No entanto este trabalho vai além, pois realiza uma avaliação de desempenho de uma *Blockchain*, considerando as métricas de vazão e tempo de resposta (ZENG et al., 2018), porém variando a dimensão da *Blockchain*, o que permite mensurar o seu comportamento em diferentes cenários e uso.

3. Conceitos e Definições

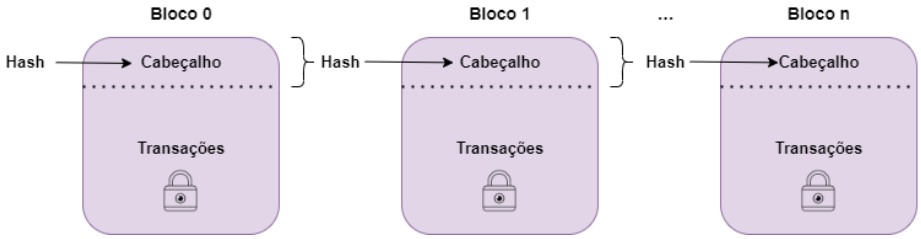
Esta seção apresenta os principais conceitos abordados neste trabalho. Explica brevemente a tecnologia *Blockchain*, como se dá o seu funcionamento e como a sua estrutura é organizada. Também aborda o conceito de IoT e suas aplicabilidades.

3.1 Blockchain

De acordo com Braga, Marino e Santos (2017), *Blockchain* trata-se de uma base de dados de transações distribuída e compartilhada por nós de um sistema distribuído organizado como uma rede peer-to-peer (P2P). Consiste em um ambiente seguro para o registro de transações, pois uma vez que um novo bloco é adicionado ele não pode ser removido ou modificado, sem que isso seja percebido pelos demais nós em toda a rede.

No contexto da IoT, *Blockchain* pode ser utilizada para autenticar, autorizar e auditar os dados gerados pelos dispositivos. Devido a sua natureza descentralizada não há necessidade de confiança em terceiros, o que torna o risco de falhas no sistema menor. (CHICARINO et al., 2017). Na figura 1 é representada a estrutura dos blocos e o seu encadeamento.

Figura 1 – Estrutura da *Blockchain*.



Fonte: Autoria própria (2021).

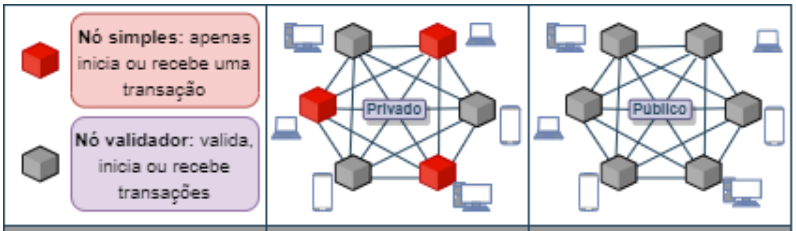
De acordo com Zheng et al. (2018) existem alguns conceitos principais relacionados a *Blockchain*, os quais são detalhadas a seguir:

- Transação: consiste nas operações executada na rede, como transferências financeiras, registro de dados, etc. As transações, ao serem criadas, são agrupadas em blocos, que serão validados e transmitidas para toda a rede, assim cada nó da *Blockchain* conterá uma cópia exata de toda a cadeia de blocos;
- Bloco: estrutura de dados utilizada para gravar um conjunto de transações que ocorreram num certo intervalo de tempo. Um bloco possui duas partes: o cabeçalho, que contém dados de identificação; e o conteúdo, onde são armazenadas as transações;
- Hash: consiste em um código de identificação único para cada bloco, gerado no momento que ele é adicionado a cadeia de blocos. Permite o encadeamento da *Blockchain*, pois cada bloco armazena o valor do hash do anterior, com isso é possível percorrer todos a cadeia até atingir o bloco inicial, conhecido como bloco gênesis.

- Protocolos de Consenso: antes de cada bloco ser adicionado ele precisa ser validado para garantir a integridade da rede. Este processo é realizado através de protocolos de consenso, sendo os mais utilizados o de prova de trabalho (do inglês, *Proof-of-work* - PoW) ou de uma prova de participação (do inglês, *proof-of-stake* - PoS), que se utilizam de poder de processamento computacional para solucionar cálculos matemáticos.

A tecnologia *Blockchain* pode ser classificada em dois grupos: públicas ou de acesso aberto, onde o acesso pode ser anônimo, as aplicações têm característica aberta e a própria rede segue suas próprias regras; e redes privadas ou de acesso autorizado, que oferecem acesso a usuários identificados, autenticados e autorizados. Nessas redes, os usuários não são anônimos, mas sim grupos selecionados de usuários conhecidos. A figura 2 apresenta algumas das principais características das redes citadas anteriormente.

