Universidade Federal do Pará
Campus Universitário de Castanhal - CCAST
Faculdade de Computação - FACOMP
Bacharelado em Engenharia de Computação

Simulação de ataque DDoS em redes Blockchain para cibersegurança

Geovane de Lima Duarte

UFPA / CCAST / FACOMP
Campus Universitário de Castanhal
Castanhal - Pará - Brasil
2025

Universidade Federal do Pará

Campus Universitário de Castanhal - CCAST

Faculdade de Computação - FACOMP

Bacharelado em Engenharia de Computação

Geovane de Lima Duarte

Simulação de ataque DDoS em redes Blockchain para cibersegurança

Monografia submetida à avaliação da Banca Examinadora aprovada pelo colegiado da Faculdade de computação da Universidade Federal do Pará e julgada adequada para a obtenção do Grau de Bacharelado em Engenharia de Computação.

Orientador: Drº José Jailton Henrique Ferreira Júnior

UFPA / CCAST / FACOMP

Campus Universitário de Castanhal

Castanhal - Pará - Brasil

2025

UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL - CCAST
FACULDADE DE COMPUTAÇÃO - FACOMP
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

Simulação de ataque DDoS em redes Blockchain para cibersegurança

Autor: Geovane de Lima Duarte

MONOGRAFIA DE GRADUAÇÃO SUBMETIDA À BANCA EXAMINADORA APROVADA PELA FACULDADE DE COMPUTAÇÃO, SENDO JULGADA ADEQUADA PARA A OBTENÇÃO DO GRAU DE BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO.

APROVADO EM: 21 de Fevereiro de 2025.

Castanhal - Pará - Brasil,

Banca Examinadora:

Drº José Jailton Henrique Ferreira Júnior
Orientador FACOMP/CCAST/UFPA

Prof.ª Drº. Igor Ruiz Gomes
(Avaliador Interno – FACOMP/CCAST/UFPA)

Prof.ª Drº. Tássio Costa Carvalho
(Avaliador Interno – FACOMP/CCAST/UFPA)

Visto:

Profª. Drª. Yomara Pinheiro Pires
(Diretora da Faculdade de Computação/CCAST/UFPA)

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

D812s Duarte, Geovane de Lima.
Simulação de ataque DDoS em redes Blockchain para cibersegurança / Geovane de Lima Duarte. — 2025.
81 f. : il. color.

Orientador(a): Prof. Dr. José Jailton Henrique Ferreira Júnior
Trabalho de Conclusão (Graduação) - Universidade Federal do Pará, Campus Universitário de Castanhal, Faculdade de Engenharia da Computação, Castanhal, 2025.

1. Blockchain. 2. Ataque DDoS. 3. Cibersegurança. 4. Sistemas distribuídos. I. Título.

CDD 004.36

Dedico este trabalho a todos que me ergueram quando caí, que me deram forças quando fraquejei e acreditaram em mim nos momentos mais sombrios. Aos que me demonstraram que a resiliência é forjada nas dificuldades e que, mesmo nas horas de fraqueza, a esperança nunca se perde. A vocês, que me ajudaram a continuar quando tudo parecia desmoronar, a minha eterna gratidão. Cada palavra de apoio, cada gesto de carinho, foi o alicerce que me permitiu alcançar este momento. Este TCC é, acima de tudo, um reflexo da força de todos que estiveram ao meu lado.

Agradecimentos

Primeiramente, agradeço imensamente a Deus, pela força infinita que me tem dado ao longo de toda a minha vida, especialmente nesta jornada acadêmica. A sua presença, mesmo nos momentos de incerteza, foi o alicerce que me sustentou, me dando coragem e sabedoria para continuar e para superar todos os obstáculos. A gratidão que sinto por tudo o que Ele me proporcionou é indescritível. Sem Ele, nada disso teria sido possível.

Aos meus familiares, não há palavras que possam expressar a profundidade da minha gratidão. Aos meus pais, Antonio e Fátima, que sempre acreditaram em mim, mesmo quando eu duvidava de mim mesmo, e me apoiaram da forma que estava ao seu alcance. Vocês foram a minha base, meus pilares. As palavras de incentivo e o exemplo de perseverança de vocês foram fundamentais para que eu alcançasse esse objetivo. A minha gratidão a vocês é eterna.

Às minhas irmãs, Luciete, Lucivane e Luciana, que sempre estiveram ao meu lado, me acompanhando nas conquistas e dificuldades. O apoio de vocês, as conversas, os conselhos e, muitas vezes, o simples gesto de estar ao meu lado, foram essenciais para me manter motivado e focado na meta que me propus. A vocês, eu dedico uma parte do meu sucesso, porque, sem o afeto e a confiança que obtive, eu não teria conseguido chegar até aqui.

A minha prima, Patrícia Lima, que me proporcionou momentos de tranquilidade e perspectiva, sempre pronta a me ouvir e a me oferecer palavras de conforto e encorajamento. A nossa amizade e cumplicidade foram de grande valia ao longo dessa caminhada, e sou imensamente grato por tê-la ao meu lado.

Ao meu orientador, mestre JJJ, não tenho palavras suficientes para expressar o quanto sou grato. Você foi muito mais do que um orientador acadêmico; foi uma figura paterna, sempre compreensivo, paciente e disposto a guiar-me. Sua orientação foi fundamental para o desenvolvimento desta monografia. Os ensinamentos que me transmitiu, a sua visão crítica e, acima de tudo, o seu apoio incondicional nos momentos de maior desafio, foram determinantes para a conclusão deste trabalho. Sem você, eu não teria conseguido ultrapassar os obstáculos e encontrar os caminhos certos. Sua contribuição foi decisiva, e sou eternamente grato por sua orientação e por sua generosidade.

À minha diretora, Yomara Pires, agradeço profundamente pela confiança que depositou em mim e pelo apoio prestado nesses últimos semestres. A sua seriedade e compromisso com o desenvolvimento dos alunos me inspiraram a buscar sempre o melhor em mim mesmo, e por isso, sou imensamente grato.

À Alícia Maia e Sarah Cabral, minhas companheiras fiéis desde o início da graduação, que ficaram ao meu lado em todos os momentos dessa caminhada. A amizade de vocês é algo que eu guardo para sempre. agradeço pelo apoio incondicional, pelos conselhos, pelas conversas e pelo companheirismo. Juntos, enfrentamos desafios, comemoramos vitórias e, acima de tudo, crescemos como pessoas e como profissionais. A minha jornada não teria sido a mesma sem a presença de vocês.

Aos demais integrantes da EC 2020.4, agradeço sinceramente pelo apoio e pela amizade que compartilharam comigo ao longo dos anos. Cada um de vocês teve um impacto importante na minha vida e no meu percurso acadêmico. As trocas de experiências, as reflexões, e os momentos de descontração ajudaram a aliviar a pressão e a me manter focado nos meus objetivos. agradecimento de coração pela presença de todos.

Ao senhor Raimundo Rocha, à Nilce Anézio e aos seus filhos Renan, Ruan, Renildo, Raiane e Rainara, não tenho palavras suficientes para expressar minha gratidão. Vocês abriram suas portas para mim durante esses quatro anos de graduação, oferecendo-me não apenas um local de apoio, mas também um lugar de acolhimento e carinho. Vocês foram pais verdadeiros para mim e mais que grandes amigos; tornaram-se família, e sem o apoio e a confiança que recebi de vocês, eu teria enfrentado ainda mais dificuldades. Muito obrigado por me ajudar a encontrar o equilíbrio entre os estudos e as demandas da vida. O que vivi com vocês fica para sempre no meu coração.

Aos amigos que se tornaram família - e partes de mim - minha mais profunda e sincera gratidão. A saber: Jean Marlisson, Ruan Waldiney (vulgo Disney), Lucas Santos, Weverson Célio, Gabriel Coelho (vulgo Coelhão), Lari, Juliana Castro, Klissia de Paula, Vini Melo, Paula Isabely, Beatriz Celestina, Maria Beatriz (Bea), Dandara Rafaela, Gaby Chagas, Wivyane (minha nãe postiça), Duda, Mary, Soraia (minha vó postiça), Time NOC – SEA Telecom e tantos outros que, mesmo não citados nominalmente, estiveram presentes com o coração: saibam que carrego cada um de vocês comigo. Obrigado por terem sido minha rede de apoio nesses últimos meses (foram dias caóticos); Obrigado por me mostrarem o valor da companhia verdadeira, da escuta generosa, da palavra amiga e do apoio silencioso nos momentos mais difíceis. Obrigado por me acolherem sem julgamentos, por me aconselharem com sabedoria, por me ajudarem a não enfraquecer diante das adversidades e, principalmente, por me ensinarem que a amizade, quando é real, se torna abrigo, força e extensão da alma. Cada um de vocês foi luz quando tudo parecia escuro demais, e por isso, levo todos no meu coração.

Aos mestres que me ensinaram durante essa trajetória acadêmica, minha eterna gratidão. Cada um de vocês contribuiu de alguma forma para o meu desenvolvimento, seja pela transmissão de conhecimentos técnicos, seja pelos ensinamentos sobre a vida e a carreira profissional. Sem o apoio e as orientações de vocês, eu não teria chegado até aqui. obrigado, de coração, a todos que me ajudaram a alcançar este objetivo.

E, por fim, à Universidade Federal do Pará, que me proporcionou a oportunidade de crescer intelectualmente e pessoalmente. A UFPA foi a base da minha formação e, sem ela, este momento não seria possível. agradecimentos à instituição, aos professores e aos colegas que fizeram parte dessa jornada e que, de alguma forma, desenvolveram para a realização deste trabalho.

A todos que, direta ou indiretamente, fizeram parte dessa caminhada, o meu mais sincero agradecimentos.

"O saber é a chave que abre todas as portas. Quando a última porta é aberta, o mundo se revela. "

Friedrich Nietzsche

Resumo

Este trabalho tem como objetivo principal a criação e avaliação de uma rede Blockchain desenvolvida com código em Python - tendo como base o algoritmo da bitcoin Ethereum - com foco na análise de sua eficiência e resiliência diante de ataques de sobrecarga, como os ataques DDoS. A proposta é investigar como a rede se comporta sob condições adversas para melhorar a cibersegurança de sistemas descentralizados, como os Blockchains.

A abordagem desenvolvida envolve a construção de um servidor local para hospedar a rede Blockchain, permitindo o controle e a análise em um ambiente controlado. Após a implementação da rede, foram realizados testes em equipamento com configuração definida inicialmente, para observar como o Blockchain responde a variações de hardware e capacidade de processamento. A simulação do ataque DDoS, em particular o tipo HTTP Flood, foi conduzida em diferentes cenários para verificar o impacto na operação da rede. O objetivo foi observar se o Blockchain consegue manter sua funcionalidade, segurança e disponibilidade diante de ataques excessivos, comuns em ataques DDoS.

A análise dos resultados envolveu a coleta de estatísticas relacionadas à padrão de transação, volume de dados e disponibilidade de serviços. Com esses dados, foi possível identificar pontos críticos e sugerir possíveis estratégias de mitigação, como a implementação de filtros de tráfego e algoritmos de consenso mais robustos, que podem aumentar a segurança e a eficiência operacional da rede em situações de ataque.

Os resultados encontrados mostraram que a solução foi eficaz em manter a estabilidade do Blockchain em diferentes cenários de ataque, com uma boa eficiência em termos de volume de dados e disponibilidade de serviços. Essa pesquisa demonstrou o potencial de redes Blockchain para resistir a ataques DDoS, combinados com estratégias adequadas de mitigação, contribuindo para um melhor entendimento das vulnerabilidades e possibilidades de aprimoramento na cibersegurança de sistemas distribuídos.

Palavras-chaves: Blockchain. Ataque DDoS. cibersegurança. Sistemas distribuídos.

Abstract

This work's main objective is to create and evaluate a Blockchain network developed with Python code - based on the bitcoin Ethereum algorithm - focusing on analyzing its efficiency and resilience in the face of overload attacks, such as DDoS attacks. The proposal is to investigate how the network behaves under adversarial conditions to improve the cybersecurity of decentralized systems, such as Blockchains.

The approach developed involves building a local server to host the Blockchain network, allowing control and analysis in a controlled environment. After implementing the network, tests were carried out on equipment with an initially defined configuration, to observe how the Blockchain responds to variations in hardware and processing capacity. The DDoS attack simulation, in particular the HTTP Flood type, was conducted in different scenarios to verify the impact on network operation. The objective was to observe whether Blockchain can maintain its functionality, security and availability in the face of excessive attacks, common in DDoS attacks.

Analysis of the results involved collecting statistics related to transaction pattern, data volume and service availability. With this data, it was possible to identify critical points and suggest possible mitigation strategies, such as the implementation of traffic filters and more robust consensus algorithms, which can increase the security and operational efficiency of the network in attack situations.

The results found showed that the solution was effective in maintaining the stability of the Blockchain in different attack scenarios, with good efficiency in terms of data volume and service availability. This research demonstrated the potential of Blockchain networks to resist DDoS attacks, combined with appropriate mitigation strategies, contributing to a better understanding of vulnerabilities and possibilities for improving the cybersecurity of distributed systems.

Keywords: Blockchain. DDoS attack. cybersecurity. Distributed systems.

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e siglas

AML	Anti-Money Laundering (Combate à Lavagem de Dinheiro)
AP	Access Point (Ponto de Acesso)
API	Application Programming Interface (Interface de Programação de Aplicações)
CNN	Convolutional Neural Network (Rede Neural Convolucional)
CPU	Central Processing Unit (Unidade Central de Processamento)
DDoS	Distributed Denial-of-Service (Negação de Serviço Distribuída)
DNN	Deep Neural Network (Rede Neural Profunda)
DNS	Domain Name System (Sistema de Nomes de Domínio)
DoS	Denial-of-Service (Negação de Serviço)
GRU	Gated Recurrent Unit (Unidade Recorrente de Portão)
HTTP	HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto)
i5	Processadores da Intel (Intel Core i5)
IA	Inteligência Artificial
IEA	International Energy Agency (Agência Internacional de Energia)
IBIP	Instituto Brasileiro de Inteligência em Pesquisa
ICMP	Internet Control Message Protocol (Protocolo de Mensagem de Controle da Internet)
IoT	Internet of Things (Internet das Coisas)
JSON	JavaScript Object Notation (Notação de Objeto JavaScript)
LEDGER	Registro de transações (Livro razão)
LSTM	Long Short-Term Memory (Memória de Longo-Curto Prazo)
ML	Machine Learning
P2P	Peer-to-Peer (Ponto-a-Ponto)

PoS	Proof of Stake (Prova de Participação)
PoW	Proof of Work (Prova de Trabalho)
PBFT	Practical Byzantine Fault Tolerance (Tolerância a Falhas Bizantinas Práticas)
REST	Representational State Transfer (Transferência de Estado Representacional)
SHA-256	Secure Hash Algorithm 256 (Algoritmo de Hash Seguro 256)
SMTP	Simple Mail Transfer Protocol (Protocolo Simples de Transferência de Correio)
SVM	Support Vector Machine (Máquina de Vetores de Suporte)
TDD	Time Division Duplex (Duplexação por Divisão de Tempo)
TCP	Transmission Control Protocol (Protocolo de Controle de Transmissão)
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuário)

Sumário

1 Introdução

Neste capítulo, pretende-se estabelecer uma base para o desenvolvimento da monografia, introduzindo o tema de forma a situar o leitor no contexto do estudo. Inicialmente, realiza-se uma contextualização, buscando oferecer uma visão sobre o assunto, além de enfatizar a importância e a relevância da pesquisa no cenário atual.

