KOKOUVI HOLA KANYI KODJOVI

ANALISE CRÍTICA DOS LIMITES DO BLOCKCHAIN EM RELACÃO A ESCALABILIDADE E CAPACIDADE DE PROCESSAMENTO DE TRANSACÕES EM GRANDE ESCALA

(*compiled at May 15, 2024*)

Trabalho do conclusão do curso de bacharelado em Ciências de computação .

Área de concentração: *Ciência da Computação*.

Orientador: Eduardo Todt.

CURITIBA PR

2023

RESUMO

O Blockchain é uma tecnologia inovadora com o potencial de transformar diversos setores, desde serviços financeiros até cadeias de suprimentos. No entanto, sua adoção em larga escala tem enfrentado desafios significativos relacionados à escalabilidade e à capacidade de processamento de transações. A escalabilidade refere-se à capacidade do Blockchain de lidar com um grande número de transações e usuários sem comprometer a eficiência. À medida que mais participantes se juntam à rede, os tempos de confirmação de transações aumentam, tornando o Blockchain ineficiente em grande escala. O aumento do volume de transações também coloca pressão nos recursos computacionais necessários para validá-las. Outros desafios incluem o armazenamento contínuo de dados, à medida que o Blockchain cresce, e questões de governança e coordenação à medida que a rede envolve múltiplas organizações. Pesquisadores e desenvolvedores têm explorado soluções, como Blockchains de segunda camada, novos algoritmos de consenso (como Prova de Participação e Prova de Autoridade), e técnicas de dimensionamento horizontal. Este estudo aborda minuciosamente a problemática da escalabilidade e o desempenho do Blockchain, oferecendo uma análise aprofundada sobre como a escalabilidade representa um desafio premente nas redes blockchain. Além disso, são explorados os avanços tecnológicos que visam aprimorar e solucionar essa questão, destacando a importância de superar os obstáculos inerentes à expansão eficiente dessas redes.A escalabilidade do Blockchain é fundamental, e apesar dos desafios, o potencial disruptivo do Blockchain continua a atrair investimentos e inovações. À medida que a pesquisa e a colaboração avançam, soluções promissoras são esperadas para permitir que o Blockchain atinja seu pleno potencial em diversos setores.

ABSTRACT

Blockchain is an innovative technology with the potential to transform various sectors, from financial services to supply chains. However, its widespread adoption has faced significant challenges related to scalability and transaction processing capacity. Scalability refers to the ability of Blockchain to handle a large number of transactions and users without compromising efficiency. As more participants join the network, transaction confirmation times increase, making Blockchain inefficient on a large scale. The growing transaction volume also puts pressure on the computational resources required to validate them. Other challenges include continuous data storage as Blockchain expands, and governance and coordination issues as the network involves multiple organizations. Researchers and developers have explored solutions, such as second-layer Blockchains, new consensus algorithms (such as Proof of Stake and Proof of Authority), and horizontal scaling techniques. This study thoroughly addresses the scalability issues and performance of Blockchain, providing a detailed analysis of how scalability poses a pressing challenge in blockchain networks. Additionally, technological advances aimed at improving and resolving this issue are explored, emphasizing the importance of overcoming inherent obstacles to the efficient expansion of these networks. Blockchain scalability is crucial, and despite the challenges, the disruptive potential of Blockchain continues to attract investments and innovations. As research and collaboration progress, promising solutions are expected to enable Blockchain to reach its full potential in various sectors.

LIST OF ACRONYMS

PoW	Proof of Work
TPS	Transações Por Segundo
HLF	Hyperledger Fabric
YMSC	Yet Another Scalability Challenge
PBFT	Practical Byzantine Fault Tolerance
IOHeavy	Input/Output Heavy
PCC	Prova de Conjectura de Collatz (Collatz Conjecture Proof)

LIST OF FIGURES

LIST OF TABLES

CONTENTS

1 INTRODUÇÃO

A tecnologia blockchain redefine de maneira fundamental a condução de transações, a assinatura de contratos e a realização de diversas operações, eliminando a necessidade de aprovações centralizadas para validação [1]. Essa inovação estabelece um registro distribuído de transações, verificado por uma rede de computadores e organizado em blocos, criando uma cadeia de informações imutáveis e resistentes à adulteração [2, 3].

Embora as origens do blockchain remontem à década de 1990, quando Stuart e W. Scott Stornetta apresentaram a "árvore de carimbos de tempo" para garantir a integridade de registros digitais, foi apenas em 2008 que a tecnologia ganhou destaque com a publicação do artigo seminal de Satoshi Nakamoto sobre o Bitcoin [4].

Apesar das conquistas e inovações, o blockchain enfrenta desafios cruciais, incluindo escalabilidade, custos de transações, interoperabilidade, privacidade e segurança [5]. A escalabilidade, em particular, emerge como um desafio proeminente, limitando a quantidade de transações que as redes blockchain podem processar, o que impacta sua aplicabilidade em setores de alto volume, como sistemas de pagamento em larga escala [6].

A avaliação da escalabilidade, geralmente medida em Transações por Segundo (TPS), destaca a importância do tamanho dos blocos e dos algoritmos de consenso, como o Proof-of-Work (PoW), na eficiência da rede. Enquanto blocos maiores podem aumentar a capacidade, há o risco de centralização e demanda por mais recursos de armazenamento. Além disso, considerações sobre privacidade e complexidade dos protocolos também influenciam a capacidade de processamento de transações [7].

Este trabalho tem como objetivo explorar os limites do Blockchain em relação à escalabilidade e capacidade de processamento de transações em grandes escalas, utilizando métodos sistemáticos de análise de literatura. Apesar de ser uma tecnologia revolucionária com grande potencial para transformar diversos setores, o Blockchain apresenta desafios que podem afetar sua eficiência em larga escala.

A análise crítica concentra-se nos desafios inerentes à escalabilidade e capacidade de processamento em larga escala nas blockchains, examinando aspectos técnicos, como armazenamento, tempos de confirmação, processamento de nós e eficiência energética, enquanto explora questões de governança e adoção generalizada.

Para embasar essa análise crítica, apresentamos uma variedade de perspectivas sobre os desafios de escalabilidade no contexto das blockchains, destacando limitações atuais e explorando soluções propostas pela comunidade acadêmica e pela indústria. Essa abordagem busca informar e orientar futuros desenvolvimentos na busca por

soluções mais eficazes e sustentáveis para os desafios enfrentados pela tecnologia blockchain.

2 FUNDAMENTOS DA BLOCKCHAIN

O Blockchain é uma tecnologia nascente de 2009, usado por Nakamoto Satoshi [8],que está transformando o mundo da tecnologia e dos negócios por sua transparência, descentralização e propriedades de segurança. Desde então, ganhou muita atenção com a sua primeira aplicação de criptomoedas, como o Bitcoin.

O conceito do blockchain, que é uma palavra em inglês e significa uma cadeia de blocos, foi apresentado por STUART HABER e AL em 1991 como um meio de marcar digitalmente documentos eletrônicos com data e horas para protegê-los contra adulteração [9]. A proposta inicial do Blockchain era resolver o problema da centralização, em que se precisava de terceiros confiáveis para processar uma transação digital [10].

Assim que entra em ação a função do blockchain, que é definida nesse caso como uma cadeia de blocos digitais conectados e associados uns aos outros como um livro razão distribuído aberto que armazena informações sobre as operações que estão sendo feitas dentro dos blocos. A tecnologia Blockchain é aplicada em diferentes áreas e é diversificada em vários tipos, tais como:

- Blockchains públicos: são aqueles que estão descentralizados e permitem a integração de qualquer pessoa à rede, assim conseguindo gerenciá-los.

- Blockchains privados: são aqueles que só aceitam a integração de pessoas de uma única rede e gerenciá-las.

- Blockchain de consórcio: são aqueles que estão entre os blockchains públicos e privados, em termos de permissões e gerenciamento. Eles permitem a integração de pessoas de várias organizações.

O blockchain, como o próprio nome sugere, possui uma arquitetura especial que lhe confere as características mencionadas anteriormente. Ele é projetado para armazenar informações de forma eficiente e segura entre duas partes. No blockchain, as informações são organizadas em uma lista crescente, onde cada elemento dessa lista é chamado de bloco. É essa estrutura de blocos conectados que dá ao blockchain seu nome, ”cadeia de blocos”.[10]

Além disso, é importante destacar que o blockchain é descentralizado, o que significa que não é controlado por uma única entidade ou autoridade central. Em vez disso, ele é mantido e verificado por uma rede de computadores distribuídos, chamados de nós, que trabalham em conjunto para validar e registrar as transações.[11]

Cada bloco do blockchain contém um conjunto de transações, que podem incluir informações como data, hora, valor e identificadores das partes envolvidas. Essas transações são verificadas e validadas pelos nós da rede, garantindo a integridade e a segurança do sistema.[8]

Além disso, o blockchain utiliza técnicas criptográficas avançadas para proteger as informações armazenadas. Cada bloco possui um código único, chamado de hash, que é gerado a partir dos dados do bloco e de seu bloco anterior(Figure 2.1). Isso cria uma ligação criptográfica entre os blocos, garantindo que qualquer alteração em um bloco anterior afetaria todos os blocos subsequentes, tornando a manipulação dos dados praticamente impossível.[12]

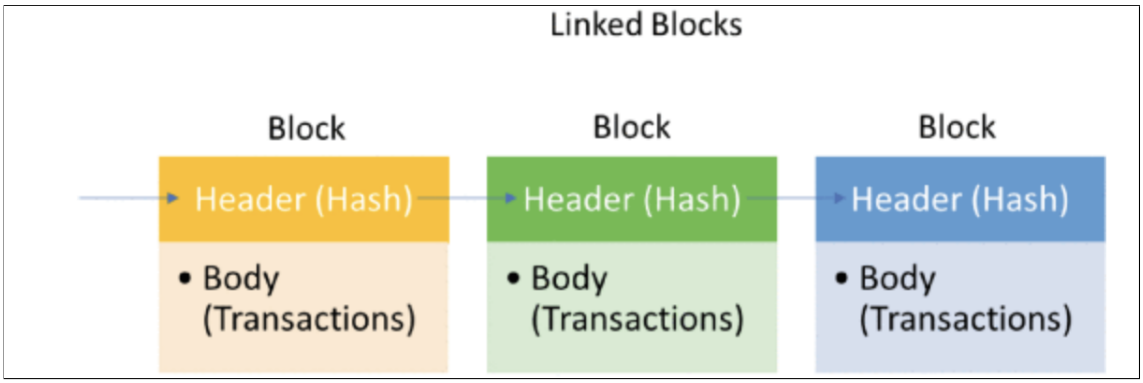

Figure 2.1: Blocks in the Blockchain architecture, [10], .