Figura 2 – *Blockchain* privada x *Blockchain* pública.



Acesso à rede	Necessita de autorização	Acesso aberto
Quem regulamenta	Legislações e regulações	Protocolos de consenso
Quem são os validadores	Grupo pré-selecionado	Anônimos
Potenciais aplicações	Ambientes corporativos	Aplicações abertas

Fonte: Autoria própria (2021).

3.2 Internet das Coisas (IoT)

Trata-se de uma tecnologia cujo objetivo é fazer com que coisas do cotidiano, tais como dispositivos portáteis ou eletrodomésticos, se conectem a Internet. A IoT suporta integração, transferência e análise de dados gerados por sensores e dispositivos inteligentes. Sua aplicação viabiliza o desenvolvimento de diversos conceitos inovadores, como as cidades inteligentes e infraestruturas de serviços que melhoram exponencialmente a qualidade de vida, utilizando-se de todos os seus recursos disponíveis (MENDEZ; PAPAPANAGIOTOU; YANG, 2018).

A conectividade ubíqua[1] é um requisito crucial para a IoT. Para atender a este requisito, as aplicações necessitam do suporte de diversos dispositivos e protocolos de comunicação, desde pequenos sensores que capturam dados, até servidores, utilizados para analisar estes dados e extrair informações. Tudo isso requer uma grande integração entre dispositivos móveis, dispositivos de ponta como roteadores e hubs inteligentes e controladores, que irão gerenciar a coleta e processamento das informações (SAGIRLAR et al., 2018).

Os principais elementos da IoT são: sensores, chamadas de serviços remotos, redes de comunicação e processamento de eventos com reconhecimento de contexto. No contexto da IoT a interconectividade entre entidades é um requisito crítico para o seu bom funcionamento, assim sua arquitetura deve garantir que tanto as entidades físicas como as virtuais operem em conjunto de maneira impecável, garantindo uma operação onde a confiabilidade seja garantida.

[1] Dispositivos conectados em todos os lugares de forma que mal se pode perceber que eles estão lá.

Monitorar as informações que percorre uma rede desse tipo é um dos principais tópicos de preocupação da IoT. Existem alguns pontos a serem considerados para uma rede IoT ser tida como confiável: a autenticação segura; a transmissão segura de dados; a segurança dos dados utilizados pelos dispositivos de IoT; o acesso seguro aos dados por pessoas autorizadas; e a utilização de protocolos de autenticação devidamente estruturados (SCHNEIDER, 2018).

Para assegurar os pontos de segurança mencionados, é necessário a adoção de métodos que garantam a integridade e autenticidade dos dados em todo o sistema IoT. Para isso é possível fazer uso da tecnologia *Blockchain* e dos *Smart Contracts*, que poderão ser usados para registras as atividades dos dispositivos, sensores, atuadores, dentre outras coisas. Os *Smart Contracts* não necessitam do envolvimento de terceiros para gestão de confiança, assim apresentam-se como um método promissor para conferir mais segurança aos dados da IoT.

4. Metodologia

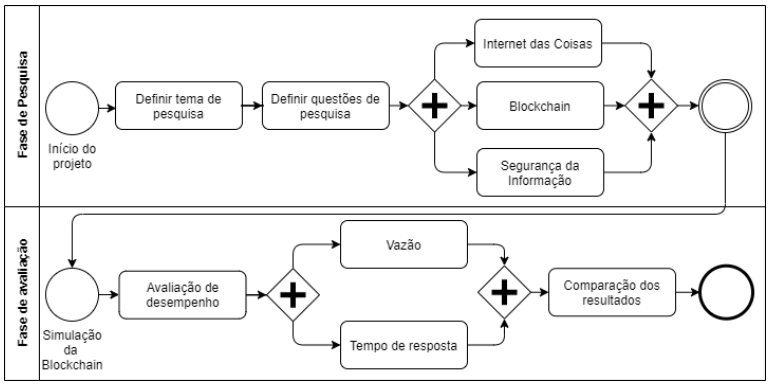
A metodologia deste trabalho, quanto a sua natureza, classifica-se como uma pesquisa descritiva, pois realiza um estudo detalhado sobre um tema, com coleta, análise e interpretação de dados. Quanto ao método científico utilizado, é classificado como uma pesquisa indutiva.

No método indutivo parte-se da observação de fenômenos que se deseja conhecer. Inicia-se a pesquisa sobre uma questão específica para depois explorar questões mais amplas. Após esse processo são realizadas comparações entre esses dois pontos e com isso, procede-se à generalização, baseando-se nos estudos que identificam a relação entre os objetos observados (PRODNOV; FREITAS, 2013).