A seguir, delineia-se o problema de pesquisa, o que representa o questionamento central que orienta esta investigação e justifica sua realização. Esse questionamento é abordado de maneira precisa, de modo a evidenciar as lacunas que essa monografia se propõe a investigar.

Na sequência, são expostos os objetivos gerais e específicos, que configuram as diretrizes principais do estudo. Esses objetivos visam discorrer cada etapa dessa análise, permitindo que o trabalho alcance resultados fundamentados. Por fim, este capítulo apresenta a estrutura da monografia, oferecendo uma visão de como o estudo será desenvolvido, que é fundamental para proporcionar uma leitura objetiva e favorecer uma compreensão gradual dos temas e abordagens adotadas ao longo da pesquisa.

1.1 Contextualização

Segundo (CARVALHO, 2023), a Cibersegurança é essencialmente a prática de salvaguardar sistemas, redes e programas no ambiente digital de ataques mal-intencionados. Ela incorpora a aplicação de técnicas como criptografia e a observância de diretrizes e regulamentos para prevenir danos tanto em hardware quanto em software. Esta área abrange uma variedade de instrumentos, políticas, estratégias de segurança, diretrizes, métodos de gestão de riscos, práticas recomendadas e tecnologias destinadas a proteger os ambientes digitais, as organizações e seus usuários. A proteção se estende a computadores, infraestruturas e sistemas de telecomunicações que armazenam informações valiosas no ambiente digital.

A finalidade da Cibersegurança é assegurar propriedades críticas como integridade, disponibilidade e confidencialidade das informações, mitigando riscos potenciais no ambiente digital. Além de focar na proteção do próprio ambiente digital, ela também visa proteger as operações que ocorrem dentro desse espaço e quaisquer ativos associados, diretamente ou indiretamente, com o ambiente digital (MOREIRA, 2023).

O termo "ciberespaço"refere-se ao domínio global interconectado por meio de sistemas de informação, como a internet, redes de telecomunicações, sistemas computacionais e controladores. A Cibersegurança enfrenta desafios constantes de atividades ilícitas, como

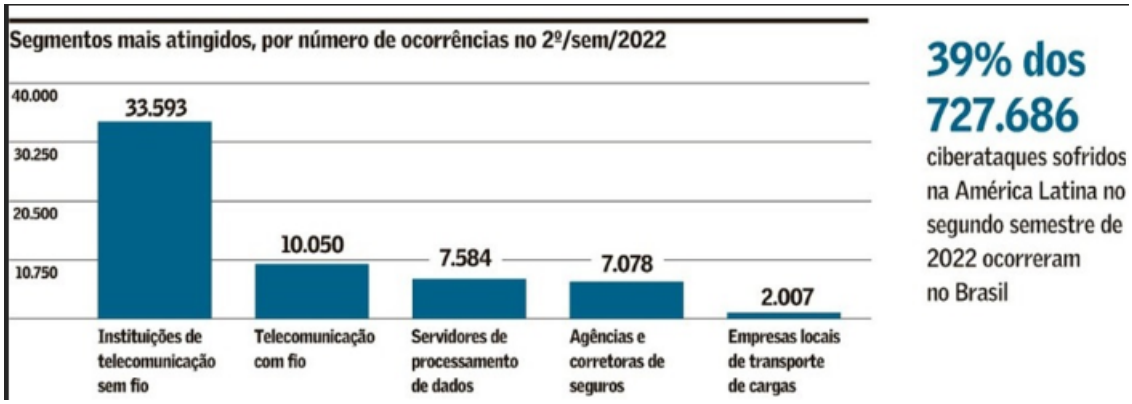
acessos não autorizados a informações confidenciais, modificações indevidas de dados e uso abusivo de recursos computacionais (CARVALHO, 2023).

A segurança nos sistemas digitais representa um desafio tanto técnico quanto social. Do ponto de vista técnico, a crescente complexidade das arquiteturas de hardware, sistemas operacionais e protocolos exige políticas de segurança mais sofisticadas. Socialmente, a falta de conhecimento técnico entre os usuários dos sistemas de informação pode aumentar a vulnerabilidade a problemas de segurança (GIL, 2021).

As organizações hoje enfrentam a necessidade premente de garantir que seus sistemas sejam robustos o suficiente para resistir a ataques cibernéticos. Um ataque bem-sucedido pode acarretar custos elevados, prejudicando a reputação, o negócio e a estabilidade financeira da entidade afetada. Isso se deve à dificuldade de detectar ataques em tempo real e à crescente sofisticação das técnicas de ataque (RABADãO, 2021).

Nos últimos anos, o panorama dos ataques cibernéticos tem se tornado uma preocupação crescente para organizações e indivíduos globalmente. A prevalência destes ataques tem aumentado exponencialmente, impulsionada pela digitalização acelerada de serviços em diversas esferas da vida cotidiana. Ataques de phishing, ransomware, violações de dados e outras formas de ciberataques têm demonstrado não apenas sua frequência, mas também a sofisticação crescente, causando impactos significativos que vão desde prejuízos financeiros substanciais até a perda de confiança e danos irreparáveis à reputação de entidades afetadas. O cenário atual exige soluções de cibersegurança mais robustas e inovadoras, capazes de combater essas ameaças digitais cada vez mais complexas e adaptativas (VAL, 2023).

Figura 1 – Dados sobre ciberataques no país



Fonte: Retirado de Relatório de Inteligência de Ameaça DDoS, 2023.

A Figura 1 apresenta um gráfico de barras que detalha a distribuição de ciberataques no Brasil, segmentados por setor, durante o segundo semestre de 2022. O estudo em questão, intitulado "Blockchain como Mecanismo de Reforço da Cibersegurança", pode se valer

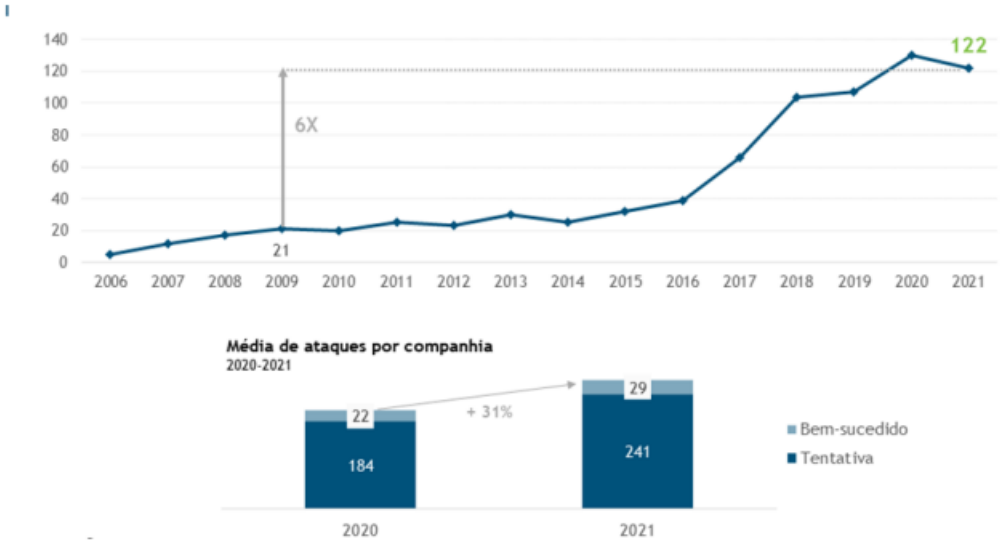
desses dados para destacar a relevância e a urgência de fortalecer as estratégias de segurança digital nas organizações.

Pode-se observar que as instituições de telecomunicações sem fio são o alvo mais frequente, com 33.593 ocorrências de ataques cibernéticos. Em seguida, as empresas de telecomunicações com fio registraram 10.050 ocorrências. Os servidores de processamento de dados sofreram 7.584 ataques, enquanto agências e corretoras de seguros enfrentaram 7.078. Por fim, as empresas locais de transporte de cargas foram alvo de 2.007 ciberataques (GLOBO, 2021).O gráfico também destaca que 39% dos 727.686 ciberataques registrados na América Latina no período mencionado ocorreram no Brasil. Este dado enfatiza a posição crítica do Brasil no cenário de cibersegurança na América Latina, indicando uma vulnerabilidade significativa na infraestrutura de TI do país (GLOBO, 2021).

Deste modo, percebe-se a importância da implementação da tecnologia blockchain como um potencial reforço à cibersegurança. O estudo poderia argumentar que, dada a frequência e a gravidade dos ciberataques nos setores mais afetados, soluções baseadas em blockchain poderiam trazer benefícios consideráveis, como a imutabilidade e a descentralização, contribuindo assim para a diminuição da vulnerabilidade das instituições a ataques externos.

A imutabilidade garante que uma vez que os dados são registrados na blockchain, eles não podem ser alterados retroativamente, o que poderia ajudar a prevenir fraudes e acessos não autorizados. A descentralização, por outro lado, assegura que a informação não esteja concentrada em um único ponto de falha, o que aumenta a resiliência das redes frente a ataques distribuídos de negação de serviço (DDoS), como os frequentemente sofridos pelas instituições mencionadas no gráfico.

Figura 2 – Números de incidentes cibernéticos significativos no mundo (2006-2021)



Fonte: Elaboração IBIP com dados IEA e Accenture, 2022

A Figura 2 apresenta um conjunto de informações estatísticas referentes ao número de incidentes cibernéticos significativos em escala global, abrangendo o período de 2006 a 2021. Através de um gráfico de linha, pode-se observar uma tendência crescente no número de incidentes, culminando em um aumento significativo de seis vezes comparado ao início do intervalo monitorado. Especificamente, o gráfico mostra um salto de 21 incidentes em 2006 para 122 em 2021.

Em adição ao gráfico de linha, há um gráfico de barras que fornece uma comparação entre a média de ataques por companhia nos anos de 2020 e 2021. É notável que, em 2021, houve um aumento de 31% na média de ataques em comparação com 2020, passando de uma média de 184 ataques por companhia para 241. O gráfico de barras diferencia ainda os ataques bem-sucedidos dos que foram apenas tentativas, o que é crucial para entender a eficácia das medidas de segurança existentes (IBP, 2022)

O gráfico da figura 2, serve como uma evidência da crescente necessidade de soluções de segurança cibernética mais eficazes e avançadas. O aumento nos incidentes cibernéticos destaca a importância de explorar novas tecnologias, como a blockchain, que podem oferecer uma estrutura mais segura devido às suas características intrínsecas de imutabilidade, descentralização e transparência.

Dentro do contexto do estudo, essas estatísticas podem ser utilizadas para argumentar a favor da implementação de blockchain como uma medida proativa e preventiva. A tecnologia poderia potencialmente reduzir o número de ataques bem-sucedidos, graças à dificuldade de alterar ou excluir informações uma vez que elas são adicionadas à cadeia de blocos, e à distribuição da rede que impede um ponto único de falha. Esta análise estatística fornece, portanto, uma base quantitativa para a pesquisa, enfatizando a relevância e a urgência de avançar na adoção do blockchain na cibersegurança para enfrentar desafios cada vez maiores neste domínio (IBP, 2022).

A blockchain, conhecida principalmente por seu papel como a base da criptomoeda Bitcoin, tem muito mais a oferecer do que apenas transações financeiras. como descrito por Rabadão (2021), é uma tecnologia de registro distribuído que utiliza criptografia para garantir a segurança e a integridade dos dados. Sua arquitetura distribuída, descentralizada e imutável oferece a possibilidade de criar registros seguros e confiáveis que não podem ser adulterados. Essas características a tornam uma opção interessante para enfrentar questões de autenticação, integridade de dados, rastreabilidade e confiança em ambientes digitais.

A arquitetura da blockchain é um sistema distribuído e descentralizado que facilita a troca segura de informações e transações entre diversos participantes, eliminando a necessidade de uma autoridade central. Essa estrutura é suportada por uma rede peer-to-peer (P2P), onde os nós interconectados mantêm uma cópia idêntica do registro completo de transações, conhecido como o livro-razão ou blockchain. As transações são agrupadas

em blocos, cada um contendo um cabeçalho com metadados importantes e um conjunto de transações. O algoritmo de consenso é essencial para determinar a validade e a ordem das transações, sendo o Proof of Work um dos mais conhecidos. Além disso, a criptografia desempenha um papel crucial na garantia da segurança e integridade das transações, enquanto os contratos inteligentes automatizam processos e operam na blockchain. Uma vez adicionada à blockchain, uma transação é considerada imutável, garantindo a integridade dos registros e fornecendo um histórico confiável de todas as transações realizadas na rede.

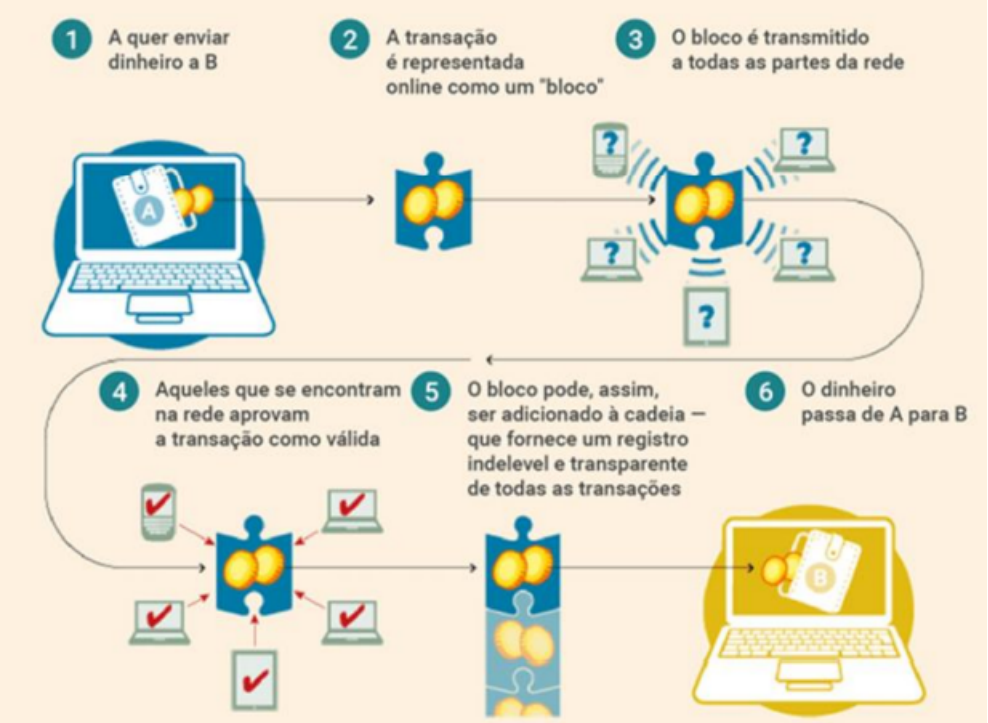
Figura 3 – Arquitetura da Blockchain

Fonte: Valuehots, 2019

A blockchain pode ser uma ferramenta eficaz para melhorar a cibersegurança, como destacado por Gil (2021). A tecnologia oferece uma série de benefícios, incluindo segurança aprimorada, integridade de dados e rastreabilidade. Ao explorar os méritos e desafios subjacentes da adoção da blockchain na cibersegurança, esse estudo pretende contribuir para o avanço do conhecimento nesse campo emergente (GIL, 2021).