O blockchain, como mencionado anteriormente, é composto por blocos que estão interligados, permitindo o envio e recebimento de informações entre eles. Essa interconexão dos blocos forma uma rede caracterizada por nós. Existem duas categorias principais de nós: os nós completos e os nós leves. No entanto, é importante ressaltar que existem subnós que se diferenciam com base em suas funcionalidades específicas.

Os nós completos, também conhecidos como nós completos do blockchain, são responsáveis por manter uma cópia completa do registro de todas as transações ocorridas na rede blockchain. Esses nós possuem um alto nível de participação na rede e desempenham um papel crucial na validação e consenso das transações. Eles têm a capacidade de verificar todas as transações e armazenar uma cópia completa do blockchain, o que requer um grande poder de processamento e espaço de armazenamento.[10]

Por outro lado, os nós leves, também chamados de nós-cliente, têm uma funcionalidade mais limitada em comparação aos nós completos. Esses nós não armazenam uma cópia completa do blockchain, mas apenas informações relevantes para suas operações específicas. Eles dependem dos nós completos para acessar o blockchain e verificar as transações. Os nós leves são mais leves em termos de requisitos de recursos, tornando-os adequados para dispositivos com capacidade de processamento e armazenamento limitados, como smartphones e dispositivos de IoT (Internet das Coisas).

Dentro dessas categorias, existem subnós com funcionalidades especializadas, como os nós mineradores. Os nós mineradores são responsáveis por adicionar novos blocos à cadeia, utilizando poder computacional para resolver problemas matemáticos complexos, conhecidos como prova de trabalho (proof-of-work). Eles desempenham

um papel crucial na manutenção da segurança e integridade do blockchain, garantindo que apenas transações válidas sejam adicionadas aos blocos.

Essa estrutura de nós no blockchain permite a descentralização e a distribuição das informações, aumentando a segurança e a transparência do sistema. Cada nó na rede possui uma cópia do blockchain e participa da validação e consenso das transações.(Figure 2.2).

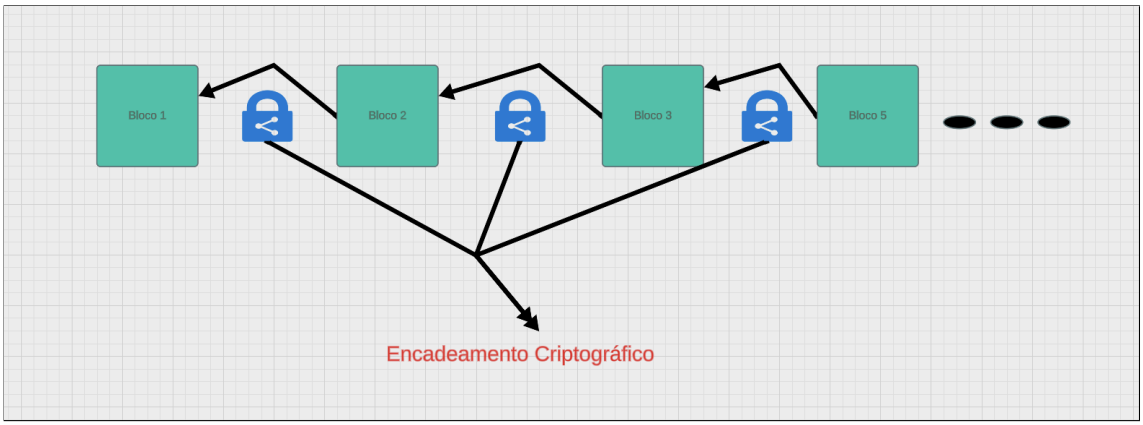

Figure 2.2: Estrutua do Blockchain.

3 DESAFIOS DE ESCALABILIDADE EM BLOCKCHAIN:IMPACTOS

3.1 ESCALABILIDADE

Nesta seção, será discutida a escalabilidade do Blockchain, um aspecto crucial para o sucesso e adoção em larga escala desta tecnologia inovadora. A escalabilidade refere-se à capacidade da tecnologia Blockchain de lidar com um aumento significativo no número de transações e usuários sem comprometer sua eficiência e desempenho.

Um dos principais desafios enfrentados em relação à escalabilidade do Blockchain é o tempo de processamento das transações. Cada nó da rede Blockchain precisa validar e registrar cada transação em todos os nós da rede, o que pode levar a atrasos à medida que o tamanho do Blockchain cresce. O mecanismo de consenso distribuído, como o algoritmo de prova de trabalho (Proof-of-Work), também pode exigir um tempo considerável para confirmar transações.

Além disso, o aumento do consumo de recursos computacionais é uma preocupação em termos de escalabilidade. Os nós da rede Blockchain, especialmente os nós completos que armazenam e validam todas as transações, requerem poder de processamento e capacidade de armazenamento significativos. À medida que o número de transações e a complexidade dos contratos inteligentes aumentam, a demanda por recursos computacionais também aumenta, o que pode levar a problemas de desempenho e custos adicionais.

No contexto do Bitcoin, é crucial mencionar que existe um limite predefinido para o tamanho de cada bloco que comporta as transações. Isso implica que cada bloco é capaz de acomodar apenas um número limitado de transações. A visão inicial de Satoshi Nakamoto, o criador do Bitcoin, explicou em seu trabalho seminal [8] que a rede é projetada para adicionar uma média específica de novos blocos a cada hora. Uma característica notável desse sistema é que, se a rede estiver processando mais blocos do que a média prevista, o desafio de Proof-of-Work se torna mais complexo. Esse ajuste dinâmico resulta no aumento da dificuldade do processo de mineração, o que, por sua vez, faz com que o número de blocos confirmados retorne à média desejada. Portanto, o ritmo de validação de blocos e, por extensão, o número de transações validadas, é limitado a cada hora.

É capital observar que, à medida que a rede Bitcoin continua a se expandir, a capacidade de processamento de transações também enfrenta limitações. Este fato levou a situações, como observado em 2017, em que as transações de Bitcoin sofreram atrasos significativos, levando horas para serem confirmadas. Durante esses períodos de alta demanda, as taxas de transferência associadas a essas transações também aumentaram consideravelmente [13].

3.2 CAPACIDADE DE PROCESSAMENTO DE TRANSACÕES EM GRANDE ESCALA

Nesta seção, será abordada a capacidade de processamento de transações, um dos principais limites da tecnologia blockchain. Embora o blockchain seja projetado para ser um sistema descentralizado e seguro, sua arquitetura distribuída pode resultar em restrições em termos de velocidade e capacidade de processamento.

Um dos fatores que afeta a capacidade de processamento é o tempo de confirmação das transações. Em blockchains que utilizam algoritmos de consenso como Prova de Trabalho (Proof-of-Work), cada transação precisa ser validada e confirmada pelos nós da rede, o que pode demandar algum tempo. Isso resulta em limitações na quantidade de transações que podem ser processadas em um determinado período [14]. Será apresentada também uma breve explicação do algoritmo de consenso Proof-of-Work (PoW), que, devido às suas características operacionais, pode tornar a rede do blockchain um pouco mais lenta.

Prova de trabalho (Proof-of-Work) O algoritmo de Prova de Trabalho (Proof-of-Work, PoW) é um dos mecanismos de consenso mais amplamente utilizados no contexto do Blockchain[15]. Foi introduzido originalmente por Nakamoto Satoshi no white paper do Bitcoin e tem sido adotado por várias outras criptomoedas e redes Blockchain [8].

O objetivo do algoritmo de Prova de Trabalho é garantir a segurança e a integridade da rede, tornando computacionalmente custoso para um participante mal-intencionado atacar a rede ou modificar o histórico de transações. Ele exige que os mineradores resolvam problemas matemáticos complexos, conhecidos como ”quebra-cabeças criptográficos” ou ”hash puzzles”, a fim de adicionar novos blocos ao Blockchain.[14]

Para resolver esses quebra-cabeças, os mineradores devem gastar uma quantidade significativa de poder computacional, que é medido em termos de poder de processamento (hashrate). O objetivo é encontrar um valor hash que atenda a certos critérios específicos, como ter um determinado número de zeros no início. Os mineradores tentam diferentes combinações até que um deles encontre a solução correta, e o bloco é adicionado ao Blockchain.

Uma vez que um minerador encontra a solução, ele a propaga para a rede, que então valida e aceita o novo bloco. O minerador que resolve o quebra-cabeça recebe uma recompensa em forma de criptomoeda, incentivando a participação no processo de mineração.

Embora o algoritmo de Prova de Trabalho seja eficaz em garantir a segurança do Blockchain, ele também tem algumas desvantagens significativas. Uma delas é o alto consumo de energia associado à mineração, especialmente em redes com um grande

número de mineradores competindo por recompensas. Isso levou a críticas em relação à sustentabilidade ambiental do Bitcoin e de outras criptomoedas baseadas em PoW.

Além disso, o algoritmo de Prova de Trabalho pode resultar em um tempo de confirmação relativamente longo para as transações, uma vez que os mineradores precisam competir para resolver os quebra-cabeças. Isso pode limitar a escalabilidade da rede, especialmente em momentos de alta demanda por transações.