Os objetivos de estudo deste trabalho são classificados como explicativos, pois visam proporcionar uma maior compreensão sobre um problema. Os procedimentos técnicos utilizados seguiram a metodologia de avaliação de desempenho de uma *Blockchain,* proposta por Morais, Lins e Callou (2020), que propõem os seguintes passos: definição dos objetivos de estudo, simulação de uma *Blockchain*, seleção de métricas para avaliação de desempenho, aplicação de cargas de trabalho e análise dos resultados e conclusões.

A figura 3 apresenta o passo a passo de execução dessa pesquisa. Após a definição do tema, iniciou-se a revisão bibliográfica sobre o uso de *Blockchain* para IoT. Em seguida realizou-se uma simulação de *Blockchain*, que permite variar a quantidade de nós, e uma avaliação de desempenho, considerando as métricas de vazão e tempo de resposta. Por fim, realizou-se um comparativo entre os resultados obtidos e os dados encontrados na literatura.

Figura 3 – Metodologia aplicada na realização deste trabalho.



Fonte: Autoria própria (2021).

5. Resultados e Discussões

Esta seção apresentada a simulação da *Blockchain* realizada para este trabalho e descreve a avaliação de desempenho, utilizando as métricas de vazão e tempo de resposta. A seguir são apresentadas as principais ferramentas utilizadas neste projeto:

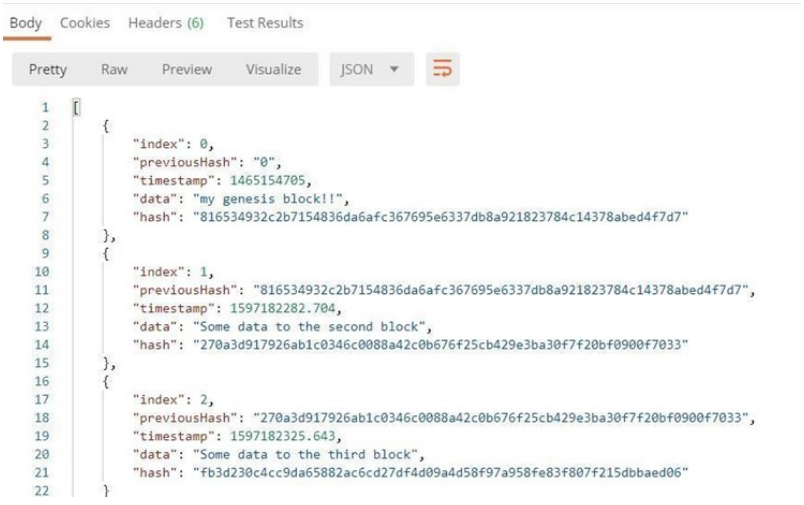
- *Node.js*: utilizado para a simulação da *Blockchain*. Consiste em um interpretador de *JavaScript*, cuja principal vantagem de utilização se dá pela boa performance apresentada e pelo seu alto desempenho.
- *GIT*: utilizado para uma melhor organização do código e para controle de versões. Para este projeto foi utilizado um repositório na plataforma *GitHub*.
- *Visual Studio*: editor de texto que suporta uma grande quantidade de linguagens de programação.
- *Postman*: ferramenta utilizada para a realização dos testes da simulação da *Blockchain*. Permite testar serviços por meio do envio de requisições HTTP e da análise do seu retorno.

5.1 Simulação da Blockchain

Para realizar a simulação de uma *Blockchain*, foi utilizada como base a aplicação proposta por Hartikka (2017) desenvolvida em *Node.js*. Optou-se pelo uso de simulação, pois ela permite entender e avaliar o comportamento de um sistema e realizar experimentos sobre ele (MORAIS et al., 2021). A estrutura principal da *Blockchain* simulada neste trabalho consiste de uma interface HTTP que controla os nós; *WebSockets*, que permitem a comunicação entre os nós e implementação de protocolos de comunicação P2P.

Ao ser inicializada, a *Blockchain* cria o bloco gênesis. A partir desse momento é possível adicionar mais blocos a cadeia. A figura 4 apresenta a estrutura de dados da *Blockchain* após a adição de dois blocos.

Figura 4 – Inserção de blocos na *Blockchain*.



Fonte: Autoria própria (2021).