Em meio à busca por medidas de proteção mais eficazes contra ameaças digitais, a tecnologia blockchain emergiu do ponto fraco das criptomoedas como o Bitcoin e agora assume um papel promissor no fornecimento de uma resposta. Uma característica definidora do blockchain é que ele é um sistema de registro de informações com uma estrutura descentralizada, distribuída e imutável. Funciona como um livro digital no qual as transações ou registros são inseridos em blocos, cada bloco está conectado criptograficamente ao anterior, formando uma cadeia contínua e segura de informações (MOREIRA, 2023).

Figura 4 – Funcionamento da cadeia de blocos de uma Blockchain)



Fonte: Horta, 2021

A Figura 4 descreve o fluxo de uma transação financeira utilizando a tecnologia blockchain, processo esse que é altamente relevante para o estudo sobre a aplicação da blockchain na cibersegurança. No início do processo (etapa 1), o usuário A deseja transferir dinheiro digital para o usuário B. Nesta etapa inicial, é crucial garantir a autenticidade do usuário A.

Os sistemas de autenticação, como autenticação de dois fatores e biometria, são fundamentais para evitar que hackers assumam identidades falsas e realizem transações fraudulentas. Essa ação é representada na etapa 2 como um bloco online, um pacote de dados que encapsula os detalhes da transação. Aqui, a criptografia desempenha um papel crucial. Os detalhes da transação devem ser criptografados para proteger as informações confidenciais, como valores transferidos e detalhes de contas bancárias, contra acesso não autorizado.

Em seguida, na etapa 3, este bloco é comunicado à rede blockchain, consistindo em diversos nós ou participantes que têm uma cópia do livro-razão (Ledger) distribuído. Durante a transmissão do bloco para a rede blockchain, é vital usar protocolos de comunicação seguros, como SSL/TLS, para proteger contra interceptação e manipulação de dados. Além disso, verificações de integridade dos dados podem ser implementadas para garantir que o bloco não tenha sido alterado durante a transmissão (HORTA, 2022)

Na etapa 4, os participantes da rede validam a transação, um passo fundamental

para assegurar que a transferência é legítima e não uma tentativa de fraude. Nesta etapa, os participantes da rede executam verificações para garantir que a transação atenda aos critérios definidos, como saldo suficiente na conta de A e conformidade com regulamentos anti-lavagem de dinheiro (AML). Para garantir que a validação ocorra de forma distribuída e confiável, são utilizados algoritmos de consenso, como Proof of Work (PoW) ou Proof of Stake (PoS) para garantir a veracidade desse processo.

Com a validação concluída, o bloco é adicionado à cadeia de blocos existente (etapa 5), atualizando o registro público de todas as transações. Esta cadeia funciona como um registro imutável, fundamental para a integridade e confiabilidade do processo. Além disso, a integridade da cadeia de blocos é fundamental. Dessa forma, mecanismos de hashing são empregados para vincular cada bloco à cadeia anterior, tornando extremamente difícil para um invasor adulterar blocos anteriores sem ser detectado. Isso garante que o histórico de transações permaneça imutável e confiável. Finalmente, na etapa 6, a transação é concluída com o dinheiro passando de A para B, solidificando a transferência de valores de maneira segura e verificável, ou seja, as medidas de segurança são implementadas para garantir que a transferência de valores ocorra de forma segura, incluindo criptografia de ponta a ponta para proteger os dados durante o trânsito e a autenticação dos usuários envolvidos para garantir que apenas as partes autorizadas possam concluir a transação. (HORTA, 2022).

A validação por múltiplos nós e a imutabilidade do registro de transações são características que naturalmente fortalecem a segurança digital, dificultando ataques como falsificação e dupla despesa. Portanto, a integração da blockchain na cibersegurança oferece um método proativo e resistente contra uma variedade de ciberameaças, o que justifica a relevância e a atualidade do tema em investigação (HORTA, 2022).

Os valores e crenças fundamentais sobre o blockchain estão incorporados na sua capacidade de garantir a transparência e a responsabilização dos dados sem qualquer controle de terceiros. Essa transparência pode ser garantida por mecanismos de consenso que definem o conjunto de regras em relação às mudanças no sistema blockchain, como a adição de novas entradas (GIL, 2021). Essas transações são verificadas pelos usuários da rede por meio de métodos criptográficos e, uma vez validadas, tornam-se parte integrante do livro-razão compartilhado. Outro aspecto é que este tipo de sistema se caracteriza pela visibilidade explícita ou certa da informação, o que, embora mantenha a proteção da identidade, contribui para a construção de confiança entre os atores (GIL, 2021).

Figura 5 – Encandeamento criptográfico da Blockchain)

Fonte: Proof, 2017

A utilização do blockchain como tecnologia na área de segurança cibernética traz novas abordagens para salvaguardar informações e sistemas de controle. Devido à sua estrutura, a tecnologia garante um nível extra de segurança que evita ataques de falsificação ou manipulação não autorizada, ao mesmo tempo que proporciona total transparência para todas as operações realizadas dentro do blockchain. Portanto, estas perspectivas revelam que a tecnologia é um meio de combate às ameaças cibernéticas que um dia revolucionarão a esfera da proteção e gestão da informação digital (MOREIRA, 2023).

A pesquisa não apenas examinará os benefícios potenciais da aplicação da blockchain, mas também identificará e analisará os possíveis obstáculos e limitações que podem surgir ao integrar essa tecnologia inovadora na cibersegurança.

Com uma abordagem baseada em uma revisão da literatura e avaliações analíticas, este estudo busca fornecer uma compreensão da viabilidade, potencialidades e desafios de utilizar a blockchain como um mecanismo de reforço da cibersegurança. Ao fazer isso, ele contribuirá para uma discussão acadêmica enriquecedora e, ao mesmo tempo, oferecerá informações relevantes para a comunidade empresarial e para os profissionais que buscam soluções inovadoras para os problemas de segurança digital.

1.2 Motivação e Desafios

A integração da tecnologia blockchain na cibersegurança tem o potencial de transformar a maneira como a proteção de dados e sistemas são abordados, oferecendo uma camada adicional de confiança e segurança. Com a ascensão contínua de violações de dados, ataques cibernéticos e fraudes, a pesquisa neste domínio é crucial para identificar como a blockchain pode ajudar a enfrentar os desafios atuais da segurança digital, abordando questões de autenticação, integridade de dados e rastreabilidade. Além disso, analisar as implicações práticas, os benefícios e as limitações da aplicação da blockchain na cibersegurança é fundamental para orientar decisões estratégicas e técnicas de organizações que buscam fortalecer suas estratégias de proteção de dados e infraestruturas digitais.

As características fundamentais da blockchain, como a imutabilidade, a transparência e a descentralização, contribuem para uma arquitetura de segurança que dificulta ataques de alteração de dados e acesso não autorizado. Por exemplo, uma análise publicada nos anais de um congresso internacional de segurança cibernética mostrou que, em sistemas de blockchain bem implementados, o tempo para comprometer a segurança de uma transação é aumentado em 40, tornando os ataques cibernéticos mais complexos e menos propensos ao sucesso (MOREIRA, 2023).

Tabela 1 – Empresas que utilizam ou planejam aplicar Blockchain na cibersegurança

Empresa	**Setor**	**Status de implementação da Blockchain**	**Observações**
AlphaTech Security	Tecnologia da Informação	Em uso	Redução de 30% nos incidentes de segurança.
BeSafe Insurance	Seguros	Em planejamento	Explorando Blockchain para autenticação segura.
CryptoData Storage	Armazenamento de Dados	Em uso	Implementou Blockchain para garantir a integridade dos dados.
FinSecure Bank	Financeiro	Em uso	Melhoria significativa na segurança das transações.
Global Health Systems	Saúde	Em planejamento	Avaliando Blockchain para proteção de prontuários médicos.

Fonte: Autor, 2024.

A tabela 1 ilustra uma variedade de empresas de diferentes setores que reconhecem a importância de integrar a blockchain em suas estratégias de cibersegurança. Algumas já estão colhendo os benefícios dessa integração, enquanto outras estão na fase de planejamento e avaliação de como a blockchain pode fortalecer suas defesas contra-ataques cibernéticos. A adoção da tecnologia reflete um movimento estratégico para aumentar a resiliência contra ameaças digitais, uma necessidade que é enfatizada pelas estatísticas de crescimento de incidentes cibernéticos globais (MOREIRA, 2023).

Dessa forma, a pergunta de pesquisa que norteia este estudo é: "De que maneira a tecnologia blockchain pode ser aplicada para reforçar a cibersegurança e mitigar os impactos decorrentes de ataques cibernéticos?"Esta indagação surge diante da crescente necessidade de soluções para enfrentar os desafios da segurança digital que foram supracitadas, em um contexto global caracterizado pela sofisticação e frequência dos ataques cibernéticos. Assim, a pesquisa visa contribuir para o avanço do entendimento sobre a integração da

blockchain na cibersegurança, além de fornecer direções para sua implementação eficaz no enfrentamento de ciberataques.

Nesse sentido, o estudo proposto visa investigar como exatamente o Blockchain pode ser empregado para fortalecer a cibersegurança, examinando suas aplicações específicas, vantagens, bem como as dificuldades e dilemas inerentes a essa adoção. Através de uma análise sistemática, o trabalho busca avaliar a eficácia e as limitações da integração do Blockchain no panorama da segurança cibernética.

1.3 Objetivos

GERAL

Desenvolver e avaliar uma rede Blockchain em Python, direcionada à análise de sua eficiência e resiliência diante de ataques de negação de serviços distribuídos (DDoS), a fim de ampliar o entendimento e aprimorar a cibersegurança de sistemas descentralizados.

ESPECÍFICOS:

- Implementar uma rede Blockchain em ambiente de servidor local para viabilizar o monitoramento e controle em condições experimentais, permitindo a simulação de ataques e a análise das respostas do sistema em um ambiente virtual;
- Simular ataques DDoS em diversos cenários, a fim de examinar o impacto sobre a operação e disponibilidade da rede sob condições de sobrecarga;
- Coletar e analisar métricas de desempenho e disponibilidade durante as simulações de ataque, visando identificar pontos críticos de vulnerabilidade .

1.4 Organização do Trabalho

Este trabalho está estruturado da seguinte forma:

Capítulo 1: Apresenta uma introdução ao contexto de ataque cibernéticos e a importância da implementação de Blockchain, justificando a relevância desta pesquisa no campo da cibersegurança. Expõe os objetivos da investigação e destaca a importância de desenvolver estratégias de mitigação para fortalecer a resiliência e a eficiência operacional dessas redes descentralizadas.

Capítulo 2: Fornecer uma revisão bibliográfica dos conceitos fundamentais e técnicas relacionadas à segurança em redes Blockchain e ataques de sobrecarga, abordando mecanismos de defesa exclusivamente utilizados contra ataques DDoS.

Capítulo 3: Apresenta estudos correlatos que fundamentaram a elaboração deste trabalho, detalhando suas contribuições e limitações, além de demonstrar como pesquisas anteriores embasaram a abordagem aplicada para a simulação de ataques DDoS.

Capítulo 4: Explica a metodologia aplicada, com foco na implementação e configuração de um ambiente de simulação para ataques DDoS em uma rede Blockchain. Detalhamos as etapas fáceis para alcançar os objetivos propostos, enfatizando as técnicas e métodos de análise que possibilitam a mensuração da resiliência.

Capítulo 5: Descreve os resultados obtidos com a simulação de ataques e a eficácia das estratégias de mitigação testadas, discutindo as métricas de desempenho e os impactos observados na disponibilidade e estabilidade da rede Blockchain sob condições adversas.

Capítulo 6: Apresenta as considerações finais do trabalho, sugestões para futuras pesquisas e os principais desafios que ainda precisam ser superados para aprimorar a cibersegurança em redes Blockchain.

2 Fundamentação Teórica

2.1 Considerações iniciais sobre o capítulo

A tecnologia Blockchain tem se consolidado como uma solução inovadora para garantir segurança, transparência e descentralização em diversas aplicações, desde criptomoedas até rastreamento de ativos e contratos inteligentes. No entanto, para compreender plenamente seu impacto e desafios, é essencial explorar seus fundamentos, sua evolução histórica e os princípios que regem sua arquitetura.

Este capítulo apresenta uma visão abrangente da Blockchain, começando por seus conceitos e componentes essenciais, passando por sua trajetória histórica e os princípios técnicos que a sustentam. Além disso, será discutida a relevância da cibersegurança no contexto da Blockchain, destacando os impactos dos ataques cibernéticos e, especificamente, a ameaça representada pelos ataques DDoS. A partir dessa análise, busca-se entender os desafios e estratégias para mitigar riscos e fortalecer a resiliência da tecnologia Blockchain diante de ameaças cibernéticas.

2.2 Blockchain

2.2.1 Conceitos

A blockchain é uma tecnologia que funciona como um sistema de registro distribuído e descentralizado, caracterizado por armazenar informações de forma imutável, segura e transparente (SOUZA et al., 2024). Essencialmente, consiste em uma série de blocos encadeados que armazenam conjuntos de transações ou dados. Cada bloco está vinculado ao anterior por meio de uma hash criptográfica, formando uma cadeia contínua que preserva a ordem cronológica dos eventos registrados (GREVE et al., 2018).

2.2.2 Características

As principais características da tecnologia blockchain, serão detalhadas na tabela a seguir, apresentando tanto os aspectos técnicos quanto os funcionais que a diferenciam.

Tabela 2 – Características da Blockchain

Característica	**Descrição**
Descentralização	Elimina intermediários e permite transações diretas entre pares, reduzindo custos e aumentando a autonomia dos participantes.
Imutabilidade	Registros não podem ser alterados sem o consenso da rede, assegurando a integridade e confiabilidade das informações armazenadas.
Transparência	Oferece visibilidade total dos dados para os participantes autorizados, facilitando auditorias e garantindo a rastreabilidade das transações.
Criptografia	Protege dados sensíveis contra acessos não autorizados, utilizando técnicas avançadas de segurança.
Auditabilidade	Facilita a verificação e o rastreamento das transações realizadas, contribuindo para maior confiança no sistema.

Fonte: Adaptado de Islam et al., 2020.