3.3 IMPACTO NA EFICIÊNCIA DO BLOCKCHAIN EM GRANDES ESCALAS

Nesta seção, será abordada a interligação direta entre os desafios de escalabilidade enfrentados pelo blockchain e sua eficiência em larga escala. Analisaremos como esses desafios impactam a eficiência do blockchain, considerando possíveis atrasos nas transações, a capacidade reduzida de processamento e os efeitos na experiência do usuário [16].

Um dos principais impactos é o aumento dos atrasos nas transações. À medida que o número de transações aumenta e a validação descentralizada ocorre em cada nó da rede, o tempo necessário para confirmar uma transação pode se tornar significativo. O processo de validação e consenso exige que várias partes alcancem um acordo, o que pode levar tempo considerável, especialmente em redes congestionadas. Isso resulta em atrasos na confirmação das transações, afetando a eficiência do blockchain em lidar com um grande volume de transações em tempo hábil [16].

Além dos atrasos, a capacidade reduzida de processamento é um impacto direto dos desafios de escalabilidade. À medida que a rede blockchain cresce e o número de transações aumenta, os nós da rede enfrentam dificuldades em processar todas as transações de forma eficiente. Os recursos computacionais necessários para validar e registrar as transações em cada nó podem se tornar sobrecarregados, levando a um processamento lento e a uma capacidade limitada de processar um grande volume de transações simultaneamente. Isso afeta a eficiência do blockchain em lidar com uma demanda crescente de transações em grande escala.

Os efeitos na experiência do usuário também são significativos. Atrasos nas transações e capacidade limitada de processamento podem resultar em uma experiência frustrante para os usuários do blockchain. Se as transações demorarem muito para serem confirmadas ou se houver atrasos na execução de contratos inteligentes, os usuários podem enfrentar inconveniências e perda de confiança na tecnologia. Além disso, a capacidade reduzida de processamento pode limitar a capacidade de uso do blockchain em aplicativos de alta demanda, como sistemas de pagamento ou cadeias de suprimentos globais. Isso pode prejudicar a adoção em larga escala do blockchain e restringir seu potencial de transformação em vários setores.

3.4 IMPACTO EM SETORES ESPECÍFICOS

Os desafios relacionados à escalabilidade e capacidade de processamento do blockchain podem limitar seu impacto e adoção em larga escala em alguns desses setores.

3.4.1 Serviços financeiros

No setor financeiro, a escalabilidade do blockchain é essencial para lidar com o grande volume de transações diárias. As transações financeiras exigem tempos de processamento rápidos e capacidade para lidar com uma demanda crescente. Se o blockchain não puder acompanhar essa demanda, pode ocorrer atrasos nas transações, o que compromete a eficiência e a experiência do usuário. Além disso, o tamanho crescente do blockchain e os requisitos de armazenamento de dados podem dificultar a integração com sistemas financeiros existentes.

3.4.2 Cadeias de suprimentos

No setor de cadeia de suprimentos, a escalabilidade do blockchain é crucial para lidar com a rastreabilidade de produtos em tempo real. À medida que os produtos passam por várias etapas da cadeia de suprimentos, é necessário registrar e verificar suas informações de forma eficiente e rápida. A capacidade limitada de processamento do blockchain pode levar a atrasos na atualização e verificação dessas

3.4.3 Setor de saúde

No setor de saúde, a escalabilidade do blockchain é fundamental para lidar com o compartilhamento seguro de informações médicas. O blockchain pode melhorar a interoperabilidade entre diferentes sistemas de saúde e permitir o acesso rápido e seguro aos registros médicos dos pacientes. No entanto, a capacidade limitada de processamento do blockchain pode levar a atrasos na recuperação e atualização dessas informações, afetando a qualidade dos cuidados de saúde.

3.5 ANÁLISE EXPERIMENTAL DE ESCALABILIDADE EM TRÊS SISTEMAS DE BLOCKCHAIN

Analisando a Figura 3.1 que ilustra três sistemas: Ethereum, Parity e Hyperledger, com uma taxa de solicitação do cliente variando entre 8 tx/s e 1024 tx/s e como eles lidam com cargas de trabalho maiores do YCSB (Yahoo Cloud Serving Benchmark). O desempenho do Parity mantém-se constante à medida que o tamanho da rede e a carga oferecida aumentam, devido à taxa constante de processamento de transações nos servidores. Na análise, observa-se que a taxa de transferência e a latência do

Ethereum degradam quase linearmente após 8 servidores, enquanto o Hyperledger para de funcionar além de 16 servidores.

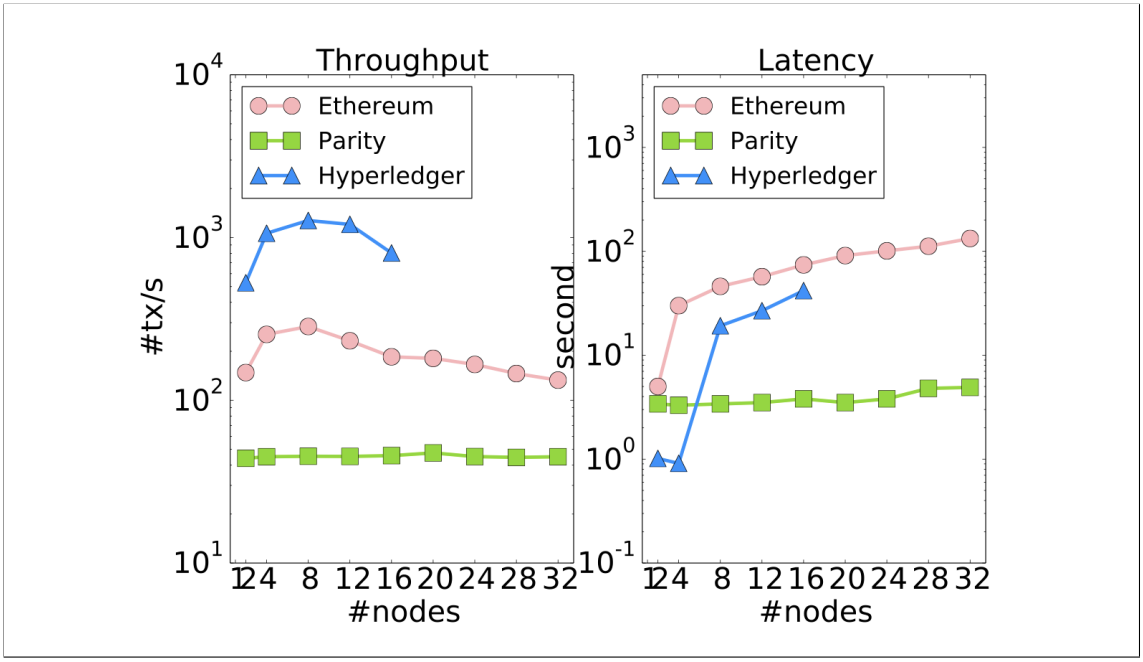

Figure 3.1: Performance scalability (with the same number of clients and servers). [17], .

Agora, procederemos à análise do motivo pelo qual o sistema Hyperledger não conseguiu escalar além de 16 servidores e 16 clientes. Ao examinar o registro do sistema Hyperledger, identificou-se que os nós estavam tentando chegar a um consenso em relação a novas visões que continham lotes de transações, porém estavam falhando continuamente nesse processo. O que ocorreu foi que os servidores estavam em visões divergentes, resultando no recebimento de mensagens conflitantes de mudança de visão provenientes do restante da rede. Em essência, esses conflitos surgiram devido à rejeição das mensagens de consenso por parte de outros pares, em virtude do congestionamento do canal de mensagens. À medida que as mensagens eram descartadas, as visões divergiam progressivamente, culminando em um impasse no consenso.

Adicionalmente, observou-se que, ao longo do tempo, as solicitações dos clientes passaram a demandar mais tempo para serem concluídas, o que evidencia que os servidores estavam sobrecarregados no processamento das mensagens da rede. Contudo, é importante salientar que o protocolo original de PBFT garante tanto a vitalidade quanto a segurança. Portanto, a incapacidade do Hyperledger de escalar além de 16 servidores pode ser atribuída à implementação específica do protocolo.

Até o momento, os resultados obtidos indicam que a tentativa de escalonar tanto o número de clientes quanto o número de servidores resulta na degradação do desempenho, levando inclusive à falha do sistema Hyperledger nesse contexto.

A figura 3.2 ilustra uma observação relevante sobre o desempenho dos sistemas em análise. Conforme o número de servidores é incrementado, nota-se uma

degradação no desempenho, indicando que os sistemas enfrentam sobrecargas na rede. Essa observação é particularmente pertinente devido à natureza dos sistemas em análise.

O Hyperledger, por sua característica de limitação da comunicação, apresenta um comportamento no qual o aumento do número de servidores resulta em uma intensificação da troca de mensagens e consequentemente uma maior sobrecarga. Por outro lado, o Ethereum, embora limitado pela capacidade de processamento, ainda demanda uma quantidade modesta de recursos de rede para a disseminação de transações e blocos para outros nós. Vale ressaltar que, em redes mais extensas, a dificuldade da rede é aumentada para acomodar os atrasos na propagação.

Uma constatação importante é que, para evitar divergências na rede, o nível de dificuldade é ajustado a uma taxa superior ao crescimento no número de nós. Portanto, uma das causas da degradação na taxa de transferência do Ethereum reside no tamanho da rede. Além disso, na configuração adotada, onde 8 clientes enviam solicitações exclusivamente para 8 servidores, nota-se que esses servidores nem sempre compartilham as transações entre si, mantendo a mineração de maneira independente em suas respectivas pools de transações. Isso resulta em uma subutilização da capacidade de mineração da rede.

Esse fenômeno revela a complexidade subjacente ao desempenho de sistemas de blockchain em ambientes com diferentes tamanhos de rede, bem como destaca a necessidade de abordagens específicas para otimizar a eficiência das operações em tais contextos. Essa análise oferece uma compreensão mais aprofundada dos desafios associados à escalabilidade e otimização de sistemas de blockchain em ambientes dinâmicos e diversificados.