Todos os blocos da *Blockchain* contêm o mesmo conjunto de informações, que consistem em:

- *index*: representa a posição do bloco na cadeia;
- *previousHash*: informação referente ao hash do bloco anterior;
- *timestamp*: corresponde ao registro de data e hora em que o bloco foi inserido na *Blockchain*;
- *data*: trata-se dos dados e informações que são incluídas na *Blockchain* a cada transação;
- *hash*: corresponde ao identificador do bloco atual. É formada pela junção das informações:

index + previousHash + timestamp + data.

5.2 Seleção das Métricas de Validação

Para a escolha das métricas utilizadas na avaliação de desempenho tomou-se como base a proposta de Zheng et al. (2018), onde são detalhadas diversas métricas para avaliação de desempenho de *Blockchain*. Foram escolhidas as métricas de vazão, que calcula o número de transações por segundo; e tempo de resposta, que considera o atraso médio de cada resposta.

5.2.1 Vazão - Transações por Segundo

As *Blockchains* apresentam velocidades diferentes para implantar e executar Smart Contracts. Para mensurar este tempo, é necessário que a taxa de transferência seja monitorada por um certo período, assim obtêm-se o número de transações por segundo. Durante o intervalo de tempo de t_i a t_j, as transações por segundo de cada par pode ser calculado pela equação:

$$TPS_u = \frac{Count\ (T_x\ in\ (t_i,t_j))}{t_j - t_i}(txs/s)$$

Onde TPS significa *Transactions Per Second*. Transação está abreviada como T_x. Ao considerar a taxa de transferência de N pares, pode-se calcular a média com:

$$\overline{TPS} = \frac{\sum u\ TPS_u}{N}(txs/s)$$

5.2.2 Tempo de Resposta

Há um intervalo entre o momento em que a transação é enviada à cadeia de blocos e o momento em que ela é de fato adicionada à *Blockchain*. Por exemplo, ao implantar um *Smart Contract* na *Blockchain*, é necessário aguardar um momento até que o mesmo seja confirmado e possa receber requisições. O atraso médio de resposta de cada par é dado pela equação:

$$ARD_u = \frac{\sum Tx\ (t_{Tx_{confirmed}} - t_{Tx_{input}})}{Count\ (Tx\ in\ (t_i,t_j))}(txs/s)$$

Onde ARD significa *Average Response Delay*. Quando considerado o atraso na resposta de todos os contratos inteligentes, pode-se calcular a média do seguinte modo:

$$\overline{ARD} = \frac{\sum u\ ARD_u}{N}(txs/s)$$

5.3 Aplicação das Métricas

Para a avaliação de desempenho foram realizados três conjuntos de testes para cada uma das métricas selecionadas. Cada conjunto de testes consiste em uma variação da quantidade de nós combinada a uma variação da quantidade de blocos.

Os testes foram executados em um ambiente de hardware com as seguintes características: Processador *Core i*5-7200U (3MB *Cache*, 3.1 GHz); memória RAM 8GB (1x8GB) 2400MHz DDR4; placa de vídeo dedicada NVIDIA *GeForce* 940MX 4GB GDDR5. Na tabela 1 é apresentado a organização dos

conjuntos de testes:

Tabela 1 – Conjuntos de Testes.

Conjuntos	Nós	Blocos
1º Conjunto	10	1.000
	20	1.000
	40	1.000
2º Conjunto	10	10.000
	20	10.000
	40	10.000
3º Conjunto	10	100.000
	20	100.000
	40	100.000

Fonte: autoria própria.

A primeira métrica avaliada foi a de vazão, onde é calculada a quantidade de transações por segundo processadas pela *Blockchain*. Para o primeiro conjunto de testes considerou-se uma quantidade de 1.000 blocos, variando a quantidade de nós da *Blockchain* em 10, 20 e 40. Os resultados obtidos são apresentados na Tabela 2.

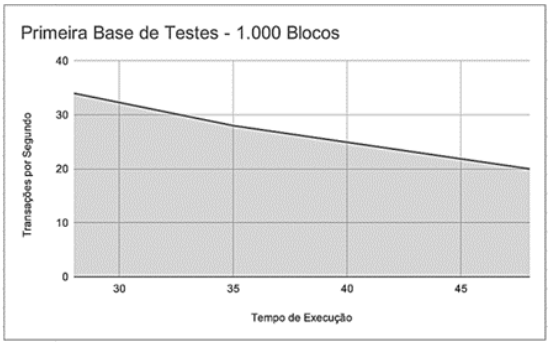
Tabela 2 – 1º Conjunto de Testes - Transações por Segundo.

1º Conjunto de Testes	Nós	Blocos	Transações por segundo
1º Teste	10	1.000	Tempo de Execução: 28,59 segundos **Transações por Segundo:** 34,96
2º Teste	20	1.000	Tempo de Execução: 35,69 segundos **Transações por Segundo:** 28,01
3º Teste	40	1.000	Tempo de Execução: 48,56 segundos **Transações por Segundo:** 20,59

Fonte: autoria própria.