2.2.3 Tipos de Blockchains

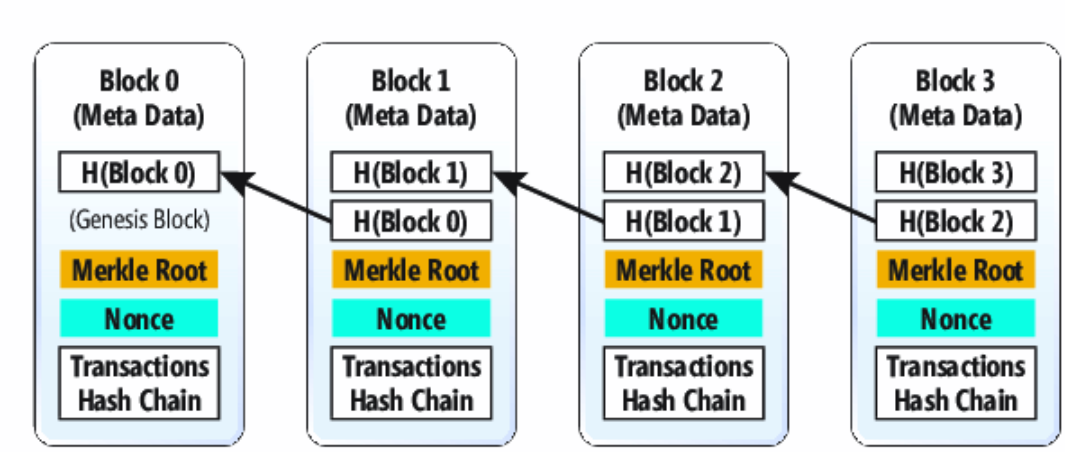
De acordo com (PEGORARO, 2023), os três tipos principais de blockchain são descritos da seguinte forma:

- **Blockchain Pública:** A rede é completamente aberta e qualquer pessoa pode participar, validar transações e acessar o livro-razão. Esse modelo garante total descentralização e transparência, como é o caso do Bitcoin. (PEGORARO, 2023, p. 45).
- **Blockchain Privada:** Somente participantes autorizados podem validar transações e manter o livro-razão. Embora ainda mantenha algumas das características da blockchain, como a imutabilidade, a privacidade e o controle sobre a rede são muito mais fortes. (PEGORARO, 2023, p. 47).
- **Blockchain Híbrida:** Combina elementos das redes públicas e privadas, permitindo que algumas partes da rede sejam abertas enquanto outras permanecem privadas.(PEGORARO, 2023, p. 49).

2.2.4 Componentes Essenciais da Blockchain

A blockchain é composta por vários componentes chave que garantem seu funcionamento. Os principais componentes que definem a estrutura e o funcionamento de uma blockchain são detalhados a seguir:

Figura 6 – Estrutura geral de blocos em Blockchain



Fonte: Microsoft, 2018.

1. **Blocos:** Os blocos são os principais elementos estruturais da blockchain. Cada bloco na blockchain contém dois elementos principais:
   - **Cabeçalho:** Inclui metadados como o timestamp (indicando o momento de criação do bloco), o hash do bloco anterior (para garantir a continuidade da cadeia) e um valor chamado nonce (usado no processo de mineração em blockchains baseadas em Prova de Trabalho).
   - **Corpo:** Contém as transações ou dados registrados, agrupados em um formato específico, como em estruturas Merkle Tree para facilitar a validação e integridade (ZHENG et al., 2018); (BAO et al., 2020).
2. **Hash Criptográfico:** O hash é uma função matemática que transforma os dados do bloco em um valor fixo e único. Ele assegura que qualquer alteração mínima nos dados resultará em um hash completamente diferente, invalidando o bloco e qualquer cadeia subsequente. Esse recurso é essencial para a imutabilidade da blockchain (GIPP; MEUSCHKE; GERNANDT, 2015).
3. **Nós:** Os nós são os dispositivos conectados à rede blockchain. Eles participam ativamente do processo de validação de transações, utilizando regras de consenso para confirmar a validade das transações antes de adicioná-las à blockchain (CHRISTIDIS; DEVETSIKIOTIS, 2016); (CATALINI; GANS, 2020). Cada nó pode ter funções específicas, como:
   - **Nós completos:** Armazenam uma cópia integral de toda a blockchain e participam da validação de transações.
   - **Nós leves:** Mantêm apenas informações essenciais, como o cabeçalho dos blocos, para economizar recursos de armazenamento.

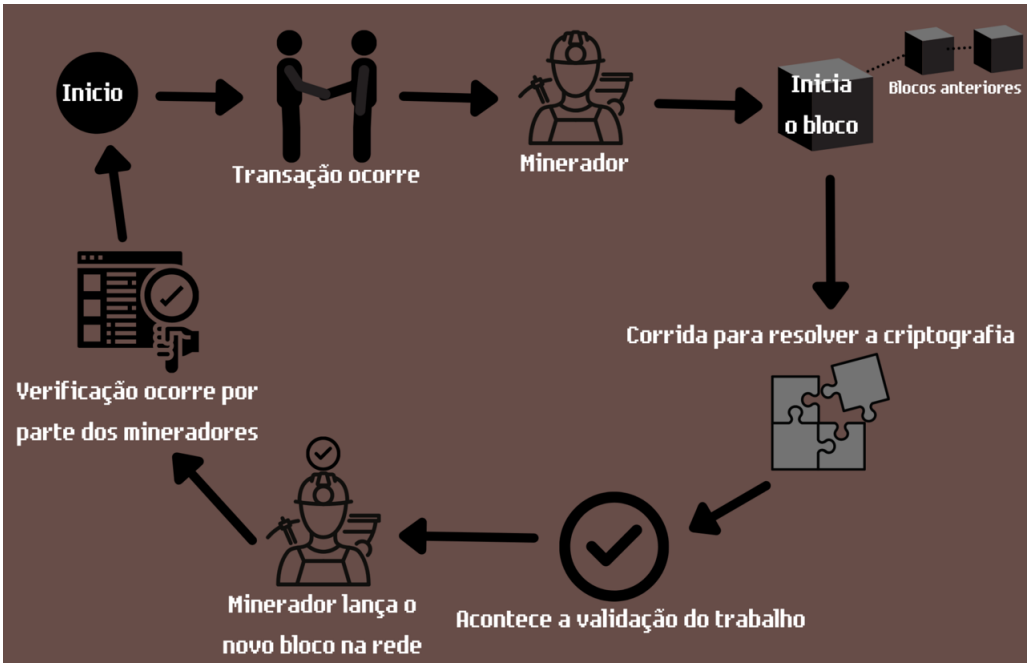
4. **Rede Peer-to-Peer (P2P):**A arquitetura P2P permite a comunicação direta entre os nós, eliminando a necessidade de uma autoridade central. Essa estrutura descentralizada melhora a resiliência da rede e facilita o consenso distribuído para validar transações, como ocorre nos mecanismos de Prova de Trabalho (PoW) e Prova de Participação (PoS) (GAO; NOBUHARA, 2017); (KARAMITSOS et al., 2022). Essa arquitetura permite:

    - **Transmissão de transações:** As transações são propagadas entre os nós até serem confirmadas.
    - **Redundância:** A replicação dos dados por todos os nós aumenta a resiliência contra falhas e ataques.

2.2.5 Processo de Funcionamento

O processo de funcionamento de uma blockchain é estruturado de maneira sequencial e distribuída, a fim de garantir a integridade e a segurança das transações realizadas. Abaixo, detalha-se cada uma das etapas principais que compõem este processo:

Figura 7 – Funcionamento da Blockchain



Fonte: PET UFMS, 2021.

O processo se inicia com a criação de uma transação entre os participantes da rede. Cada transação contém informações relevantes, como o remetente, o destinatário e o valor, que serão posteriormente validadas e registradas no blockchain. A segurança dessas transações é garantida por mecanismos de criptografia, como as assinaturas digitais, que

permitem verificar a autenticidade dos dados e a identidade dos participantes (LUCENA; HENRIQUES, 2016)

Uma vez que os participantes validam o desejo de realizar a transação, ela é transmitida para a rede. Esta transação ainda não é registrada de forma permanente, aguardando a validação. A transmissão ocorre por meio de um sistema descentralizado, em que todos os nós da rede recebem uma cópia da transação para validação (SWAN, 2015).

O minerador, ou validador, é um nó da rede que se responsabiliza por agrupar as transações em um novo bloco. Ele deve validar a transação, verificando sua autenticidade por meio do algoritmo de consenso. O minerador verifica também se os fundos estão disponíveis e se não há tentativas de fraude, como o gasto duplo, e então adiciona a transação ao bloco, que ainda não foi registrado permanentemente na blockchain (CARO, 2017).

A partir do bloco gênese, o primeiro bloco da cadeia, os mineradores começam a formar novos blocos. Cada bloco subsequente contém, além das transações, o hash do bloco anterior, criando uma ligação entre eles. Este encadeamento contínuo de blocos é o que dá origem ao nome "blockchain". O mecanismo de hash assegura que, caso qualquer dado seja alterado, isso alteraria também todos os blocos subsequentes, o que torna qualquer tentativa de modificação facilmente detectável pela rede (KUROSE; ROSS, 2006).

Após a formação do bloco, o minerador deve resolver um problema computacional complexo. Este problema está relacionado ao algoritmo de consenso utilizado pela blockchain. No caso do Proof of Work (PoW), por exemplo, o minerador deve encontrar um valor específico (chamado de nonce) que, quando combinado com os dados do bloco, resulta em um hash que atenda a certos critérios, como ter um número específico de zeros no início. Este processo é altamente intensivo em termos de computação e energia (NAKAMOTO, 2008).

Uma vez que o minerador encontra a solução para o problema computacional e a rede valida seu trabalho, o bloco é adicionado à cadeia. O novo bloco é então propagado para todos os nós na rede, que armazenam uma cópia do blockchain atualizado. Esse processo é crucial para a descentralização, pois assegura que todos os participantes da rede possuam a mesma versão do histórico de transações (SWAN, 2015).

Após o lançamento do novo bloco, outros mineradores e nós da rede verificam a integridade do bloco e das transações nele contidas. Essa verificação é parte do processo de consenso, onde cada minerador valida que a solução do problema computacional está correta e que a transação é válida. Caso algum erro ou fraude seja detectado, o bloco é rejeitado, e o minerador que propôs o bloco incorreto pode ser penalizado. A segurança e a confiança no sistema são mantidas por esse processo rigoroso de validação distribuída (LUCENA; HENRIQUES, 2016).

Este ciclo contínuo garante a integridade da blockchain, tornando-a resistente a fraudes e manipulações, assegurando que o sistema permaneça seguro e eficiente sem a necessidade de uma autoridade central. O uso de algoritmos de consenso, juntamente com técnicas como o hash e as assinaturas digitais, são fundamentais para a operação segura e descentralizada desse sistema (NAKAMOTO, 2008); (CARO, 2017).

2.3 Histórico e Evolução da Blockchain

2.3.1 As primeiras ideias de um sistema de contabilidade distribuída

A ideia de um sistema de contabilidade distribuída tem raízes que precedem a criação do Bitcoin e a blockchain. No final dos anos 1970 e início dos anos 1980, pesquisadores já exploravam conceitos de criptografia e protocolos de comunicação seguros. Essas ideias foram fundamentais para a criação de um sistema onde os participantes pudessem realizar transações de maneira segura e confiável sem depender de uma autoridade central.

Um dos primeiros marcos na evolução desses conceitos foi o trabalho de David Chaum, um criptógrafo pioneiro que introduziu a ideia de dinheiro digital anônimo em 1983 com seu artigo *Blind Signatures for Untraceable Payments* (CHAUM, 1983). Nesse estudo, ele propôs um sistema de transações eletrônicas que preservava a privacidade dos usuários, utilizando uma técnica chamada "assinatura cega". Embora seu trabalho não envolvesse uma blockchain, ele lançou as bases para a criação de sistemas de pagamento eletrônico.

Nos anos seguintes, outros avanços importantes foram feitos. No início dos anos 1990, Stuart Haber e W. Scott Stornetta propuseram um sistema de marcação temporal para documentos digitais, que utilizava uma cadeia de blocos para garantir a integridade e a imutabilidade dos dados (HABER; STORNETTA, 1991). Eles descreveram um método para criar um registro cronológico das transações, onde cada bloco continha um hash criptográfico do bloco anterior. Este trabalho foi um precursor direto do conceito de blockchain.

2.3.2 O estudo de Satoshi Nakamoto

A verdadeira revolução na área de sistemas de contabilidade distribuída veio em 2008, quando um indivíduo ou grupo de indivíduos sob o pseudônimo de Satoshi Nakamoto publicou o artigo intitulado *Bitcoin: A Peer-to-Peer Electronic Cash System* (NAKAMOTO, 2008). Este artigo não apenas introduziu o Bitcoin como a primeira criptomoeda descentralizada, mas também descreveu em detalhes o funcionamento do sistema blockchain que sustenta o Bitcoin.

No artigo, Nakamoto apresentou a blockchain como uma solução para o problema do "gasto duplo"em sistemas de moeda digital. O gasto duplo refere-se ao risco de um ativo digital ser gasto mais de uma vez. Antes do Bitcoin, esse problema era resolvido por intermediários centralizados, como bancos, que verificavam e registravam todas as transações. Nakamoto, no entanto, propôs um sistema descentralizado, onde a rede de participantes validaria as transações coletivamente.

A blockchain, conforme descrita por Nakamoto, é uma cadeia de blocos onde cada bloco contém um conjunto de transações e um hash criptográfico do bloco anterior. Esta estrutura garante que, uma vez que um bloco é adicionado à cadeia, ele não pode ser alterado sem modificar todos os blocos subsequentes, o que exigiria o consenso da maioria da rede. Isso torna a blockchain resistente a fraudes e manipulações.

O artigo de Nakamoto também introduziu o conceito de "prova de trabalho"(Proof of Work), um mecanismo de consenso que exige que os participantes (mineradores) resolvam problemas matemáticos complexos para validar novas transações e adicionar novos blocos à cadeia. Este processo, conhecido como mineração, não só protege a rede contra ataques, mas também controla a emissão de novos bitcoins.

A publicação do artigo de Nakamoto e o subsequente lançamento do software Bitcoin em 2009 marcaram o início de uma nova era na tecnologia financeira e na computação distribuída. O Bitcoin demonstrou que era possível criar um sistema monetário funcional sem a necessidade de intermediários centralizados, utilizando apenas a criptografia e a colaboração entre participantes da rede.

Desde então, a tecnologia blockchain tem sido amplamente explorada e adotada em diversos setores além das criptomoedas, incluindo cadeias de suprimentos, votação eletrônica, contratos inteligentes, e identidade digital. A inovação de Nakamoto inspirou milhares de novos projetos e pesquisas, consolidando a blockchain como uma das inovações tecnológicas mais importantes do século XXI.

2.3.3 Evolução da Blockchain

Com o advento do Bitcoin e sua subsequente popularização, a tecnologia blockchain passou por um desenvolvimento significativo, podendo ser categorizada em diferentes gerações, cada uma marcando uma evolução na aplicação e funcionalidade dessa tecnologia inovadora.

2.3.3.1 Blockchain 1.0 - A Primeira Geração

A primeira geração, conhecida como Blockchain 1.0, foi impulsionada pela descentralização do dinheiro, exemplificada pelo próprio Bitcoin. Este proporcionou um sistema de pagamento digital seguro e sem intermediários, estabelecendo um novo modelo

de transações financeiras (COMERT, 2020). O Bitcoin revolucionou a forma como as transações financeiras eram realizadas, oferecendo um sistema que não dependia de uma autoridade central para validar e registrar transações, garantindo assim maior segurança e transparência.

2.3.3.2 Blockchain 2.0 - A Segunda Geração

A segunda geração, ou Blockchain 2.0, expandiu a aplicação do blockchain para além dos meios de pagamento, permitindo a descentralização de mercados em geral. Esse avanço foi marcado pelo surgimento do Ethereum em 2014, uma plataforma de código aberto criada por Vitalik Buterin. O Ethereum introduziu os contratos inteligentes, que possibilitaram a automação e execução de acordos complexos sem a necessidade de intermediários ((ROCIO, 2022) apud (SWAN, 2015)) . Os contratos inteligentes são programas que automaticamente executam e verificam termos contratuais, proporcionando eficiência e reduzindo custos operacionais em diversas indústrias.