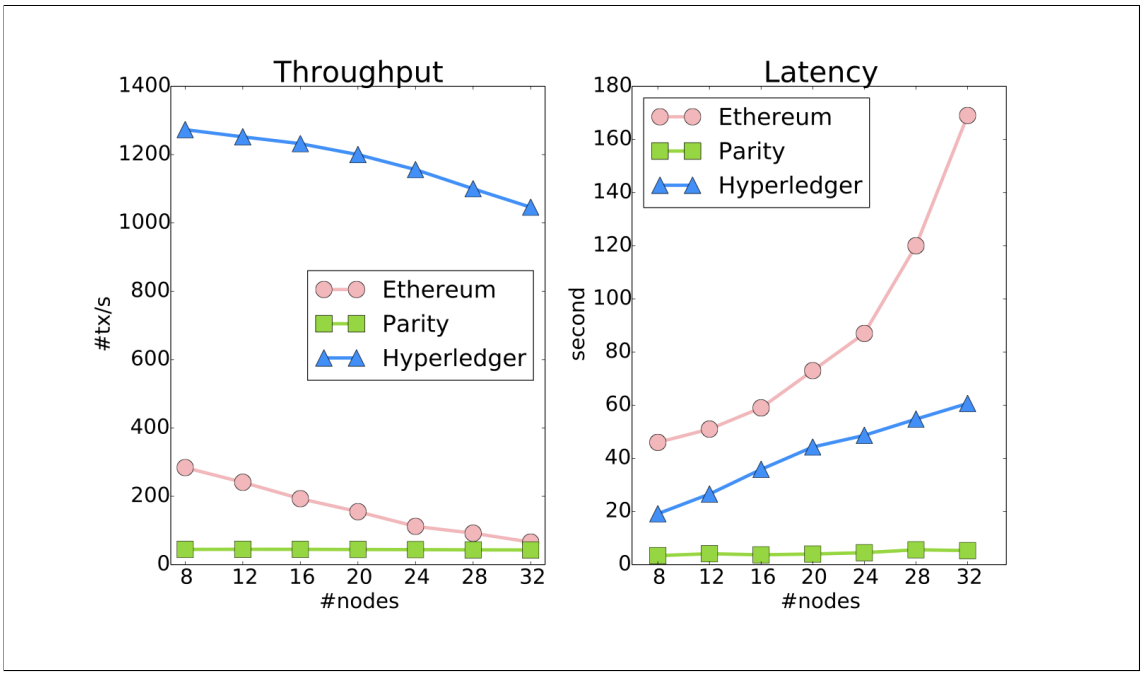

Figure 3.2: Performance scalability (with 8 clients)). [17], .

4 ANÁLISE DE DESEMPENHO DO BLOCKCHAIN

O Blockchain é amplamente reconhecido hoje como uma tecnologia disruptiva com o potencial de transformar diversos setores. Sua capacidade de oferecer um registro distribuído seguro e imutável abriu caminho para inovações em finanças, cadeia de suprimentos, saúde e muitos outros campos. À medida que diversas plataformas e projetos adotam essa tecnologia, torna-se imperativo avaliar seu desempenho em diversos contextos. Neste contexto, iremos explorar as diferentes dimensões do desempenho do blockchain, com ênfase especial em uma métrica-chave e uma análise aprofundada

4.1 MÉTRICA DO DESEMPENHO

A medida do desempenho do Blockchain e a metrica para a velocidade das transações são conceitos que evoluíram ao longo do tempo à medida que a technologia blockchain se desenvolveu. Uma das metricas mais frequentemente consideradas é a ”velocidade de transações” ou ”transaçoes por segundos(TPS)”, que mede quantas transões a rede blockchain pode processar em um determinado periodo.

4.1.1 Mediçaõ do desempenho do Blockchain

A medição do desempenho do Blockchain começou a ganhar destaque logo após o lançamento do Bitcoin em 2009. Como foi especificado no meu desenvolvimento , o Bitcoin do Satochi foi a primeira implementação pratica da tecnologia blockchain, e a medida que a rede crescia, surgiram preocupações sobre sua capacidade de lidar com um grande número de transações .Isso que levou a discussões sobre a escalabilidade e eficiência da rede , inaugurando uma era de medição de desempenho mais sistemática. Uma lista representativa de pesquisas existentes, mostrada na tabela abaixo , identificando a necessidade pesquisas sistematica sobre a avaliação do desempenho do blockchain.

Year	Survey	Research Scope
2018	Kim et al.[18]	Escalability Solution
2019	Rouhani and Deters[19]	security, performance, and applications of smart contract
2019	Zheng et al.[20]	challenges of performance and security
2019	Wang et al. [21]	benchmarking tools and performance optimization methods
2020	Zhou et al. [22]	scaling solutions to blockchain
2020	Yu et al. [23]	sharding for blockchain scalability

Table 4.1: Escopo de pesquisas relacionados aos desempenhos existentes.

4.1.2 Metricas para velocidade das transaçoes

A métrica para a velocidade das transações, conhecida como ”transações por segundo” (TPS), tornou-se relevante à medida que o Bitcoin e outras criptomoedas ganhavam popularidade. A TPS é uma métrica simples que representa o número de transações que uma rede blockchain pode processar em um segundo. Ela se tornou importante devido às diversas razões tais como:

- Concorencia com Sistemas Financeiros Tradicionais : À medida que as criptomoedas começaram a competir com sistemas financeiros tradicionais, a capacidade de processar transações rapidamente se tornou um ponto crítico de avaliação. Os sistemas de pagamento tradicionais, como cartões de crédito, processam milhares de transações por segundo, e o blockchain precisava demonstrar sua capacidade de competir nesse aspecto.
- Congestionamento da Rede : Com o aumento do uso, o Bitcoin enfrentou congestionamentos na rede que levaram a atrasos nas transações e ao aumento das taxas de transação. A métrica TPS se tornou uma maneira clara de avaliar a capacidade da rede de lidar com a demanda.
- Melhorias da tednologia : A busca por aumentar a TPS levou ao desenvolvimento de novas tecnologias e algoritmos de consenso, como o Segregated Wit-

ness (SegWit) no Bitcoin e o Ethereum 2.0. Essas melhorias foram impulsionadas pela necessidade de aumentar o desempenho.

Portanto, a métrica TPS surgiu organicamente da necessidade de avaliar a capacidade do blockchain de processar transações de forma eficiente e competir com sistemas financeiros existentes. Desde então, ela se tornou uma métrica padrão para medir o desempenho de redes blockchain e continua a evoluir à medida que novas soluções são desenvolvidas para melhorar a escalabilidade e a eficiência das redes blockchain.

4.2 ANÁLISE DE DESEMPENHO BLOCKCHAIN BASEADA EM EVIDENCIAS

A ”Analíse de desempenho Blockchain Baseada em Evidências ” representa uma abordagem essential na avaliação critica da tecnologia blockchain .À medida que os bockchains continuam a se difundir em diversos setores , a necessidade de uma avaliação fundamentada em dados torna-se cada vez mais premente. Esta analise empírica não apenas permite a comprensão aprofundada do funcionamento de sistema blockchain, mas também ajuda a tomar decisões informadas sobre a sua implementação.Neste texto, exploraremos a importância e os métodos dessa análise baseada em evidências, destacando como ela pode moldar o futuro dessas tecnologias disruptivas. As abordagens de avaliação revistas podem ser categorizadas em dois grupos principais: avaliação empírica e modelagem analítica, conforme demonstrado na figura 4.1.

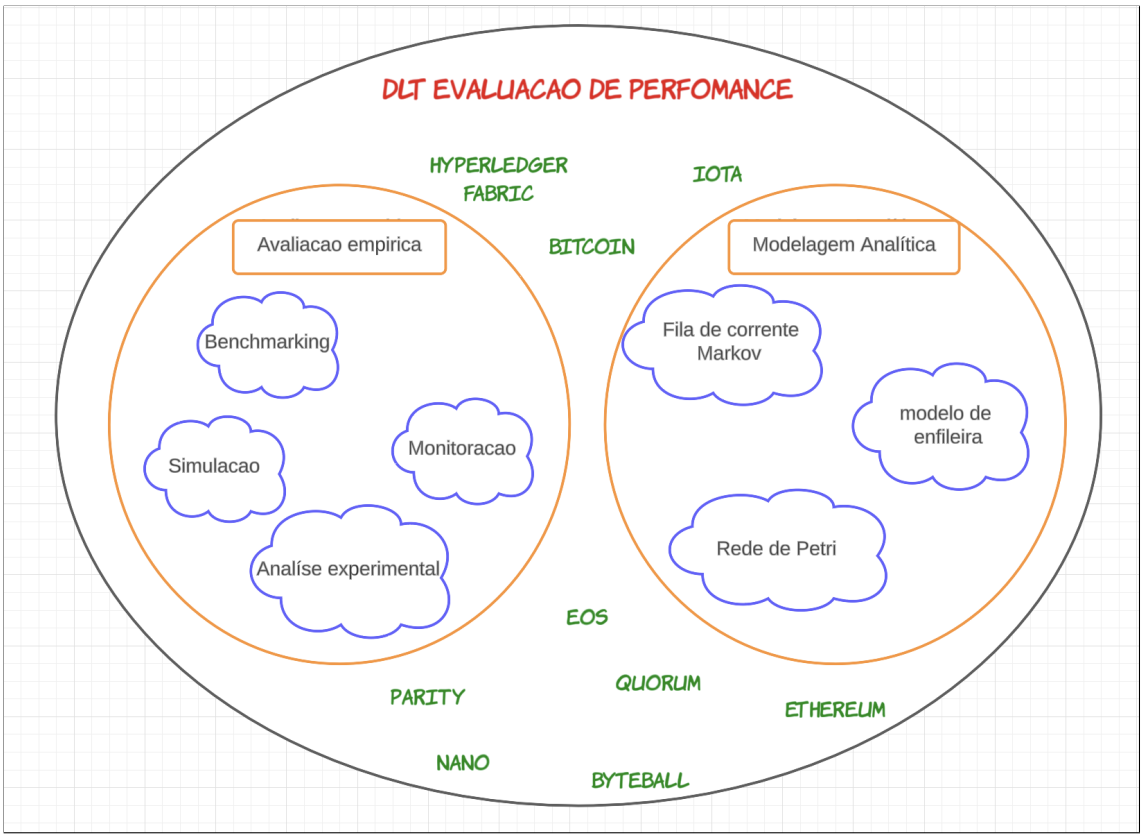

Figure 4.1: Cenário de abordagens de avaliação de desempenho DLT e livros-razão avaliados. [24], .