A quantidade de transações por segundo obtida neste primeiro conjunto de testes é apresentada no gráfico da figura 5. É possível notar que quanto maior a base de testes, a quantidade de transações por segundos diminui.

Figura 5 – Primeiro conjunto de testes - 1.000 Blocos.



Fonte: Autoria própria (2021).

Para o segundo conjunto de testes considerou-se uma quantidade de 10.000 blocos, variando

novamente a quantidade de nós da *Blockchain* em 10, 20 e 40. Os resultados obtidos são apresentados na Tabela 3.

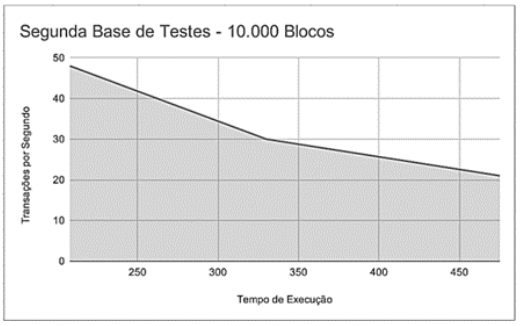
Tabela 3 – 2º Conjunto de Testes - Transações por Segundo.

2º Conjunto de Testes	Nós	Blocos	Transações por segundo
1º Teste	10	10.000	Tempo de Execução: 208,2 segundos **Transações por Segundo:** 48,02
2º Teste	20	10.000	Tempo de Execução: 330,09 **Transações por Segundo:** 30,29
3º Teste	40	10.000	Tempo de Execução: 475,18 **Transações por Segundo:** 21,04

Fonte: autoria própria.

A quantidade de transações por segundo obtida neste segundo conjunto de testes é apresentada no gráfico da figura 6. Novamente é possível perceber há uma diminuição na quantidade de transações por segundos a medida em que a base de testes aumenta.

Figura 6 – Segundo conjunto de testes - 10.000 Blocos.



Fonte: Autoria própria (2021).

Para o terceiro conjunto de testes considerou-se uma quantidade de 100.000 blocos, variando novamente a quantidade de nós da *Blockchain* em 10, 20 e 40. Os resultados obtidos são apresentados na Tabela 4.

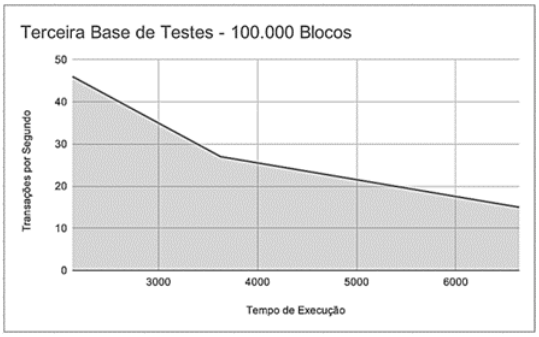
Tabela 4 – 3º Conjunto de Testes - Transações por Segundo.

3º Conjunto de Testes	Nós	Blocos	Transações por segundo
1º Teste	10	100.000	Tempo de Execução: 2.133 segundos **Transações por Segundo:** 46,88
2º Teste	20	100.000	Tempo de Execução: 3.627 segundos **Transações por Segundo:** 27,56
3º Teste	40	100.000	Tempo de Execução: 6.639 segundos **Transações por Segundo:** 15,06

Fonte: autoria própria.

A quantidade de transações por segundo neste terceiro conjunto de testes é apresentada no gráfico da figura 7. Neste teste o mesmo comportamento se repete, pois quão maior a quantidade de nós e de blocos, maior será o tempo até que sua verificação seja concluída. Desse modo, pode-se observar uma perda de desempenho ao longo das execuções.

Figura 7 – Terceiro conjunto de testes - 100.000 Blocos.



Fonte: Autoria própria (2021).

A segunda métrica a ser considerada durante a avaliação de desempenho foi a de tempo de resposta, onde é calculada o atraso médio de resposta da *Blockchain*. Para o primeiro conjunto de testes considerou-se uma quantidade de 1.000 blocos, variando a quantidade de nós da *Blockchain* em 10, 20 e 40. Os resultados obtidos são apresentados na Tabela 5.