2.3.3.3 Blockchain 3.0 - A Terceira Geração

A terceira geração, referida por alguns estudiosos como Blockchain 3.0, foca na utilização do blockchain em pesquisas e projetos governamentais, visando a aplicação da tecnologia em setores mais amplos e regulamentados((ROCIO, 2022) apud (LEVIS; FONTANA; UGHETTO, 2021)). Esta fase busca integrar a tecnologia blockchain em infraestruturas públicas e governamentais, promovendo maior transparência, segurança e eficiência nos serviços públicos. Exemplos incluem o registro de identidades, a votação eletrônica e a gestão de cadeias de suprimentos.

2.3.3.4 Integração das Gerações

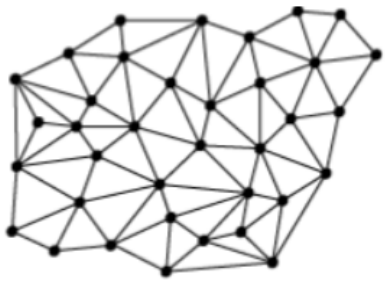
Há uma perspectiva alternativa que sugere a consolidação das gerações 2.0 e 3.0 em uma única fase de desenvolvimento, dada a sobreposição de suas funcionalidades e objetivos. Essa visão unificada destaca o Ethereum como um marco significativo na evolução do blockchain, transformando-o em uma plataforma versátil para aplicações descentralizadas em diversos setores (FIGUEIREDO et al., 2021); (MOUGAYAR, 2016). Independentemente da classificação, é inegável que o blockchain continua a evoluir e a impactar profundamente vários aspectos da sociedade e da economia global.

2.4 Arquitetura e Princípios Básicos

A arquitetura da Blockchain é uma solução que responde a desafios específicos das redes distribuídas. Diferentemente das redes centralizadas, em que um servidor central gerencia todas as transações, a rede Blockchain permite a comunicação direta entre os

nós (computadores) de uma rede ponto a ponto (P2P), facilitando o compartilhamento eficiente de dados e serviços (MURTHY et al., 2020). Esse modelo descentralizado elimina a necessidade de intermediários, o que não só aprimora a eficiência como também reduz o risco de falhas centralizadas e aumenta a segurança das transações realizadas dentro da rede.

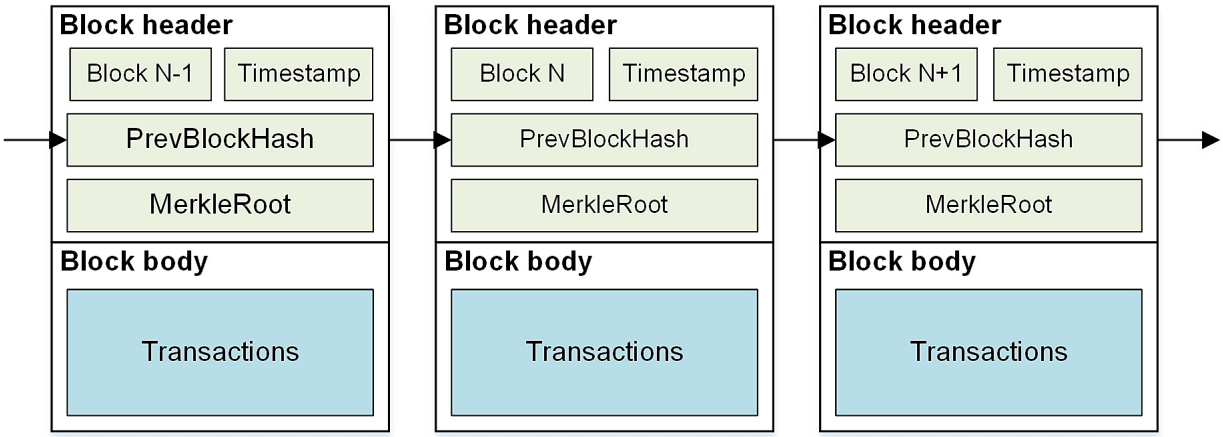
Figura 8 – Arquitetura distribuída de uma rede Blockchain



Fonte: Adaptado de PITZ, 2017.

Outro aspecto essencial da arquitetura da Blockchain é sua estrutura de lista encadeada, na qual cada novo bloco contém um ponteiro para o bloco anterior (CROSBY et al., 2016). Esse ponteiro é implementado por meio de um hash, garantindo a integridade e a imutabilidade da cadeia. Como resultado, cada bloco depende diretamente do anterior, formando uma cadeia contínua que cresce com a mineração de novos blocos. Essa interdependência é o que torna a Blockchain segura e confiável, pois a alteração de qualquer bloco anterior invalidaria toda a cadeia subsequente, tornando-a praticamente impossível de ser manipulada sem ser detectada.

Figura 9 – Encadeamento de blocos de uma Blockchain



Fonte: Nicehash, 2023.

A estrutura básica de uma Blockchain, como mostra a figura acima, é composta por blocos encadeados, onde cada bloco contém um cabeçalho e um corpo. O cabeçalho inclui

elementos cruciais, como a versão do protocolo, o Merkle Root (um valor de hash que representa o bloco atual) e o nonce, que é utilizado no processo de algoritmo de consenso para garantir que os blocos sejam adicionados de maneira segura e em conformidade com os requisitos de consenso da rede (WANG et al., 2019). Além disso, o campo de dificuldade é ajustado periodicamente para refletir o poder computacional da rede, mantendo o tempo de geração de blocos constante, independentemente do crescimento da capacidade de processamento dos participantes ((WANG et al., 2019). Este processo de validação e criação de blocos permite que a Blockchain seja segura, imutável e resistente a ataques.

2.5 Segurança e Mecanismos de Consenso

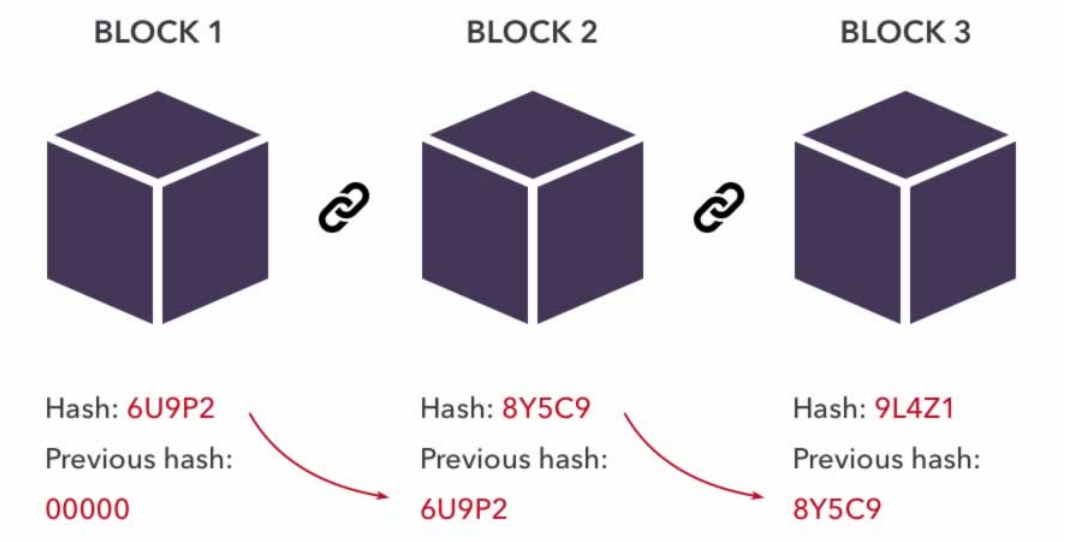
A segurança e os algoritmos de consenso são pilares essenciais para o funcionamento das redes Blockchain. A segurança é garantida principalmente pelo uso de técnicas criptográficas, como funções de hash e assinaturas digitais, que asseguram a integridade e autenticidade das transações (WANG et al., 2019). Além disso, o modelo descentralizado da Blockchain elimina a necessidade de um ponto único de falha, tornando a rede mais resistente a ataques.

2.5.1 Funções hash

As funções de hash, como SHA-256, transformam uma entrada de dados de tamanho variável em uma saída de tamanho fixo (de 256 bits), que é única para cada entrada. Esta característica permite que qualquer alteração nos dados de um bloco, por exemplo, resulte em uma mudança no hash, o que torna impossível modificar os dados sem ser detectado (WANG et al., 2019).

Durante o processo de mineração, os mineradores buscam um valor chamado nonce, que, quando combinado com os dados do bloco e indicado ao algoritmo SHA-256, deve resultar em um hash que atenda aos critérios estabelecidos pela rede (SILVA, 2024). Para que um bloco seja considerado válido, seu hash deve ser inferior a um valor determinado pelo sistema de dificuldade. A exigência de dificuldade exige que o hash gerado comece com um número específico de zeros, e esse padrão varia de acordo com a capacidade computacional da rede (BRUCE, 2023). Esse ajuste garante que novos blocos sejam minerados aproximadamente a cada dez minutos, regulando a emissão do Bitcoin e fortalecendo a segurança da blockchain contra manipulações maliciosas.

Figura 10 – Funções hashl



Fonte: PET Produção UFC, 2021.

Isso proporciona a imutabilidade da Blockchain, pois qualquer tentativa de manipulação de um bloco afetaria todos os blocos subsequentes, invalidando toda a cadeia. A função de hash garante a integridade da Blockchain, pois cada bloco contém o hash do bloco anterior. Caso um bloco seja alterado, seu hash muda, o que, por sua vez, altera o hash de todos os blocos subsequentes, tornando a manipulação detectável. Além disso, a função de hash é utilizada para garantir a eficiência no processo de verificação de transações em redes distribuídas, facilitando a validação sem a necessidade de um servidor central(TSCHORSCH; SCHEUERMANN, 2016).

A dificuldade de incluir novos blocos na rede Bitcoin é controlada pelo mecanismo de ajuste de dificuldade , que garante que um novo bloco seja minerado, em média, a cada 10 minutos. Esse ajuste é feito a cada bloco mineral de 2016, ou que ocorre aproximadamente a cada duas semanas. A principal variável para ajustar essa dificuldade é o tempo necessário para minerar os blocos anteriores (ZHU, 2023).

A mineração no Bitcoin funciona por meio da tentativa de encontrar um hash, que é um valor resultante de uma função criptográfica (SHA-256), que atende a uma condição específica de dificuldade. Essa condição envolve uma quantidade de zeros à frente do hash, o que significa que, para que o hash de um bloco seja válido, ele precisa ser menor que um valor alvo definido pela rede. Esse valor alvo é o que determina a dificuldade da (GOUVEIA, 2021).

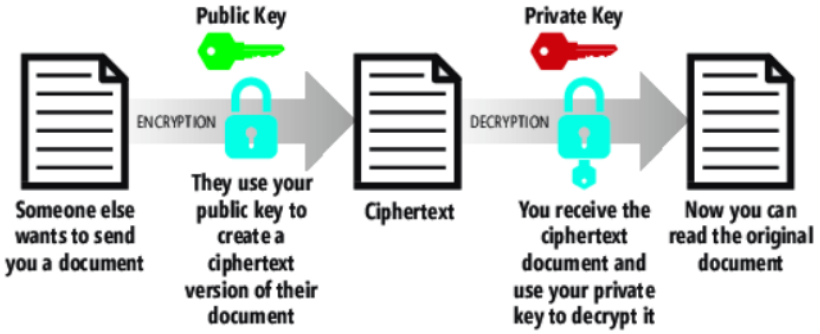
Quando mais mineradores entram na rede ou há um aumento no poder de computação disponível (hashrate), os blocos podem ser minerados mais rapidamente, o que faz com que a dificuldade seja ajustada para um nível mais alto, exigindo que o hash tenha mais zeros à frente. Por outro lado, se a mineração for muito lenta, a dificuldade será

reduzida, tornando mais fácil encontrar o hash válido (CHICARINO et al., 2017).

2.5.2 Assinaturas digitais

Já as assinaturas digitais são usadas para autenticar a identidade do remetente e garantir a integridade dos dados em uma transação. Elas funcionam através de criptografia assimétrica, onde uma chave privada é usada para gerar a assinatura e a chave pública correspondente permite verificar a autenticidade da assinatura. Essa combinação de chaves é fundamental para garantir que as transações sejam realizadas de forma segura e sem a necessidade de confiar em uma terceira parte (CONOSCENTI; VETRO; MARTIN, 2016). Na rede Blockchain, as assinaturas digitais são usadas para validar as transações, assegurando que apenas o proprietário da chave privada possa autorizar a movimentação dos ativos. Isso contribui para a confiança e segurança na rede, permitindo que as partes envolvidas na transação verifiquem a autoria e a integridade dos dados sem a intervenção de uma autoridade central (MURTHY et al., 2020).

Figura 11 – Assinatura digital



Fonte: Microsoft, 2018.

2.5.3 Algoritmos de consenso

Os algoritmos - ou mecanismos - de consenso são fundamentais para o funcionamento das redes Blockchain, pois permitem que todos os nós da rede cheguem a um acordo sobre o estado atual do livro razão (ledger), sem a necessidade de uma autoridade central. Em uma rede descentralizada, cada participante tem uma cópia do ledger e, para garantir que todos possuam dados consistentes e precisos, é necessário um processo que valide as transações e as adicione à Blockchain de forma confiável. Isso é feito através de algoritmos de consenso, que asseguram que todos os nós concordem sobre a validade das transações e a ordem em que elas devem ser registradas, promovendo a confiança entre os participantes sem a intermediação de um ente centralizado (MURTHY et al., 2020).

Existem diversos tipos de mecanismos de consenso utilizados em diferentes implementações de Blockchain, sendo os mais comuns descritos na tabela abaixo:

Tabela 3 – Algoritmos de Consenso na Blockchain

Algoritmo	**Descrição**
Proof of Work (PoW)	Exigido no Bitcoin, onde mineradores resolvem problemas computacionais complexos antes de adicionar blocos à blockchain, garantindo a segurança e imutabilidade dos dados registrados. (NAKAMOTO, 2008)
Proof of Stake (PoS)	Substitui o trabalho computacional por um processo de seleção de validadores baseado na quantidade de criptomoeda que os participantes possuem, sendo mais eficiente em termos de consumo energético. Adotado em redes como o Ethereum 2.0. (BUTERIN, 2014)
Delegated Proof of Stake (DPoS)	Permite que os participantes escolham representantes para validar blocos, aumentando a velocidade de validação das transações. (LARIMER, 2014)
Practical Byzantine Fault Tolerance (PBFT)	Foca na resistência a falhas e na rapidez na validação das transações, sendo eficaz para redes que exigem alta confiabilidade, especialmente em blockchains empresariais. (CASTRO; LISKOV, 2002)

Fonte: Autor, 2024.

Esses - e outros - mecanismos de consenso são essenciais para assegurar a integridade, segurança e a transparência das transações, sem a necessidade de confiar em uma terceira parte ou autoridade centralizada. Eles garantem que a rede opere de maneira descentralizada e imutável, reforçando as vantagens da Blockchain sobre sistemas tradicionais.

2.5.4 Validação dos nós da Blockchain

Os validadores são responsáveis por verificar a modificação das transações e dos blocos antes de aceitá-los na blockchain (DOURADO, 2020). Eles operam de acordo com um conjunto de regras definido pelo protocolo do Bitcoin, garantindo que todas as transações estejam em conformidade com os princípios da rede (MARTINS et al., 2021). A principal função desses nós é garantir que os blocos suplementares contenham apenas transações válidas e que não haja possibilidade de gastos duplos. A descentralização fornecida por eles impede que entidades individuais manipulem unilateralmente os registros da blockchain, consolidando a segurança do sistema (DAUMAS, 2023).