4.2.1 Instrumentos de Benchmarking Blockchain

O Benchmarking é uma prática essencial na avaliação do desempenho do blockchain. Essas ferramentas são projetadas para medir e comparar o desempenho de diferentes sistemas blockchain em relação a métricas específicas. O benchmarking de desempenho tem sido extensivamente pesquisado e documentado em relação a sistemas de nuvem, como Hadoop, MapReduce e Spark, bem como em sistemas de banco de dados, abrangendo sistemas relacionais e NoSQL.[24] O surgimento constante de sistemas blockchain, que buscam aprimorar o desempenho do Ledger Distribuído (DTL), torna-se imperativo desenvolver uma solução capaz de comparar as diversas plataformas de maneira significativa.

Até junho de 2020 exitem três Benchmarks Populares de Blockchain dedicados à avaliação de sistemas de blockchain, conforme listado na Tabela 4.2.

Frameworks	Supported DLTs	Workloads Used	Evaluated Metrics	Pros & Cons
Blockbench [49]	Ethereum, Hyperledger Fabric (HLF), Parity and Quorum.	• macro: YCSB(k-v store), Smallbank(OLTP), EtherId, Doubler, and WavesPresale • micro: DoNothing, Analytics, IOHeavy, and CPUHeavy	throughput, latency, scalability and fault-tolerance.	adaptor-based framework, scalable; carefully designed workloads; but they are constant.
DAGbench [56]	IOTA, Nano and Byteball	• value/data transfer • transaction query: 1) input/output transaction numbers and 2) balance for a given account	throughput, latency, scalability, success indicator, resource consumption, transaction data size and transaction fee	adaptor-based framework, scalable; specific for DAG DLT; workloads are not representatives.
Hyperledger Caliper [57]	Hyperledger blockchains (Fabric, Sawtooth, Iroha, Burrow and Besu), Ethereum, FISCO BCOS	Self-defined in the configuration file	throughput, latency, resource consumption, success rate	adaptor-based framework, scalable; no pre-defined workload design, but support more DLT systems.

Figure 4.2: Comparação de Três Benchmarks PoPulares de Blockchain, [24], .

O BlockBench é uma ferramenta de de benchmarking amplamente utilizada para avaliar o desempenho de sistemas blockchain . Ela oferece um ambiente de simulação que permite aos pesquisadores e desenvolvedores testar e comparar o desempenho de diferentes blockchains sob várias condições controladas. Atualemente ele suporta medição de em quatro grandes plataformas privadas de blockchains , a saber , Etherium , Parity,HLF e Quorum. No design do BlockBench, formam identificadas quatro camadas de abstração que desempenham papéis essenciais no funcionamento de sistemas blockchain. Essas camadas são organizadas em uma hieraquia que vai desde o nível mais baixo até o nivel maos alto. Figure 4.3

- **Camada de Consenso:** A camada mais fundamental é a de consenso. Aqui, as regras de acordo são estabelecidas e implementadas para garantir que todos os participantes da rede cheguem a um consenso sobre o conteúdo que será adicionado a um bloco e, subsequentemente, ao blockchain. É nessa camada

que são definidos os algoritmos de consenso que garantem a integridade e a validade das transações.

- **Camada de Modelo de Dados:** A camada de modelo de dados é responsável por definir a estrutura, o conteúdo e as operações que podem ser realizadas nos dados armazenados no blockchain. Essa camada desempenha um papel crucial na definição das informações que podem ser registradas no blockchain e na forma como esses dados são organizados.

- **Camada de Mecanismo de Execução:** A terceira camada, o mecanismo de execução, abrange o ambiente de tempo de execução, onde ocorre a execução de códigos e contratos inteligentes. Nela, estão presentes recursos essenciais, como a Máquina Virtual Ethereum (EVM) e tecnologias como Docker, que oferecem suporte às operações de execução nos blockchains. Essa camada permite que os contratos inteligentes sejam executados e que as ações programadas sejam processadas com eficiência.

- **Camada de Aplicativos:** Por fim, a camada de aplicativos é o nível mais alto da hierarquia. Nessa camada, encontram-se diversos tipos de aplicativos blockchain, incluindo contratos inteligentes e Decentralized Applications (DApps). Aqui é onde a funcionalidade real é entregue aos usuários e aplicativos, abrangendo uma ampla gama de casos de uso, desde finanças descentralizadas até cadeias de suprimentos transparentes.

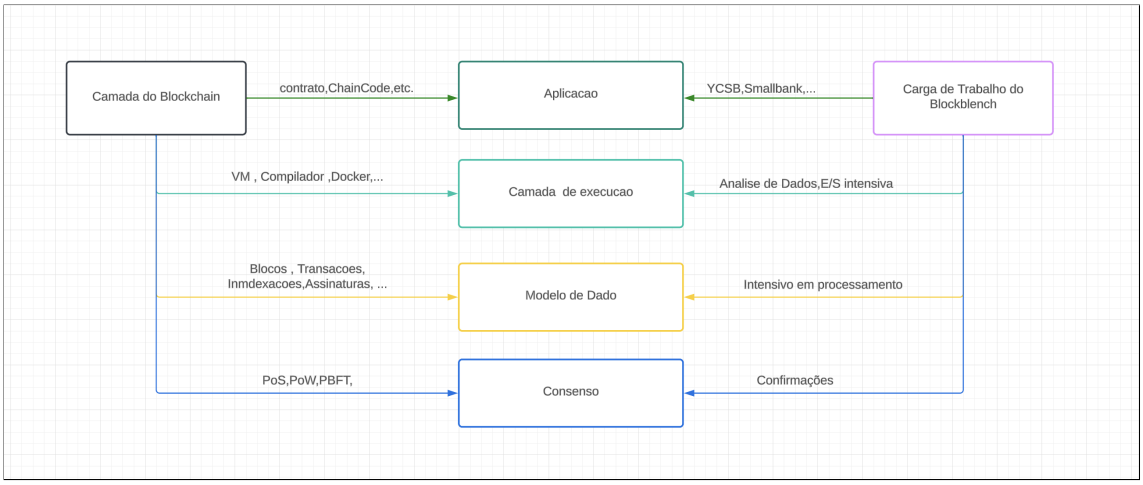

Figure 4.3: Abstraction layers in blockchain, and the corresponding workloads in BLOCKBENCH. [17], .

4.2.2 Supervisionamento do desempenho do Blockchain

A prática de benchmarking em blockchains geralmente demanda um ambiente padronizado e uma carga de trabalho bem documentada como entradas. No entanto,

quando se trata de sistemas públicos de blockchain, enfrentamos desafios adicionais devido à impossibilidade de controlar totalmente a carga de trabalho real e os participantes do consenso. Isso torna o benchmarking uma tarefa mais complexa. No contexto da avaliação de blockchains públicos, duas abordagens têm se destacado.

A primeira abordagem envolve a criação de uma versão privada da rede de teste correspondente e o subsequente uso de benchmarks já existentes, conforme mencionados anteriormente, para avaliar o desempenho do blockchain sob cargas de trabalho artificialmente projetadas. Essa estratégia pode requerer o desenvolvimento de um novo adaptador para cargas de trabalho ou a configuração de uma rede blockchain privada específica. No entanto, é importante notar que essa abordagem deve lidar com o desafio da escalabilidade do blockchain. A versão privada testada do blockchain pode não refletir completamente os problemas de escalabilidade que podem surgir quando a implementação acontece em um ambiente público. Portanto, os resultados obtidos nesse ambiente controlado podem apresentar valores de métricas de desempenho mais otimistas em comparação com a rede pública real.

A segunda abordagem consiste em monitorar e avaliar o desempenho do sistema público em tempo real, sob cargas de trabalho realistas.Zheng et al. [22] propuseram uma estrutura abrangente de monitoramento de desempenho em tempo real que utiliza uma abordagem baseada em registros. Essa abordagem apresenta vantagens, como menor sobrecarga, detalhes mais abrangentes e melhor escalabilidade, em comparação com a solução que faz uso de chamadas de procedimento remoto (RPC) como contraparte. Isso permite uma avaliação mais precisa do desempenho do sistema em um ambiente de produção, onde a carga de trabalho reflete situações reais de uso.[24]

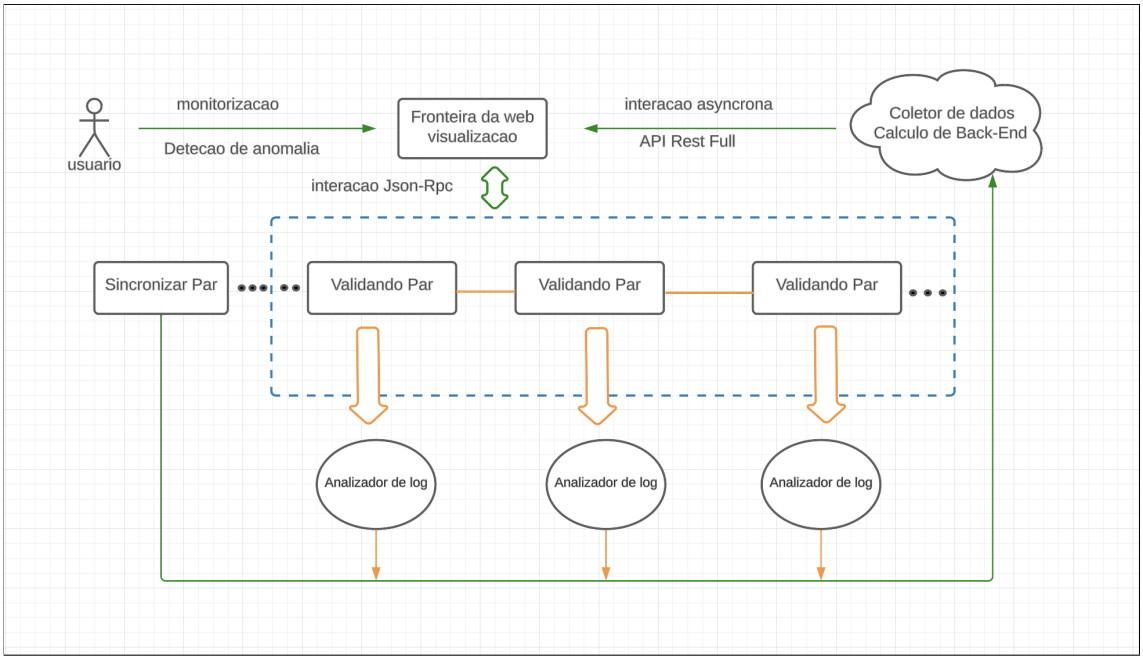

Figure 4.4: Estrutura de monitoramento de desempenho blockchain. [24], .