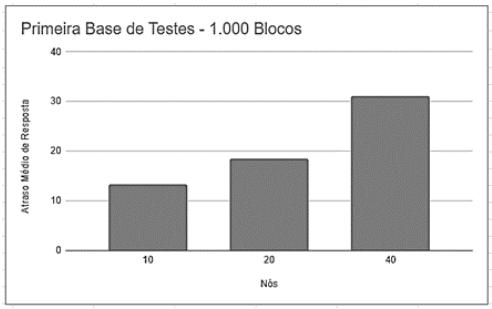
Tabela 5 – 1º Conjunto de Testes - Atraso Médio de Resposta.

1º Conjunto de Testes	Nós	Blocos	Atraso Médio de Resposta
1º Teste	10	1.000	13,27 s
2º Teste	20	1.000	18,55 s
3º Teste	40	1.000	31,07 s

Fonte: autoria própria.

O resultado obtido neste primeiro conjunto de testes é apresentado no gráfico da figura 8. É possível notar que a taxa de atraso médio de resposta aumenta de acordo com a adição de mais nós em cada teste.

Figura 8 – Primeiro conjunto de testes - 1.000 Blocos.



Fonte: Autoria própria (2021).

Para o segundo conjunto de testes considerou-se uma quantidade de 10.000 blocos, variando novamente a quantidade de nós da *Blockchain* em 10, 20 e 40. Os resultados obtidos são apresentados na Tabela 6.

Tabela 6 – 2º Conjunto de Testes - Atraso Médio de Resposta.

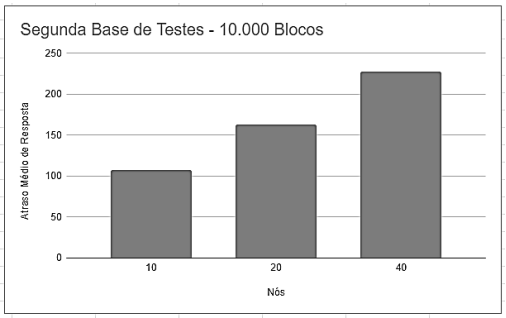
2º Conjunto de Testes	Nós	Blocos	Atraso Médio de Resposta
1º Teste	10	10.000	107,56 s
2º Teste	20	10.000	163,36 s
3º Teste	40	10.000	227.82 s

Fonte: autoria própria.

A taxa de atraso médio de resposta obtida neste segundo conjunto de testes é apresentada no gráfico

da figura 9. Novamente é possível perceber um crescimento dos valores de tempo a medida em que a base de testes aumenta.

Figura 9 – Segundo conjunto de testes - 10.000 Blocos.



Fonte: Autoria própria (2021).

Para o terceiro conjunto de testes considerou-se 100.000 blocos, variando a quantidade de nós da *Blockchain* em 10, 20 e 40. A Tabela 7 apresenta os resultados obtidos.

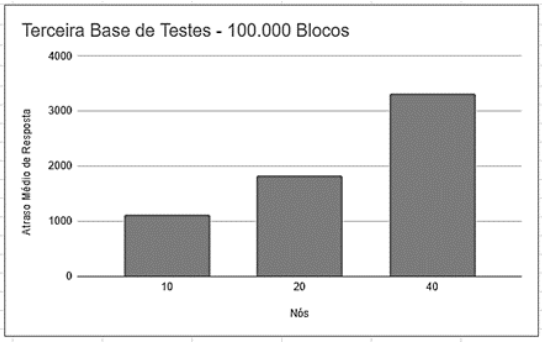
Tabela 7 – 3º Conjunto de Testes - Atraso Médio de Resposta.

3º Conjunto de Testes	Nós	Blocos	Atraso Médio de Resposta
1º Teste	10	100.000	1.121,50 s
2º Teste	20	100.000	1.833,62 s
3º Teste	40	100.000	3.319,52 s

Fonte: autoria própria.

A taxa de atraso médio de resposta obtida neste segundo conjunto de testes é apresentada no gráfico da figura 10. Também neste teste é possível perceber um crescimento considerável dos valores de tempo a medida em que a base de testes aumenta.

Figura 10 – Terceiro conjunto de testes - 100.000 Blocos.



Fonte: Autoria própria (2021).

Após a realização da avaliação de desempenho realizou-se um comparativo dos resultados obtidos com os dados apresentados por Zheng et al. (2018), que em seu trabalho buscaram responder a seguinte questão de pesquisa: como é a performance detalhada da *Blockchain* em diferentes situações?

De acordo com os autores a performance é um dos principais requisitos em sistemas *Blockchain*. O trabalho afirma que dois tipos de análises devem ser feitos: análise de performance geral, utilizada para selecionar a *Blockchain* que atende melhor ao usuário final; e análise de performance detalhada, que provê informações sobre todo o processo de execução da *Blockchain*, permitindo identificar e solucionar pontos de gargalo. Diante disso, este trabalho buscou dar ênfase as métricas de performance geral: *vazão* e tempo *de resposta*.