2.5.5 Ciclo de Halving

O halving é um evento programado que reduz pela metade as recompensas dos mineradores a cada 210.000 blocos minerados, aproximadamente a cada quatro anos. Esse evento reflete a escassez programada do Bitcoin, com um limite máximo de 21 milhões de unidades em circulação, diferenciando radicalmente das moedas fiduciárias que podem ser emitidas sem limites por bancos centrais (SALTIÉL, 2024).

Figura 12 – Representação do ciclo de Halving

Ano	Recompensas por bloco	Bitcoin minerado por dia
2009-2012	50 BTC	7200 BTC
2012-2016	25 BTC	3600 BTC
2016-2020	12,5 BTC	1800 BTC
2020-2024	6,25 BTC	900 BTC
2024-2028	3,125 BTC	450 BTC
2028-2032	1,5625 BTC	225 BTC
...	...	...
2140	0	0

Fonte: Coinext, 2024

Desde o início, a recompensa do bloco minerado era de 50 BTC. Após sucessivos halvings, em 2024 uma recompensa será de 3.125 BTC, com o último Bitcoin estimado para ser minerado em 2140. Esse modelo de escassez reforça o Bitcoin como uma reserva de valor, influenciando sua valorização e estabilidade no mercado financeiro global (PEREIRA, 2025).

O halving tem implicações diretas na oferta de novos Bitcoins no mercado. Como a recompensa é reduzida, o ritmo de criação de novos Bitcoins diminui, o que leva a uma escassez relativa de novos Bitcoins. Isso cria uma pressão de demanda, o que tende a aumentar o valor do Bitcoin ao longo do tempo, especialmente se a adoção crescer (KUHN et al., 2022).

Outro aspecto de limitação está na capacidade de processamento da rede. O Bitcoin é limitado a um bloco a cada 10 minutos, e a cada bloco, é possível incluir apenas um número limitado de transações (GREVE et al., 2018). Isso resulta em escalabilidade limitada, o que significa que, em momentos de alta demanda, as taxas de transação aumentam, e o tempo de confirmação das transações pode demorar mais. Esse é um dos desafios que a comunidade do Bitcoin está tentando resolver com soluções como a Lightning Network, que busca melhorar a escalabilidade sem comprometer a segurança e a descentralização(TRASFERETTI; MENTOR; PINESCHI, 2024).

Dessa forma, o Bitcoin é forte devido à sua escassez, segurança e descentralização, mas também é limitado pelo fornecido finito e pelas restrições de capacidade de transações da rede, o que reflete a visão de Satoshi Nakamoto de criar uma moeda que fosse segura e imune à inflação, mas com um protocolo finito e estruturado.

2.6 Cibersegurança em Blockchain

A implementação das tecnologias de Blockchain têm gerado impactos positivos em alguns setores, consolidando essa tecnologia como uma ferramenta essencial para a proteção de dados em um mundo cada vez mais digital. A descentralização é um dos fatores

mais marcantes nesse contexto, eliminando a dependência de servidores centralizados, que frequentemente representam um ponto único de falha e alvo atrativo para cibercriminosos. Com os dados distribuídos entre diversos nós na rede, a Blockchain aumenta a resiliência das infraestruturas digitais, dificultando ataques coordenados que busquem interromper ou comprometer sistemas. Essas características demonstram como a Blockchain está redefinindo as estratégias de proteção digital, contribuindo para a criação de ambientes mais seguros e confiáveis.

2.6.0.1 Impactos dos Ataques Cibernéticos em Blockchain

A cibersegurança é uma área essencial para garantir a integridade, a confidencialidade e a disponibilidade dos dados nas redes descentralizadas. No entanto, é importante entender que, embora a Blockchain proporcione uma estrutura para proteger transações e dados, ela não deve ser vista como a única solução para os desafios de segurança em um sistema digital mais amplo. A Blockchain, com seus mecanismos de criptografia, algoritmos de consenso e descentralização, proporciona segurança intrínseca, mas essa segurança é focada em aspectos específicos, como a validação de transações e a imutabilidade dos registros (MURTHY et al., 2020).

Para proteger uma infraestrutura digital de forma eficaz, é necessário adotar uma abordagem de segurança em várias camadas, que envolva tanto as soluções oferecidas pela Blockchain quanto outras medidas tradicionais e emergentes de cibersegurança. Por exemplo, em redes Blockchain, a criptografia (como as funções de hash e as assinaturas digitais) e os mecanismos de consenso (como o Proof of Work e o Proof of Stake) desempenham um papel central na proteção contra fraudes e ataques. No entanto, esses mecanismos se concentram principalmente na segurança das transações e na integridade dos dados dentro da rede. Eles não abordam questões de segurança mais amplas, como ataques a dispositivos finais, falhas de configuração de rede, ou vulnerabilidades na camada de aplicações (WANG et al., 2019).

Uma solução abrangente de cibersegurança deve incluir não apenas os mecanismos fornecidos pela Blockchain, mas também outras práticas de segurança complementares. Isso envolve o uso de firewalls, sistemas de detecção de intrusões (IDS), e a autenticação multifatorial, que ajudam a proteger contra ataques direcionados a sistemas externos ou a infraestrutura que suporta a Blockchain. A implementação de políticas rigorosas de controle de acesso e auditoria também é necessária para prevenir brechas de segurança e garantir a proteção contra ameaças internas (CROSBY et al., 2016).

A cibersegurança em Blockchain deve, portanto, ser encarada como uma parte de um ecossistema de segurança digital mais amplo. Para que as redes Blockchain sejam verdadeiramente seguras, é necessário considerar não apenas a proteção das transações, mas também a proteção da infraestrutura subjacente, das interfaces de usuário, e das redes

que sustentam os sistemas Blockchain. Isso implica na implementação de medidas contínuas de monitoramento, auditoria e atualização dos sistemas de segurança, além de incentivar a inovação em novas tecnologias de segurança, como o uso de inteligência artificial para detectar padrões de comportamento anômalos e ataques sofisticados (CONOSCENTI; VETRO; MARTIN, 2016).

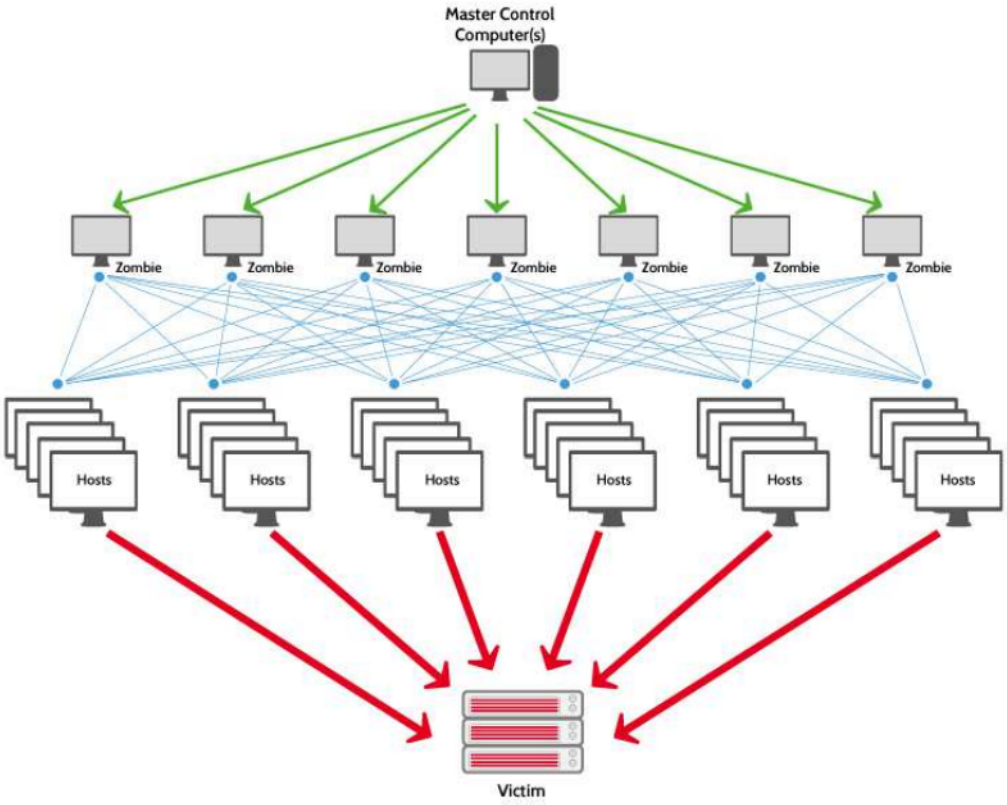
Portanto, enquanto a Blockchain oferece fortes garantias de segurança para transações descentralizadas, ela precisa ser complementada por outras camadas de segurança para proteger a infraestrutura digital como um todo, criando um sistema resiliente capaz de enfrentar as ameaças emergentes em um ambiente de cibersegurança em constante evolução.

2.7 Ataques DDoS: Visão Geral e Classificação

2.7.1 Definição de Ataques DDoS

Os ataques de Negação de Serviço Distribuída (DoS - Denial-of-Service) representam uma das formas mais sofisticadas e devastadoras de ataque cibernético, tendo como objetivo interromper ou degradar significativamente o funcionamento de servidores, serviços ou redes de comunicação, tornando-os inacessíveis ou extremamente lentos (HOQUE; BHATTACHARYYA; KALITA, 2015). A principal característica que distingue os ataques DDoS de outros tipos de ataques de negação de serviço (DoS) é a utilização de múltiplas fontes de tráfego malicioso, o que torna esse tipo de ataque particularmente complexo e difícil de mitigar (CERIBELLI, 2020).

Figura 13 – Esquema de Ataques de negação de serviço

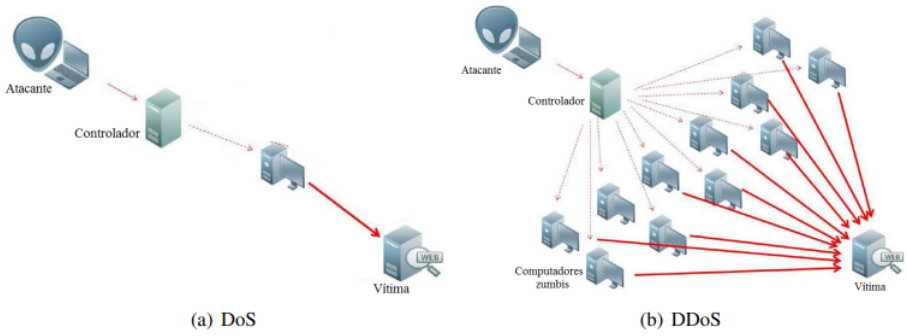


Fonte: (UFMS, 2018)

Em um ataque DDoS, a origem do tráfego é distribuída por múltiplos dispositivos comprometidos, que podem incluir computadores, dispositivos móveis e até servidores inteiros infectados com software malicioso, formando uma botnet (CARVALHO, 2018). Esse tráfego distribuído dificulta a identificação e o bloqueio do ataque, uma vez que ele simula requisições legítimas provenientes de uma variedade de fontes, o que torna mais difícil para as soluções de segurança distinguirem o tráfego malicioso do tráfego regular (SILVEIRA, 2020).

Conceitualmente, o ataque de DoS pode acontecer de duas formas: quando apenas um atacante está provocando a indisponibilidade ou quando o ataque é realizado de forma distribuída, originada de vários lugares, sendo assim, um ataque de DDoS (Distributed Denial-of-Service).

Figura 14 – Ataques de negação de serviço: individualizados e distribuídos



Fonte: (HELPSEC, 2016)

A Figura acima ilustra a execução de um ataque DoS e DDoS. Em ambas as representações, o atacante é o usuário malicioso responsável por provocar a indisponibilidade do serviço. Também está presente o controlador, que hospeda o serviço de comunicação e de onde são emitidas as instruções para o ataque. No lado "a", o controlador se comunica com uma única máquina, que executa o ataque diretamente. Já na lado "b", o controlador interage com múltiplos computadores zumbis, que são dispositivos previamente infectados e que seguem os comandos do atacante. Por fim, em ambas as figuras, a vítima é representada por um servidor web.

Atualmente, o ataque DDoS é amplamente utilizado devido à sua capacidade de causar indisponibilidade de forma mais rápida e eficiente, sem exigir grandes quantidades de recursos computacionais. Isso ocorre porque o ataque se vale de máquinas de terceiros, frequentemente infectadas por malware, para executar o ataque (MORAES, 2023). Em comparação aos dois tipos de ataques, (ALMEIDA, 2013) observa que o poder do DDoS é significativamente superior ao do DoS, principalmente por dois motivos: a dificuldade maior que os sistemas de detecção enfrentam para identificar a origem do ataque e o volume de pacotes gerados por um ataque DDoS. Assim, no contexto desta pesquisa, os ataques de negação de serviço serão abordados em sua modalidade distribuída, ou seja, o DDoS.

2.7.2 Classificação dos Ataques DDoS

Existem diferentes tipos de ataques DDoS, que variam conforme a camada de atuação ou o protocolo utilizado. De acordo com (BHOSALE; NENOVA; ILIEV, 2017), esses ataques podem ser classificados em três categorias principais: ataques baseados em volume, ataques baseados em protocolos e ataques na camada de aplicação. Cada uma dessas categorias representa uma abordagem distinta de como o tráfego malicioso é gerado e como ele afeta os sistemas-alvo. Na sequência, será descrito um pouco mais detalhadamente cada um desses tipos de ataques, abordando suas características, mecanismos de execução

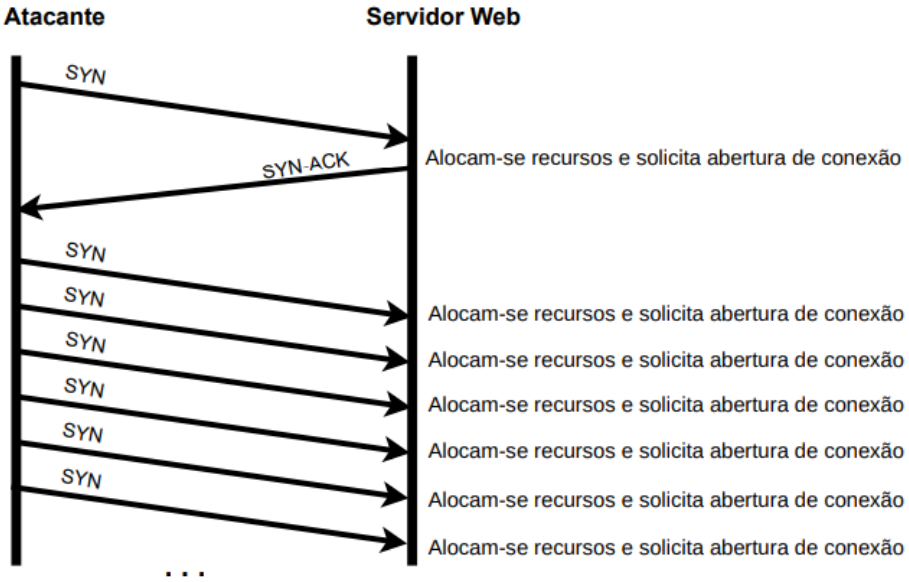
e impactos, a fim de fornecer uma compreensão abrangente sobre o funcionamento dos ataques DDoS.