4.2.3 Analise experimental de sistema Blockchain

Nesta seção, conduzimos uma análise experimental focada nos sistemas Ethereum, Parity e Hyperledger, com um foco especial na avaliação de seu desempenho. A escolha dessas plataformas foi motivada por sua posição proeminente no domínio do blockchain e pela complexidade e maturidade de seus códigos-base.[25]

4.2.3.1 Etherium

Como uma das principais plataformas de contrato inteligente e criptomoedas, Ethereum é amplamente adotado em uma variedade de casos de uso. A análise de desempenho abrangeu áreas como transações por segundo (TPS), latência, consumo de recursos e escalabilidade. Investiguei como o Ethereum lida com cargas de trabalho crescentes e quais são os principais fatores que afetam seu desempenho.

4.2.3.2 Parity

Parity é conhecido por sua eficiência e segurança. Uma breve análise detalhada de seu desempenho, avaliando sua capacidade de processar transações em alta velocidade e como ele se comporta em ambientes de alto volume. Além disso, seu uso em cenários de consórcio e o impacto disso no desempenho.

4.2.3.3 Hyperledger

Hyperledger é uma plataforma de blockchain empresarial com diversas implementações, incluindo o Hyperledger Fabric e o Hyperledger Sawtooth. A análise se concentrou na comparação de desempenho entre essas implementações, levando em consideração métricas como latência, escalabilidade e eficiência.

4.2.3.4 Análise comparativa

Para desenvolver um aplicativo habilitado para Blockchain, os desenvolvedores devem avaliar a adequação da implementação do blockchain. É necessário realizar uma análise comparativa de desempenho para selecionar a plataforma de blockchain que ofereça um desempenho adequado para alcançar os objetivos do aplicativo a ser desenvolvido .

Após a criação do Blockbench, Dinh et al.[17] empregaram essa ferramenta para conduzir uma análise comparativa de desempenho em três blockchains privados tradicionais: Ethereum (geth v1.4.18), Parity (v1.6.0) e Hyperledger Fabric (HLF v0.6.0-preview). Suas descobertas, baseadas em extensa pesquisa,

- ⋆ Desempenho Superior do HLF : Notou-se que o Hyperledger Fabric apresenta um desempenho consistentemente superior em relação ao Ethereum e ao Parity

em todos os benchmarks, sejam eles de macroescala, como taxa de transferência e latência, ou microescala, como IOHeavy. Isso destaca a robustez do HLF em vários cenários de uso. No entanto, é importante observar que o HLF enfrenta um desafio em termos de escalabilidade, já que não consegue operar eficientemente com mais de 16 nós na rede.

- ⋆ Identificação dos Gargalos: Os autores identificaram que os protocolos de consenso são os principais gargalos para o Hyperledger Fabric e o Ethereum, afetando seu desempenho. Enquanto isso, a assinatura de transações representa um gargalo para o Parity, limitando sua capacidade de processamento.

  Os autores aprofundaram a análise, comparando o desempenho de duas versões distintas do HLF, a v0.6.0 e a v1.0.0, com foco na carga de trabalho IOHeavy. Essa análise adicional proporciona insights valiosos sobre a evolução do desempenho do Hyperledger Fabric ao longo das versões, contribuindo para uma compreensão mais abrangente das capacidades dessas plataformas.[26]

A avaliação de diferentes blockchains continua sendo um desafio devido à ausência de padrões de interface. Como resposta a essa questão, um avanço foi alcançado na forma de uma carga de trabalho genérica que executa as mesmas operações em várias interfaces blockchain. Esse esforço foi notável e pode ser observado em [27], onde essa carga de trabalho foi concebida. Ela se mostrou essencial para a avaliação comparativa de três proeminentes plataformas de blockchain consórcio para o contexto da Internet das Coisas (IoT). As plataformas em foco incluíram o HLF v0.6 com o consenso Practical Byzantine Fault Tolerance (PBFT), o HLF v1.0 com o consenso de replicação de máquina de estado tolerante a falhas bizantinas (BFT-SMaRt) e o Ripple, que utiliza o consenso Ripple. Os resultados dessa avaliação revelaram que os blockchains analisados conseguiram proporcionar uma taxa de transferência razoável. No entanto, destacou-se uma limitação significativa em termos de escalabilidade. Essas descobertas têm implicações cruciais, especialmente em aplicações voltadas para a Internet das Coisas, onde a escalabilidade desempenha um papel vital. Esse cenário sublinha a importância contínua de pesquisas e desenvolvimentos em busca de soluções que atendam às crescentes demandas de escalabilidade e eficiência, particularmente em cenários complexos como o da IoT, onde a necessidade de processar grandes volumes de transações de forma confiável é primordial.

Pongnumkul et al. [28] conduziram uma análise preliminar de desempenho envolvendo duas das plataformas blockchain privadas mais populares: o Hyperledger Fabric (HLF v0.6) e o Ethereum (geth 1.5.8 em implantação privada). Esse estudo avaliou o desempenho sob várias cargas de trabalho, utilizando métricas como tempo de execução, latência e taxa de transferência. Os resultados experimentais demonstraram

que o Hyperledger Fabric supera o Ethereum em todas as métricas avaliadas, o que é um indicativo do robusto desempenho do HLF em cenários diversificados.

No entanto, é importante observar que ambos os sistemas ainda não atingem níveis de desempenho competitivos em comparação com os sistemas de banco de dados tradicionais, especialmente quando submetidos a cargas de trabalho mais elevadas. Essa constatação é reforçada por um estudo mais recente [25], no qual o Ethereum foi comparado com o sistema de gerenciamento de banco de dados MySQL. Os resultados desse estudo corroboraram a conclusão anterior, enfatizando que, embora os blockchains ofereçam vantagens em segurança e descentralização, o desempenho puro ainda precisa ser aprimorado para competir eficazmente com sistemas de banco de dados convencionais.

A análise comparativa também se estende aos algoritmos de consenso empregados por diferentes blockchains. Por exemplo, Hao et al. [29] conduziram uma avaliação comparativa de desempenho entre o Hyperledger (utilizando o algoritmo Practical Byzantine Fault Tolerance - PBFT) e o Ethereum privado (baseado em Proof of Work - PoW). Eles desenvolveram uma estrutura de benchmark abrangente, composta por quatro módulos: um módulo de configuração de carga de trabalho, um módulo de contrato inteligente de consenso, um módulo de coleta de dados e as próprias plataformas blockchain. Os resultados dessa avaliação revelaram que o Hyperledger Fabric supera consistentemente o Ethereum em termos de taxa de transferência média (TPS) e latência. Este estudo destacou a influência significativa do mecanismo de consenso no desempenho de blockchains privados.

Outro exemplo notável é a análise de desempenho realizada em dois algoritmos de consenso: o Proof of Work (PoW) e a Conjectura Proof-of-Collatz (PCC)[30]. O PCC [31] é um algoritmo PoW teórico recentemente introduzido, baseado nas órbitas de Collatz, uma métrica definida no algoritmo da Conjectura de Collatz. Os autores conduziram uma avaliação minuciosa desses algoritmos de consenso, considerando o tempo de execução, o tempo de implantação e a latência em uma rede blockchain privada. Os resultados desses experimentos revelaram que o blockchain baseado na Conjectura Proof-of-Collatz supera consistentemente o blockchain baseado em PoW em todas as métricas avaliadas. Surpreendentemente, alcançou uma velocidade de execução até 1000 vezes mais rápida que o PoW. Esses resultados destacam a importância de inovações em algoritmos de consenso e seu potencial para aprimorar significativamente o desempenho de blockchains.

5 ANALISE EXPERIMENTAL DO DESEMPENHO DO BLOCKCHAIN COM CONTAINERS DOCKER

* **Estudos de caso**

Nesta seção, foi abordado um estudo de caso com o propósito de simular uma rede blockchain por meio da utilização de containers Docker. O principal objetivo dessa simulação foi explorar as potencialidades e desafios associados à implementação de uma infraestrutura baseada em blockchain em um ambiente de contêineres virtualizados. Ao longo do estudo, foram conduzidas diversas atividades para alcançar uma compreensão aprofundada do funcionamento da rede simulada. Inicialmente, foram configurados e interligados os containers Docker, replicando assim a estrutura distribuída de uma rede blockchain. Esta fase envolveu a criação de nós, a definição de suas interações e a configuração de parâmetros específicos.

Optei por concentrar a pesquisa no registro de diplomas digitais, apesar das diversas aplicações potenciais para a simulação de Blockchain. Essa decisão estratégica foi motivada pela complexidade e relevância específicas desse cenário, destacando-se, em parte, devido às limitações observadas ao tentar utilizar outros simuladores. Muitas vezes, essas plataformas carecem dos recursos tecnológicos necessários para realizar testes abrangentes e coletar resultados de maneira eficaz.