Os autores afirmam que sistemas *Blockchain* com protocolos de consenso *Proof-of-Work* possuem uma performance mais baixa do que os que possuem outros tipos de protocolos, apesar de que este protocolo assegura um maior nível de segurança a rede. Sugerem ainda que o PoW seja evitado em cenários em que ocorram um grande tráfego de dados. A simulação realizada neste trabalho não utiliza esse protocolo, desse modo, é possível comparar algumas características encontradas com os resultados de Zheng et al. (2018).

No trabalho de referência são testados 4 tipos de *Blockchain*: *Ethereum*, *Parity*, *Hyperledger Fabric* e CITA. A seguir são detalhadas brevemente cada uma das redes (ZHENG et al. 2018).

- *Ethereum*: *Blockchain* pública de código aberto utilizada para o desenvolvimento de aplicativos descentralizados e *Smart Contracts*. Utiliza o protocolo de consenso PoW.
- *Parity*: consiste em outra versão da *Ethereum*. Utiliza um protocolo de consenso chamado PoA (*Proof os Authority*), com ele é possível obter uma maior taxa de transferência em comparação ao PoW utilizado na rede *Ethereum* original.
- *Hyperledger Fabric*: sua principal característica é a fácil adaptação em ambientes como contêineres para a hospedagem de contratos inteligentes, chamados de "*chaincode*".
- CITA: sigla de *Cryptape Inter-enterprise Trust Automation*. Utiliza micros serviços para impulsionar a performance da rede. Com isso, a lógica dos nós pode ser escalada para *clusters* de servidores.

Para os testes os autores consideram uma base contendo 1000 blocos em execução, desse modo optou-se por comparar aqui os dados obtidos nos testes em que forma utilizados também 1.000 blocos, considerando a *Blockchain* com 40 nós (Tabela 2). O trabalho de referência não detalha os resultados para a métrica *Atraso Médio de Resposta*. Na Tabela 11, mostrada a seguir, estão os resultados para a métrica de Vazão.

Tabela 11 – Comparativo dos Resultados.

Blockchain	**Vazão (transações por segundo)**
Ethereum	5,55
Parity	3,95
Hyperledger Fabric	600,61
CITA	256,63
Este trabalho (40 nós, 1000 blocos)	20,59

Fonte: Zheng et al. (2018).

As *Blockchains Hyperledger Fabric* e CITA processam uma maior taxa de transações por segundo, devido ao protocolo de consenso utilizado. Na *Ethereum* e *Parity* a utilização do protocolo de consenso PoW, que demanda mais recursos computacionais torna o registro mais seguro, porém acarreta em uma taxa de vazão consideravelmente menor. A *Blockchain* simulada neste trabalho não utiliza protocolos de consenso PoW, desse modo, pode-se observar que ela irá executar mais transações por segundo do que as redes *Ethereum* e *Parity*, demonstrando que, de fato, existe um custo computacional maior associado ao uso desse tipo de protocolo.

Diferentes metodologias podem ser adotadas para implementação de *Blockchains*. Por exemplo, com PoW alguns nós precisam trabalhar como mineradores, o que gera um alto custo de hardware e consumo de energia para realizar a prova de trabalho e atingir o consenso. Ou seja, *Blockchains* que lidam com protocolos PoW são capazes de manter taxas de transferências relativamente baixas, enquanto que uma rede que não

utiliza esse tipo de protocolo irá utilizar menor recursos computacionais para validar os blocos e atingir o consenso. A avaliação de desempenho realizada pode indicar alguns pontos relevantes, tais como:

- Algumas aplicações IoT necessitam de um rápido tempo de resposta, onde demoras de processamento podem acarretar em problemas reais para o usuário.
- É necessário considerar cada cenário como único. Ao projetar soluções IoT baseadas em *Blockchain* é preciso levar em consideração o desempenho e o nível de segurança requeridos, para oferecer a solução mais adequada a cada cenário, garantindo um bom fluxo de execução que não irá sobrecarregar os dispositivos IoT ou a rede.
- Protocolos de consenso são a chave para definir a viabilidade da utilização de um tipo de *Blockchain* aplicada a IoT. Aplicações que demandam uma maior vazão e tempo de resposta devem utilizar protocolos que tenham um menor custo de recursos computacionais, evitando assim, sobrecarga nos dispositivos que inviabilizem seu uso.