2.7.2.1 Ataques Baseados em Volume

Ataques DDoS baseados em volume têm como característica principal a geração de uma quantidade massiva de tráfego direcionado ao alvo, resultando em uma "inundação"de pacotes (VASCONCELOS, 2022). O objetivo central desses ataques é sobrecarregar a infraestrutura de rede e os recursos computacionais do alvo, como largura de banda, capacidade de processamento e memória, impedindo que o servidor ou serviço seja capaz de processar requisições legítimas (JUNIOR, 2023). Ao esgotar esses recursos, o sistema-alvo se torna incapaz de atender aos usuários legítimos, levando à indisponibilidade do serviço. A sobrecarga de pacotes pode resultar em degradação do desempenho, lentidão extrema ou até mesmo falhas críticas no sistema (RIBEIRO, 2022).

Esses ataques são caracterizados pela quantidade excessiva de tráfego que é gerada de forma contínua, sem a necessidade de interação significativa com o serviço de destino. Eles visam, essencialmente, esgotar os recursos de rede do alvo, geralmente não tentando invadir ou comprometer dados, mas simplesmente tornar o serviço inacessível pela saturação de sua capacidade de tráfego (FRANÇA, 2020).

Figura 15 – Esquema de ataque DDoS baseado em volume



Fonte: (Adaptado de Imperva, 2019)

O ataque é geralmente realizado por meio de ferramentas automatizadas ou botnets, que são redes de dispositivos infectados e controlados remotamente. Esses dispositivos, muitas vezes comprometidos sem o conhecimento de seus donos, enviam pacotes de dados em massa para o alvo. A natureza distribuída do ataque dificulta a identificação e a

mitigação, uma vez que o tráfego provém de múltiplas fontes simultaneamente (COSTA; PORTELA; LOPES, 2021).

2.7.2.2 Ataques Baseados em Protocolos

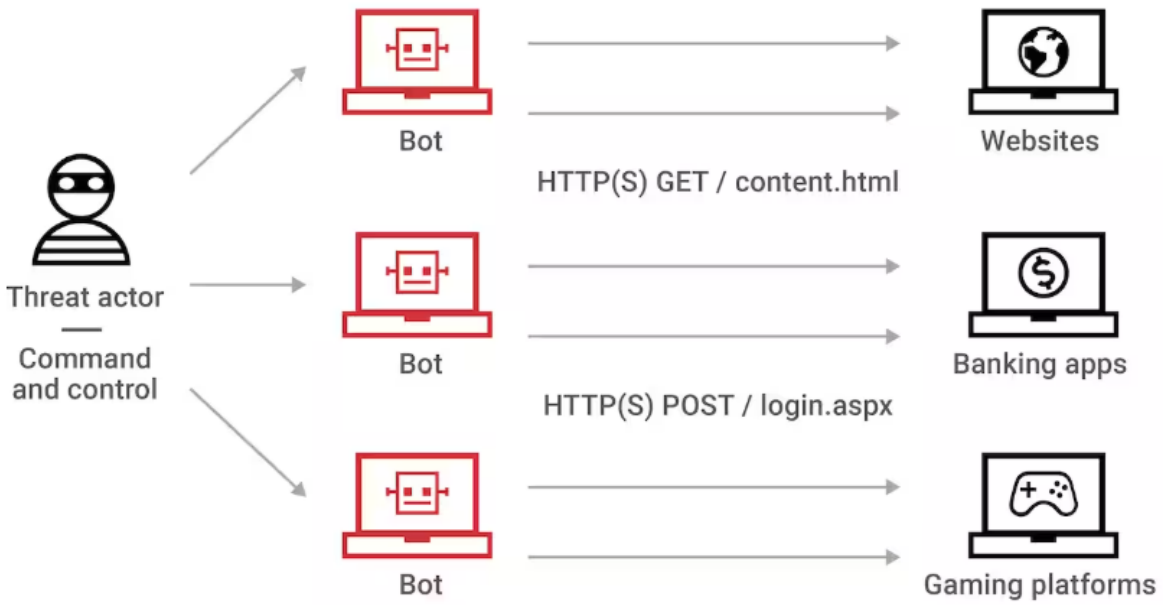
Os ataques baseados em protocolo são um tipo de ataque DDoS que exploram vulnerabilidades específicas nos protocolos da rede, geralmente nas camadas inferiores do modelo OSI (Open System Interconnection), como a camada de rede e a camada de transporte (TANEMBAUM, 2003). Esses ataques visam afetar diretamente o funcionamento de protocolos fundamentais para a comunicação de rede, como TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e ICMP (Internet Control Message Protocol), entre outros (MIRKOVIC; REIHER, 2004). O principal objetivo desses ataques é explorar falhas de implementação ou sobrecarregar os recursos de rede e servidores, dificultando a comunicação e comprometendo a disponibilidade dos serviços (WANG et al., 2019).

Os ataques baseados em protocolo afetam as camadas de rede e transporte de forma a comprometer a capacidade de comunicação e processamento de pacotes dentro da rede (COSTA; PORTELA; LOPES, 2021). Eles não apenas causam sobrecarga nas redes e servidores, mas também podem explorar falhas nas implementações desses protocolos para gerar impactos mais profundos, como corrupção de dados e falhas de segurança (MIRKOVIC; REIHER, 2004). A consequência imediata é a indisponibilidade dos serviços e a degradação do desempenho da rede, o que pode afetar diretamente a experiência do usuário e causar danos financeiros e reputacionais às organizações vítimas desses ataques.

2.7.2.3 Ataques na Camada de Aplicação

Os ataques de negação de serviço distribuída (DDoS) que visam explorar vulnerabilidades na camada de aplicação do modelo OSI (Open Systems Interconnection) (TANEMBAUM, 2003) e são conhecidos por sua capacidade de causar danos significativos com o uso de recursos limitados (MOURA, 2023). Esses ataques são direcionados especificamente a falhas ou fraquezas presentes nos protocolos de comunicação da camada de aplicação, como HTTP, DNS, e SMTP, bem como nas próprias aplicações que operam sobre essas camadas. Ao contrário dos ataques que se concentram em sobrecarregar a rede ou o servidor com grandes volumes de tráfego, os ataques de aplicação buscam explorar essas vulnerabilidades para esgotar os recursos do sistema alvo de maneira mais sutil e eficiente (CERIBELLI, 2020).

Figura 16 – Esquema de ataque DDoS na camada de aplicação



Fonte: (Akami, 2022)

A característica desse tipo de ataque é a necessidade reduzida de recursos para causar uma grande interrupção nos serviços. Em vez de simplesmente inundar a rede com pacotes, como nos ataques baseados em volume, os ataques na camada de aplicação buscam consumir recursos de processamento e memória do servidor de maneira mais estratégica. Isso é feito geralmente por meio de requisições aparentemente legítimas, que, quando repetidas em grande quantidade ou de forma maliciosa, podem saturar os recursos da aplicação e tornar o serviço inacessível (MIRKOVIC; REIHER, 2004); (PRASEED; THILAGAM, 2018); (TRIPATHI; HUBBALLI, 2021).

Os ataques DDoS na camada de aplicação são extremamente eficazes em termos de recursos, pois podem causar grandes impactos no desempenho do servidor com uma quantidade relativamente pequena de tráfego (TRIPATHI; HUBBALLI, 2021); (PRASEED; THILAGAM, 2018). O impacto principal desses ataques é a indisponibilidade do serviço, uma vez que os recursos do servidor, como memória, capacidade de processamento e conexões simultâneas, são consumidos excessivamente por requisições aparentemente legítimas (WANG et al., 2019). Isso pode resultar em interrupções prolongadas, prejudicando a experiência do usuário e causando danos à reputação do serviço. Além disso, devido à sua natureza, os ataques de camada de aplicação são mais difíceis de detectar e mitigar, exigindo soluções especializadas e monitoramento contínuo para identificar padrões de tráfego anormais (ZADE; PATIL, 2011); (ZARGAR; JOSHI; TIPPER, 2013).

2.8 Considerações finais sobre o capítulo

Neste capítulo, foram apresentados os principais fundamentos da tecnologia Blockchain, desde seus conceitos e componentes essenciais até sua evolução histórica e princípios arquiteturais. Além disso, discutiu-se a importância da cibersegurança nesse contexto, analisando os impactos dos ataques cibernéticos e, em particular, a ameaça representada pelos ataques DDoS.

Compreender esses aspectos é essencial para o desenvolvimento e aprimoramento de soluções baseadas em Blockchain, garantindo sua segurança, escalabilidade e eficiência. A análise dos riscos e desafios enfrentados pela tecnologia reforça a necessidade de estratégias robustas de defesa e mitigação, que permitam explorar todo o potencial da Blockchain sem comprometer sua integridade e confiabilidade.

3 Trabalhos Correlatos

3.1 Considerações iniciais sobre o capítulo

Este capítulo oferece uma revisão dos principais estudos e avanços relacionados à simulação de ataques DDoS em redes Blockchain externas, no contexto da cibersegurança. O desenvolvimento do capítulo remonta aos primeiros esforços para entender e neutralizar ataques de negação de serviço distribuídos, que se tornaram uma preocupação crescente à medida que a internet e as tecnologias de redes se expandiram. Inicialmente, os estudos focaram em técnicas tradicionais de mitigação, mas, com o tempo, a introdução da tecnologia Blockchain trouxe novas perspectivas para a proteção contra esses ataques, graças à sua natureza descentralizada e resiliente. Ao longo dos anos, a pesquisa evoluiu, explorando diversas abordagens para melhorar a robustez das redes Blockchain frente a cenários adversos.

Para a procura e seleção dos artigos utilizados nesta revisão, foi empregada a inteligência artificial ResearchRabbit, que auxiliou na organização das referências mais relevantes para o tema. Dessa forma, este capítulo discutirá as principais pesquisas utilizadas estudar os ataques DDoS em sistemas Blockchain, com o intuito de fornecer uma base teórica sólida para contextualizar o estudo atual e identificar potenciais lacunas na literatura que podem ser abordadas em futuras investigações.

3.2 Levantamento do estado da arte

Para dar início ao levantamento bibliográfico deste trabalho, foi realizada uma pesquisa no Google Acadêmico. O Google Acadêmico é uma ferramenta de busca gratuita que indexa a literatura acadêmica, proporcionando acesso global, atualizado e de alta qualidade à produção científica. A plataforma cobre todas as áreas do conhecimento e disponibiliza uma vasta gama de recursos, incluindo artigos científicos, teses, livros, patentes e trabalhos de conferências, tornando-se um recurso essencial para estudantes, professores, pesquisadores e técnicos.

A pesquisa foi realizada utilizando as seguintes palavras-chave:

("DDoS attack simulation" *OR* **"Distributed Denial of Service"** *OR* ***"DDoS mitigation"***) *AND* (**"Blockchain"** *OR* **"Blockchain networks"**) *AND* (**"Cybersecurity"** *OR* **"network security"**) *AND* (**"resilience"** *OR* **"system resilience"**).

Essas palavras-chave foram selecionadas para garantir que os resultados fossem abrangentes e relevantes, cobrindo os principais tópicos relacionados à simulação de

ataques DDoS, estratégias de mitigação e resiliência em redes Blockchain no contexto de cibersegurança.

Para garantir a seleção dos artigos mais relevantes, utilizou-se a ferramenta Parsifal para a triagem e análise dos artigos. Parsifal é uma ferramenta online que facilita o processo de revisão sistemática, permitindo a identificação, seleção e extração de dados de estudos relevantes de maneira eficiente e estruturada. Esta ferramenta é amplamente utilizada para garantir a transparência e a reprodutibilidade das revisões sistemáticas, assegurando que os estudos incluídos sejam rigorosamente avaliados e selecionados com base em critérios previamente definidos.

A busca retornou 47 trabalhos publicados do repositório.

A revisão sistemática foi então representada, baseando-se nos seguintes critérios de inclusão:

- Estudos em inglês;
- A partir de 2019;
- Tratavam sobre Blockchain e ataque DDoS.

Para exclusão:

- Estudos duplicados;
- Muito obsoletos;
- Artigos incompletos;
- Estudos fora do escopo da pesquisa;
- Publicações de baixa qualidade (ex.: conferências de menor relevância ou revistas sem revisão por pares).

Após essa seleção inicial, a ferramenta ResearchRabbit foi empregada para organizar os estudos de forma cronológica, permitindo uma melhor compreensão da evolução da área e facilitando a identificação de tendências e lacunas ao longo do tempo. Para um melhor detalhamento individual dos trabalhos correlatos, foram selecionados cinco estudos que apresentam similaridade com a temática da pesquisa e a metodologia desenvolvida.

A pesquisa feita por (WANI et al., 2021))aborda o problema do Ataque de Negação de Serviço Distribuído (DDoS), que representa uma grande ameaça ao impedir o serviço de solicitações legítimas em redes. O estudo aponta que estimativas indicam que esses ataques irão dobrar, alcançando mais de 15 milhões nos próximos dois anos e, embora vários

esquemas de mitigação tenham sido desenvolvidos desde então, a crescente complexidade dos ataques exige soluções mais avançadas baseadas em tecnologias emergentes.

O blockchain tem se destacado como uma tecnologia promissora e viável para a mitigação de DDoS.Este estudo explora diferentes abordagens para a mitigação de DDoS utilizando blockchain em diversos domínios. O objetivo do artigo é fornecer uma revisão abrangente, destacando detalhes essenciais, pontos fortes, desafios e limitações de diferentes métodos. Além disso, pretende-se que esta pesquisa sirva como uma plataforma única para entender a mecânica das abordagens atuais, visando aprimorar a pesquisa e o desenvolvimento no campo da mitigação de DDoS.

O estudo desenvolvido por (SHAH et al., 2022) aborda a utilização de dispositivos de Internet das Coisas (IoT) em diversos setores, como cidades inteligentes, agricultura inteligente, medicina inteligente e logística inteligente. No entanto, ataques de Negação de Serviço Distribuída (DDoS) representam uma séria ameaça à segurança da IoT, pois invasores podem explorar facilmente as vulnerabilidades desses dispositivos e controlá-los como parte de botnets para lançar ataques DDoS, devido às suas limitações em memória e recursos de computação. Esta pesquisa realiza uma análise de algumas soluções baseadas em Blockchain para mitigar ataques DDoS na IoT. Primeiramente, discute-se como as redes de IoT são vulneráveis a ataques DDoS, seu impacto sobre as redes e serviços associados, e o uso do Blockchain como uma tecnologia potencial para lidar com esses ataques, além dos desafios de implementação do Blockchain na IoT.

Em seguida, são discutidas várias soluções existentes baseadas em Blockchain para mitigar ataques DDoS no ambiente de IoT. As soluções são classificadas em quatro categorias: soluções baseadas em Arquitetura Distribuída, soluções baseadas em Gerenciamento de Acesso, soluções baseadas em Controle de Tráfego e soluções baseadas na Plataforma Ethereum. Todas as soluções são avaliadas criticamente quanto aos seus princípios de funcionamento, mecanismos de defesa contra DDoS (prevenção, detecção, reação), pontos fortes e fracos. Finalmente, discute-se futuras direções de pesquisa que podem ser exploradas para projetar e desenvolver melhores soluções baseadas em Blockchain para mitigar ataques DDoS na IoT.