Morais (2019) sugere que instituições de ensino possuam a capacidade de emitir diplomas e certificados em formato digital, com a proposta de registrar esses documentos em uma Blockchain para garantir sua autenticidade. Esse conceito envolve a geração de um identificador único para cada documento, que, uma vez registrado na Blockchain, estabelece uma referência permanente. Isso viabiliza a verificação da existência do documento original sempre que necessário.

Ao selecionar o registro de diplomas digitais como foco da pesquisa, não apenas busco explorar a eficácia do Blockchain nesse contexto específico, mas também superar as limitações encontradas em outros simuladores.A simulação, desenvolvida em Node.js, cria o bloco gênesis da cadeia e estabelece os nós da Blockchain em containers por meio do Docker. Cada container é equipado com uma imagem Linux que armazena uma réplica dos registros da cadeia de blocos. Após a inicialização, os nós passam a monitorar a validade dos novos blocos adicionados, decidindo se podem ser integrados à rede.[32] Inicialmente, optei por simular uma rede com 10 nós, representando um ambiente de pequena escala. Posteriormente, esse número foi aumentado para 20, com o objetivo de observar o comportamento da rede com o dobro de nós. Ao ser executada, a aplicação gera exclusivamente o bloco gênesis, marcando o início da cadeia, e o distribui para

todos os nós. A partir desse ponto, os nós monitoram a validade dos novos blocos adicionados, decidindo se eles podem ser integrados à cadeia.

Os testes foram realizados em um sistema operacional Linux Mint 19.1 de 64 bits. A Figura 5.1 exibe uma representação visual da rede Blockchain gerada pela aplicação, destacando o bloco gênesis da cadeia, o timestamp que indica o momento de sua geração, e o hash de identificação correspondente.

Figure 5.1: Representação grafica do primeiro bloco .

* **Definição de indicadores de desempenho para análise sistemática**

Os parâmetros selecionados para análise compreenderam a vazão (throughput), representando a taxa na qual as requisições são atendidas pelo sistema, e o tempo de resposta, que consiste no intervalo decorrido entre o início e a conclusão de um serviço.

* **Aplicação de cargas de trabalho**

Para extrair as métricas de vazão e tempo de resposta, conduzimos 30 experimentos. Este número significativo de iterações confere ao experimento uma elevada confiabilidade, aproximando os resultados de uma dinâmica realista. O desvio padrão dos dados experimentais foi de 1,18. Foi aplicado diversas cargas de trabalho, simbolizando distintas quantidades de usuários realizando acessos simultâneos à aplicação. As cargas variaram de 1, 5, 10, 50, 100, 500 e 1000 acessos simultâneos. Inicialmente, foi incluido 10 nós na Blockchain e aplicamos várias cargas de trabalho para simular acessos simultâneos à rede. Os testes foram conduzidos em um sistema equipado com um processador Intel Core i5-10210U de 1,60 GHz e 8 GB de memória RAM. A ferramenta JMeter possibilita a definição da quantidade de acessos simultâneos. Neste experimento, cada acesso realiza o envio de dados no formato JSON para a aplicação, utilizando o método POST. Esse processo, em um contexto real, simboliza o registro de um diploma digital na cadeia de blocos.

* **Simulação de Cargas de Trabalho**

A ferramenta JMeter oferece a capacidade de configurar a quantidade de acessos simultâneos. Neste experimento, cada acesso realiza o envio de dados no formato JSON para a aplicação, utilizando o método POST. Esse procedimento, em um cenário real, representa a inclusão de um diploma digital na cadeia de blocos.

* **Resultados**

Primeiramente, foi realizada uma análise da vazão. O gráfico da Figura 5.2 ilustra que, à medida que o número de acessos simultâneos aumenta, o valor da vazão tende a se estabilizar. Esse fenômeno ocorreu por volta de 23 requisições por milissegundo, indicando o limite da capacidade de vazão da aplicação.

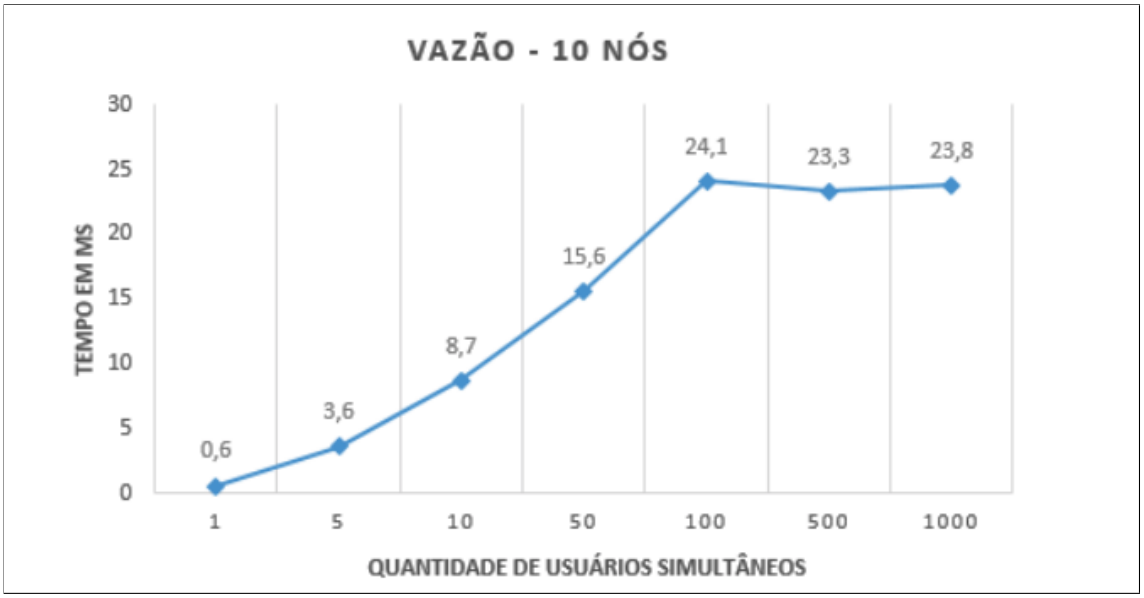

Figure 5.2: Vazão da Blockchain com 10 nós para diferentes cargas de trabalho.

Na segunda métrica, levamos em consideração o tempo de resposta. O gráfico apresentado na Figura 5.3 ilustra os resultados obtidos durante o teste com 10 nós. Observa-se no gráfico que, à medida que o número de usuários simultâneos aumenta, o tempo de resposta da aplicação também cresce. Para 1000 acessos simultâneos, o tempo total de resposta atingiu 12845 milissegundos.

Figure 5.3: Tempo de resposta com 10 nós para diferentes cargas de trabalho.

Em seguida , foi realizado uma simulação da Blockchain com 20 nós para avaliar seu comportamento ao dobrar a quantidade de máquinas conectadas. Uma rede com mais nós oferece maior segurança, tornando mais difícil para um atacante malicioso comprometer a rede, exigindo a alteração de mais de 51

Focamos na análise do desempenho da Blockchain, considerando vazão e tempo de resposta com o aumento da quantidade de nós conectados. Os resultados indicam que, ao aplicarmos as mesmas cargas de trabalho, a vazão se estabiliza em torno de 23 requisições por milissegundo (Figura 5.4).

Figure 5.4: Vazão da Blockchain com 20 nós para diferentes cargas de trabalho.

Também foi avaliado o tempo de resposta da Blockchain com 20 nós, notando um aumento significativo para todos os casos testados (Figura 5.5).

Figure 5.5: Tempo de resposta com 20 nós para diferentes cargas de trabalho.

* **Considerações Finais**

Este estudo abordou a simulação de uma rede Blockchain por meio de containers Docker e apresentou uma metodologia bem definida para avaliação de desempenho em sistemas baseados em Blockchain. A pesquisa envolveu a variação na quantidade de nós na Blockchain, examinando cenários com 10 e 20 nós, e aplicando diferentes cargas de trabalho para avaliação do desempenho. Utilizando a ferramenta JMeter, as métricas de vazão e tempo de resposta foram consideradas nos testes.

Os resultados destacaram que a Blockchain com 20 nós apresentou um tempo de resposta 70% maior em comparação com a configuração anterior, indicando que, embora o uso de Blockchain proporcione maior segurança, pode ocorrer uma redução no desempenho da aplicação. Isso sublinha a importância de equilibrar segurança e desempenho ao projetar sistemas baseados em Blockchain. A utilização de simulações possibilita avaliar o comportamento da aplicação antes da implementação, permitindo uma análise prévia do seu desempenho.

6 DISCUSSÕES

O blockchain, desde sua concepção revolucionária com o advento do Bitcoin em 2008, tem passado por uma notável trajetória de evolução. Nos últimos anos, observamos avanços significativos na tecnologia, impulsionados pela busca incessante por soluções para desafios preexistentes e pela expansão contínua de casos de uso em diversos setores.

Inicialmente concebido como a infraestrutura subjacente para criptomoedas, o blockchain tem ampliado suas fronteiras muito além do escopo financeiro. Uma das transformações mais marcantes é a expansão para contratos inteligentes. Esses protocolos autoexecutáveis não apenas automatizam processos, mas também introduzem uma camada de programabilidade ao blockchain, permitindo uma gama diversificada de aplicações.

O algoritmo de consenso, fundamental para a segurança e integridade do blockchain, também testemunhou mudanças notáveis. A transição do Proof-of-Work (PoW) para alternativas como Proof-of-Stake (PoS) e outras abordagens tem sido debatida intensamente. Essa busca por mecanismos de consenso mais eficientes visa mitigar preocupações ambientais associadas ao alto consumo de energia do PoW, enquanto busca melhorar a escalabilidade das redes.

O blockchain, outrora restrito às criptomoedas, tornou-se uma tecnologia adotada em setores como saúde, logística e governança. Inovações em segurança e privacidade são centrais para essa expansão, proporcionando confiança nas aplicações do blockchain em ambientes críticos.