6. Considerações Finais

Internet das Coisas é uma tecnologia que pode ser aplicada em diferentes contextos e possui potencial para revolucionar a maneira como utilizamos as coisas ao nosso redor. Para isso é preciso gerenciar com eficiência um grande número de dispositivos conectados e trocando dados entre si. A maioria das soluções atualmente são baseadas em infraestruturas centralizadas. Diante disso a tecnologia *Blockchain* surge como uma alternativa a ser utilizada para o registro descentralizado de dados da IoT, no entanto é necessário avaliar a viabilidade de uso de tal tecnologia em termos de desempenho.

Este trabalho realizou uma simulação de uma *Blockchain* e apresentou uma avaliação de desempenho, onde foi possível alterar a quantidade de nós da rede para, com isso, analisar o seu comportamento em diferentes situações. Inicialmente foi realizado um estudo bibliográfico a respeito das temáticas abordadas. Em seguida foram escolhidas duas métricas para avaliação de desempenho: vazão e tempo de resposta. Por fim, foram aplicadas tais métricas na *Blockchain* simulada, visando analisar a utilização de tal tecnologia em sistemas IoT e, posteriormente, foram discutidos e apresentados os resultados, comparando-os com o estudo de referência.

A principal contribuição cientifica apresentada por este trabalho é a simulação e a avaliação de desempenho de uma *Blockchain*, que permite mensurar o seu comportamento antes de implementar uma solução para Internet das Coisas. As principais limitações deste trabalho se deram devido as restrições do ambiente de teste, que podem ter impactado nos resultados finais. Como trabalhos futuros é possível repetir os testes aqui realizados, considerando outras métricas e aplicando-os em outra *Blockchain*, com diferentes protocolos de consenso e com dados reais de dispositivos IoT. Também é possível a realização de testes que tenham como foco o hardware dos dispositivos IoT para validar o comportamento de cada ponto da rede, validando quais momentos de execução da *Blockchain* podem ser otimizados, melhorando assim o desempenho total.

Referências

Braga, A. M., Marino, F. C. H., & dos Santos, R. R. (2017). **Segurança de aplicaçoes blockchain além das criptomoedas**. *Livro-texto dos minicursos SBSeg*, 99-148.

Chicarino, V. R., Jesus, E. F., Albuquerque, C. V. N., & Aragão Rocha, A. A. (2017). **Uso de blockchain para privacidade e segurança em internet das coisas**. *Livro de Minicursos do VII Simpósio Brasileiro de*

Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, *28*.

Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020, November). **A blockchain solution for enhancing cybersecurity defence of IoT**. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 490-495). IEEE.

Han, R., Gramoli, V., & Xu, X. (2018, February). **Evaluating blockchains for IoT**. In *2018 9Th IFIP international conference on new technologies, mobility and security (NTMS)* (pp. 1-5). IEEE.

Hartikka, L. (2017) **A Blockchain in 200 lines of code**. Disponível em: https://medium.com/@lhartikk/ablockchain-in-200-lines-of-code-963cc1cc0e54. Acesso em: 06/09/2021.

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. ***Information Security Journal: A Global Perspective***, *27*(3), 162-182.

Mikkelsen, L., Mortensen, K., Rasmussen, H., Schwefel, H. P., & Madsen, T. (2018, December). **Realization and evaluation of marketplace functionalities using ethereum blockchain**. In *2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)* (pp. 47-52). IEEE.

Morais, A. M., de Almeida Callou, G. R., & Lins, F. A. A. (2020). Simulação e Avaliação de Desempenho de uma Rede Blockchain Utilizando Containers Docker. **Cadernos do IME-Série Informática**, 44, 73-87.

Morais, A. M., Neto, J. D. S. C., de Medeiros, R. W. A., de Oliveira Nóbrega, O., & Lins, F. A. A. (2021). A solution for integrating virtual learning environments with Blockchain. ***Research, Society and Development***, *10*(12).

Pilkington, M. (2016). **Blockchain technology: principles and applications**. In *Research handbook on digital transformations*. Edward Elgar Publishing.

Prodanov, C. C., & De Freitas, E. C. (2013). ***Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico****-2ª Edição*. Editora Feevale.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. ***Future generation computer systems***, *88*, 173-190.

Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., & Ragnoli, E. (2018, July). **Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains**. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1007-1016). IEEE.

Schneider, E. (2018). Internet of Things (IoT) Technology, Economic View and Technical Standardization. *Institut Luxembourgeois de La Normalisation*, *July*, 108. https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-iot-july-2018.pdf. Acesso em: 30/10/2020.

Zheng, P., Zheng, Z., Luo, X., Chen, X., & Liu, X. (2018, May). **A detailed and real-time performance monitoring framework for blockchain systems**. In *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP)* (pp. 134-143). IEEE.