Contudo, apesar dos avanços, desafios persistem. A escalabilidade, notoriamente, continua sendo uma área de foco. Soluções como camadas secundárias e a exploração de algoritmos de consenso alternativos buscam endereçar essas preocupações, mas o debate sobre a abordagem mais eficaz permanece em curso.

O diálogo em torno do blockchain nos últimos anos não apenas reflete avanços tecnológicos, mas também destaca a importância crescente da colaboração entre setores. Iniciativas de consórcio e padrões interindustriais estão moldando um ecossistema mais coeso, impulsionando a interoperabilidade e facilitando a adoção em larga escala.

Em suma, a evolução do blockchain nos últimos anos é marcada por um constante fluxo de inovações e ajustes. À medida que a tecnologia amadurece, as discussões em torno de seu papel na sociedade e na economia se intensificam. O blockchain, longe de ser uma tecnologia estática, continua a se metamorfosear, prometendo não apenas revolucionar setores específicos, mas também fundamentar a infraestrutura da próxima era digital.

7 CONCLUSÃO

A tecnologia blockchain emergiu como uma inovação transformadora, proporcionando descentralização e confiança em transações, contratos e registros digitais. Ao longo das décadas, desde sua concepção por Stuart e W. Scott Stornetta, até o aprimoramento por Satoshi Nakamoto com o advento do Bitcoin, a blockchain evoluiu significativamente. No entanto, apesar de suas conquistas, a tecnologia enfrenta desafios inerentes que exigem abordagens analíticas e soluções inovadoras.

A escalabilidade, custos de transação, interoperabilidade e privacidade destacam-se como desafios cruciais. A limitação na capacidade de processamento de transações em larga escala, muitas vezes avaliada em termos de Transações por Segundo (TPS), revela-se um obstáculo para a integração generalizada, especialmente em setores de alto volume, como sistemas de pagamento.

A modelagem analítica, utilizando ferramentas como cadeias de Markov, surge como uma abordagem valiosa para entender e superar esses desafios. Estudos, como aquele realizado por Cao et al. [33], exploram a relação entre taxas de chegada de transações, peso cumulativo e atraso de confirmação. Esses modelos fornecem insights valiosos para otimizar o desempenho da blockchain.

Além disso, a análise crítica das limitações da tecnologia blockchain destaca a necessidade de abordagens multifacetadas. Soluções propostas pela comunidade acadêmica e da indústria incluem o uso de estruturas inovadoras, como o Tangle no IOTA, que elimina a necessidade de mineradores e oferece escalabilidade potencialmente ilimitada.

Diante desses desafios, a pesquisa contínua e a colaboração entre acadêmicos, desenvolvedores e profissionais da indústria são essenciais. A implementação bem-sucedida de modelos analíticos, como cadeias de Markov, combinada com soluções inovadoras, pode moldar o futuro da blockchain, tornando-a mais eficiente, segura e adaptável às demandas de uma variedade de setores.

Em resumo, a evolução da tecnologia blockchain, seus desafios e soluções propostas refletem um campo dinâmico e promissor. Ao enfrentar esses desafios de maneira colaborativa, podemos construir uma base sólida para o desenvolvimento contínuo da blockchain e sua integração eficaz em diversas aplicações.

REFERENCES

[1] M. Di Pierro. What is a blockchain? In *Computing in Science & Engineering*, pages 19–25, 2017.

[2] IBM. *O que é a tecnologia blockchain?*

[3] Frank Hofmann, Simone Wurster, Eyal Ron, and Moritz Bohmecke-Schwafert. The immutability concept of blockchains and benefits of early standardization. In *Kaleidoscope: Challenges for a Data-Driven Society (ITU k)*, pages 1–8, 2017.

[4] Stornetta W.S Haber S. Springerlink journals journal of cryptology, vol.3 (2), p. *How to time-stamp a digital document*, pages 99–111, 1991.

[5] Abdurrashid Ibrahim Sanka, Muhammad Irfan, Ian Huang, and Ray C.C. Cheung. A survey of breakthroughs in blockchain technology: Adoptions, applications, challenges, and future research. In *Computer Communications*, pages 179–201, March 2021.

[6] Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform*, 2013.

[7] Christophe Schinckus. Proof-of-work based blockchain technology and anthropocene: An undermined situation? volume 152. *Renewable and Sustainable Energy Reviews*, Dezember 2021.

[8] Satoshi Nakamoto et al. A peer-to-peer electronic cash system. bitcoin (2008), 2020.

[9] Ross Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

[10] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, and Yue Cao. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, 9:61048–61073, 2021.

[11] Don Tapscott, Alex Tapscott, and B Revolution. How the technology behind bitcoin is changing money, business, and the world. *Information Systems*, pages 100–150, 2016.

[12] Melanie Swan. Blockchain: Blueprint for a new economy.–o'reill media. *Inc., Sebastopol, CA*, 2015.

[13] D Marques. *O que é fazer se a sua transação fica presa?* https://guiadobitcoin.com.br/o-que-fazer-se-a-sua-transacao-bitcoin-ficar-presa/, 2017.

[14] Xinle Yang, Yang Chen, and Xiaohu Chen. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 261–265. IEEE, 2019.

[15] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. 2014. *URL: https://github. com/ethereum/wiki/wiki/White-Paper*, 2019.

[16] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek. Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, 8:126927–126950, 2020.

[17] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan. *BLOCKBENCH: A Framework for Analyzing Private Blockchains*. ACM, 2017.

[18] Soohyeong Kim, Yongseok Kwon, and Sunghyun Cho. A survey of scalability solutions on blockchain. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1204–1207. IEEE, 2018.

[19] Sara Rouhani and Ralph Deters. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, 7:50759–50779, 2019.

[20] Xiaoying Zheng, Yongxin Zhu, and Xueming Si. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Applied Sciences*, 9(22):4731, 2019.

[21] Faruk Alpak, Yixuan Wang, Guohua Gao, and Vivek Jain. Benchmarking and field-testing of the distributed quasi-newton derivative-free optimization method for field development optimization. In *SPE Annual Technical Conference and Exhibition?*, page D021S040R005. SPE, 2021.

[22] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to scalability of blockchain: A survey. *Ieee Access*, 8:16440–16455, 2020.

[23] Junfeng Xie, F Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, and Yunjie Liu. A survey on the scalability of blockchain systems. *IEEE network*, 33(5):166–173, 2019.

[24] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek. Avaliação de desempenho de sistemas blockchain: Uma pesquisa sistemática. *IEEE Access*, 8:126927–126950, 2020.

[25] S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke. A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems. *Proceedings of the International Conference on Distributed Ambient and Pervasive Interactions (DAPI)*, pages 21–34, 2018.

[26] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7):1366–1385, Jul. 2018.

[27] V. Gramoli R. Han and X. Xu. Evaluating blockchains for iot. *Proc. 9th IFIP Int. Conf. New Technol. Mobility Secur. (NTMS), pp. 1-5*, Feb. 2018.

[28] C. Siripanpornchana S. Pongnumkul and S. Thajchayapong. Performance analysis of private blockchain platforms in varying workloads. *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), pp. 1-6*, Jul. 2017.

[29] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen. Análise de desempenho do algoritmo de consenso em blockchain privado. *Proc. IEEE Intell. Símbolo de Veículos (IV)*, pages 280–285, junho 2018.

[30] H. M. A. Aljassas e S. Sasi. Avaliação de desempenho de algoritmos de consenso de conjecturas de prova de trabalho e collatz. *Proc. 2nd Int. Conf. Compute. Aplicação. Inf. Secur. (ICCAIS), pp. 1-6*, maio de 2019.

[31] R. Deloin. Prova de conjectura de collatz. *Asian Res. J. Matemática, vol. 14, no. 2, pp. 1-18*, junho de 2019.

[32] RR Yadav, ETG Sousa, and GRA Callou. Performance comparison between virtual machines and docker containers. *IEEE Latin America Transactions*, 16(8):2282–2288, 2018.

[33] Bin Cao, Shouming Huang, Daquan Feng, Lei Zhang, Shengli Zhang, and Mugen Peng. Impact of network load on direct acyclic graph based blockchain for internet of things. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 215–218. IEEE, 2019.

[34] M. Swan. Blockchain: blueprint for a new economy. *O'Reilly Media, Inc.*, 2015.

[35] Jens Ducrée. Satoshi nakamoto and the origins of bitcoin–narratio in nomine, datis et numeris. *arXiv preprint arXiv:2206.10257*, 2022.

[36] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck. Disruptive technologies and business models: A case of blockchain. *Business & Information Systems Engineering*, pages 183–187, March 2017.

[37] Baidyanath Biswas and Rohit Gupta. Analysis of barriers to implement blockchain in industry and service sectors. *Computers Industrial Engineering*, 136:225–241, 2019.

[38] Pooja Dixit, Anuja Bansal, Pramod Singh Rathore, and Manju Payal. An overview of blockchain technology: Architecture, consensus algorithm, and its challenges. *Blockchain Technology and the Internet of Things*, pages 21–46, 2020.

[39] S. Rouhani and R. Deters. Performance analysis of ethereum transactions in private blockchain. *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS), pp. 70-74.*, Nov. 2017.

[40] Merunas Grincalaitis. *Mastering Ethereum: Implement advanced blockchain applications using Ethereum-supported tools, services, and protocols*. Packt Publishing Ltd, 2019.

[41] Gunter Bolch, Stefan Greiner, Hermann De Meer, and Kishor S Trivedi. *Queueing networks and Markov chains: modeling and performance evaluation with computer science applications*. John Wiley & Sons, 2006.

[42] Diego Ongaro and John Ousterhout. In search of an understandable consensus algorithm (extended version). In *Proceeding of USENIX annual technical conference, USENIX ATC*, pages 19–20, 2014.

[43] Dongyan Huang, Xiaoli Ma, and Shengli Zhang. Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1):172–181, 2019.

[44] Fengyang Guo, Xun Xiao, Artur Hecker, and Schahram Dustdar. Characterizing iota tangle with empirical data. In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pages 1–6. IEEE, 2020.