O estudo proposto por (LI et al., 2023) aborda a crescente adoção da tecnologia blockchain devido às suas características descentralizadas, seguras e transparentes, enfatizando a importância de garantir sua resiliência contra ameaças de rede, especialmente ataques de Negação de Serviço Distribuída (DDoS). A pesquisa foca na vulnerabilidade dos sistemas blockchain a esses ataques, que comprometem suas características descentralizadas, representando uma ameaça à segurança e confiabilidade da tecnologia. Foi desenvolvida uma nova técnica de integração adaptativa para a detecção e identificação de variados ataques DDoS. Para garantir a robustez e validade da abordagem, foi utilizado um conjunto de dados derivado do CIC-DDoS2019, que reúne múltiplos ataques DDoS.

A metodologia foi aplicada para detectar ameaças DDoS e classificá-las em sete subcategorias de ataques únicas. Para lidar com a ampla gama de variações nos ataques DDoS, foi proposto um framework holístico que integra de forma harmoniosa cinco modelos de aprendizado de máquina: Gate Recurrent Unit (GRU), Redes Neurais Convolucionais (CNN), Long-Short Term Memory (LSTM), Redes Neurais Profundas (DNN) e Support Vector Machine (SVM). O aspecto inovador do framework é a introdução de um mecanismo dinâmico de ajuste de peso, aprimorando a adaptabilidade do sistema. Os resultados experimentais confirmam a superioridade do método em conjunto em comparação com modelos individuais, em diversas métricas de avaliação.

O framework demonstrou uma precisão notável, com taxas de 99,7 para detecção e 87,6 para as tarefas de classificação. Ao desenvolver uma metodologia abrangente e adaptativa, este estudo abre caminho para fortalecer os mecanismos de defesa dos sistemas blockchain contra ataques DDoS, combinando a abordagem de ensemble com o mecanismo dinâmico de ajuste de peso.

O trabalho de (QURESHI, 2024) aborda os ataques de Negação de Serviço (DoS), que representam uma ameaça significativa no cenário digital atual, com atacantes sobrecarregando sistemas, redes ou aplicações para torná-los inacessíveis aos usuários legítimos. Esses ataques podem paralisar serviços online, causando perdas financeiras substanciais, danos reputacionais e interrupções operacionais para as empresas. Soluções inovadoras para mitigar ataques DoS agora incorporam uma combinação de estratégias defensivas tradicionais e tecnologias de ponta, como inteligência artificial (IA), aprendizado de máquina (ML) e mecanismos avançados de filtragem de tráfego.

A adoção dessas técnicas, juntamente com monitoramento contínuo, sistemas de detecção de anomalias e práticas robustas de arquitetura de rede, proporciona uma defesa abrangente contra ataques DoS. No entanto, como os atacantes continuamente refinam seus métodos, as organizações devem permanecer proativas atualizando regularmente suas defesas, conduzindo avaliações de vulnerabilidade e mantendo-se informadas sobre ameaças emergentes.

O estudo de (RIANDARI et al., 2024) propõe um algoritmo de otimização dinâmica projetado para aumentar a resiliência de redes blockchain contra ataques distribuídos, como os ataques de Negação de Serviço Distribuída (DDoS), Sybil e Eclipse. O objetivo principal é desenvolver uma estratégia de controle adaptável em tempo real, que minimize a degradação do desempenho da rede enquanto responde dinamicamente às ameaças em evolução. A pesquisa integra otimização multiobjetivo, teoria dos jogos e aprendizado por reforço para formular uma estratégia de defesa capaz de se adaptar a condições adversas.

A metodologia utilizou um modelo de espaço de estado modificado, onde o desempenho do blockchain é representado por um sistema de equações dinâmicas, influenciadas por ações de controle (medidas defensivas) e vetores de ataque. O problema de otimização

é formulado para minimizar uma função de custo que equilibra a resiliência da rede e o uso eficiente de recursos.

Os estudos revisados apresentam diferentes abordagens para mitigar ataques DDoS utilizando a tecnologia blockchain em diversos cenários, como redes tradicionais e IoT. Cada pesquisa explora soluções e enfrenta desafios no combate a essas ameaças. A Tabela 1 resume os principais objetivos, lacunas e resultados de cada trabalho discutido, fornecendo uma visão geral das contribuições e limitações das abordagens abordadas.

Tabela 4 – Resumo dos Trabalhos Correlatos

Referência	**Objetivos**	**Lacunas**	**Resultados**
(WANI et al., 2021)	Analisar soluções baseadas em blockchain para mitigar ataques DDoS em redes de IoT.	Desafios na implementação do blockchain em IoT e a diversidade das soluções.	Discussão de quatro categorias de soluções baseadas em blockchain para DDoS na IoT.
(SHAH et al., 2022)	Explorar o uso de blockchain para mitigar ataques DDoS, destacando suas abordagens em diversos domínios.	Necessidade de soluções mais avançadas devido à crescente complexidade dos ataques.	Revisão abrangente das abordagens para mitigação de DDoS usando blockchain.
(LI et al., 2023)	Desenvolver uma técnica de integração adaptativa para detectar e classificar ataques DDoS em sistemas blockchain.	Desafios ao lidar com a ampla variedade de ataques DDoS.	Framework utilizando cinco modelos de aprendizado de máquina, com alta precisão de detecção e classificação (99,7% e 87,6%, respectivamente).
(QURESHI, 2024)	Propor uma defesa contra ataques DoS, incorporando IA, ML e técnicas avançadas de filtragem de tráfego.	Exigência de atualização contínua das defesas devido à evolução dos métodos dos atacantes.	Combinação de IA e ML para mitigar ataques DoS, com ênfase no monitoramento contínuo e sistemas de detecção de anomalias.
(RIANDARI et al., 2024)	Criar uma estratégia de controle adaptável para aumentar a resiliência de redes blockchain contra ataques distribuídos.	Complexidade em equilibrar a resiliência da rede e o uso eficiente de recursos.	Algoritmo de otimização dinâmica que responde em tempo real a ameaças, equilibrando resiliência e uso de recursos.

Fonte: Autor, 2024.

Esses trabalhos foram selecionados devido à sua relevância direta para o tema central deste estudo, que se concentra em mitigar ataques de Negação de Serviço Distribuída (DDoS) utilizando tecnologias emergentes, como o blockchain. Dessa forman, eles fornecem uma base de conhecimento e apresentam lacunas e desafios que podem ser explorados para aprimorar as abordagens atuais na mitigação de DDoS utilizando blockchain, alinhando-se com o escopo e as metas da pesquisa proposta.

3.3 Considerações finais sobre o capítulo

Os estudos analisados destacam os desafios e as estratégias associadas à simulação de ataques DDoS e às técnicas de mitigação em redes blockchain voltadas para a cibersegurança. A partir das limitações observadas nos trabalhos correlatos, é possível identificar lacunas significativas que ainda precisam ser abordadas para aprimorar a robustez e a eficiência dos sistemas de blockchain contra ataques DDoS.

Primeiramente, muitos dos estudos revisados apresentaram limitações em termos da escala e da diversidade dos cenários de simulação utilizados, o que pode comprometer a generalização dos resultados para ambientes reais e diversos. Além disso, a otimização de parâmetros e a seleção de características para detectar e mitigar ataques ainda representam um desafio significativo, devido à complexidade e à dinamicidade das redes blockchain.

Outro ponto crítico identificado é a necessidade de conjuntos de dados mais representativos. A maioria dos trabalhos estudados utilizou dados específicos e limitados, levantando preocupações sobre a capacidade dos modelos propostos de se generalizarem para diferentes contextos e ataques.

Para superar essas limitações, este trabalho foca em realizar uma simulação local com o objetivo de identificar a resiliência da rede. Embora não seja realizado um aumento do conjunto de dados de treinamento ou a utilização de técnicas de aumento de dados, a simulação fornecerá informações sobre o comportamento e a robustez da rede em diferentes cenários. A análise e os resultados obtidos poderão contribuir significativamente para o entendimento das vulnerabilidades e pontos fortes da rede, fornecendo uma base para futuras melhorias e otimizações.

Portanto, esta seção delineou os trabalhos correlatos que fundamentaram a realização desta pesquisa, fornecendo a base teórica para o desenvolvimento dos modelos propostos. A seção subsequente expõe detalhadamente a metodologia empregada neste estudo, abordando as técnicas de simulação utilizada e avaliação de desempenho utilizadas para mitigar ataques DDoS em redes blockchain, contribuindo para o avanço da cibersegurança neste campo.

4 Materiais e Métodos

4.1 Considerações iniciais sobre o capítulo

Esta seção tem como objetivo discorrer sobre a criação e avaliação de uma rede Blockchain desenvolvida em Python, com foco na análise de sua eficiência e resiliência diante de ataques de sobrecarga, como os ataques DDoS. A proposta é investigar o comportamento da rede sob condições adversas e avaliar a eficácia de diferentes estratégias de mitigação para melhorar a cibersegurança em sistemas descentralizados.

4.2 Metodologia

4.2.1 Considerações gerais da metodologia aplicada

Este estudo caracteriza-se como exploratório e experimental. O estudo exploratório busca investigar o comportamento da rede Blockchain sob ataques de sobrecarga, como os ataques DDoS, identificando possíveis vulnerabilidades e soluções. Já o estudo experimental se concentra na realização de testes controlados para observar a resiliência do sistema sob diferentes cenários de ataque e analisar o impacto na operação da rede. Além disso, o estudo é de natureza quantitativa, pois envolve a coleta e análise de dados numéricos, como tempo de resposta, volume de dados e taxa de disponibilidade dos serviços, que serão utilizados para avaliar a eficiência e a resiliência do Blockchain.

A pesquisa pode ser classificada como aplicada. O objetivo principal é o desenvolvimento e avaliação de uma solução prática, no caso: a rede Blockchain. A pesquisa visa melhorar a segurança cibernética e a eficiência de sistemas descentralizados, oferecendo contribuições significativas para a área de cibersegurança, com ênfase na mitigação de ataques DDoS. O estudo também tem uma característica descritiva, pois busca observar e descrever o comportamento da rede Blockchain durante a simulação dos ataques, coletando métricas e informações sobre o desempenho e a resiliência do sistema.

O estudo foi realizado em um ambiente controlado e local, utilizando máquina com configurações específicas para hospedar a rede Blockchain e simular os ataques. O ambiente experimental será montado de forma que seja possível testar diferentes cenários, garantindo um controle rigoroso sobre as condições de hardware e software.

4.2.2 Criação de código Python

A rede Blockchain foi implementada utilizando a linguagem Python, em conjunto com uma adaptação da linguagem Ethereum, amplamente reconhecida pela sua aplicação em redes como a do Bitcoin. Essa adaptação permitiu criar uma blockchain funcional e eficiente, aproveitando conceitos consolidados no desenvolvimento de sistemas descentralizados, enquanto o código foi ajustado para atender às necessidades específicas deste projeto.

A escolha do Python como linguagem de implementação foi motivada pelas suas características, tais como a facilidade de aprendizado e a vasta disponibilidade de bibliotecas específicas para a área de cibersegurança. Dentre as bibliotecas mais relevantes, destacam-se **Cryptografy** e **PyCrypto**, que oferecem suporte robusto para operações criptográficas essenciais à segurança da blockchain, como geração de chaves, assinatura digital e funções de hashing.

O desenvolvimento do código seguiu o paradigma de **Programação Orientada a Objetos (POO)**, o que garantiu maior organização, modularidade e clareza no entendimento do sistema. A POO permitiu a divisão do sistema em classes distintas, cada uma representando um componente ou funcionalidade específica do blockchain, facilitando tanto a manutenção quanto a expansão do código. O código desenvolvido está disponível no GitHub[1].

A seguir, são apresentadas as principais classes desenvolvidas no projeto:

- **Classe `main`**: A classe `main` implementa um menu interativo em linha de comando, responsável por gerenciar as funcionalidades relacionadas à blockchain e à simulação de ataques DDoS. Essa estrutura centraliza a simulação e o gerenciamento da blockchain, oferecendo um ambiente controlado para a realização de testes que monitoram o comportamento da blockchain em um ambiente local.

- **Classe `Blockchain`**: A classe `Blockchain` é responsável por armazenar e gerenciar a cadeia de blocos. Ela inclui métodos para adicionar novos blocos, verificar a integridade da cadeia e validar os hashes, assegurando que a sequência de blocos não seja comprometida por alterações maliciosas. Além de processar e minerar blocos, a classe é capaz de gerar relatórios detalhados. Ao final da simulação, ela exibe estatísticas em uma tabela formatada e exporta os dados da blockchain para uma planilha Excele um arquivo de nota com as estatísticas. Essa planilha contém informações detalhadas sobre cada bloco, como hash, hash anterior, timestamp e transações, além de diferenciar visualmente os blocos válidos dos descartados por meio de cores.

[1] Disponível em: *<[https://github.com/Geovane-lima/Geovane-Lima-TCC-Simulacao-de-ataque-DDoS-em-redes-Blockchain-para-ciberseguranca]>*

- **Classe `Bloco`**: A classe `Bloco` representa cada bloco individual dentro da cadeia. Ela contém atributos como índice, timestamp, transações, hash do bloco atual e referência ao hash do bloco anterior. Além disso, implementa métodos para calcular e validar o hash com base nos dados contidos no bloco, sendo crucial para garantir a segurança e integridade da cadeia.

- **Classe `Transação`**: A classe `Transação` gerencia as transações realizadas na rede. Ela contém métodos para criar e validar transações, assegurando que cada uma seja assinada digitalmente pelo remetente. Esse processo garante a segurança da rede e impede fraudes, como tentativas de gasto duplo.

- **Classe `server`**: A classe `server` implementa um servidor HTTP local, utilizado para interagir com a blockchain local por meio de uma API REST, utilizando o framework *Flask*. Esse servidor permite que os usuários enviem transações e visualizem a cadeia de blocos, criando uma interface acessível para testar o desempenho do sistema e avaliar a sua resiliência contra ataques simulados, como DDoS.

- **Classe `AtaqueDDoS`**: A classe `AtaqueDDoS` simula um ataque de negação de serviço distribuído (DDoS), em que múltiplas requisições simultâneas são enviadas a um servidor com o intuito de sobrecarregá-lo e, consequentemente, torná-lo indisponível. Além de simular o ataque, a classe integra a monitoração de métricas de desempenho da rede, como resiliência, volume de dados e padrões de transações. Isso permite analisar como o servidor reage ao ataque e obter dados detalhados sobre o impacto nas métricas da rede.

4.2.3 Desenvolvimento da Rede Blockchain

4.2.3.1 Construção de um Servidor Local

Para a construção da rede Blockchain, optou-se pelo desenvolvimento de um servidor local utilizando o framework Flask. Essa escolha deu-se por razões específica do Flask, características que o tornam ideal para criar aplicações web e APIs em Python de forma prática e eficiente. Além disso, o Flask permite integração com outras bibliotecas Python relevantes para a implementação de Blockchains, como hashlib (responsável por funções de hash criptográfico), json (para manipulação de dados no formato JSON) e requests (que viabiliza a comunicação HTTP entre diferentes nós). da rede).

O servidor desenvolvido desempenha um papel fundamental no projeto e foi criado como um ambiente controlado para o desenvolvimento, execução dos testes e a análise do desempenho da rede Blockchain. Nessa estrutura, a rede Blockchain foi projetada como uma cadeia de dados composta por blocos interconectados. Cada bloco contém informações essenciais: transações registradas, um timestamp que marca o momento de sua criação, o

hash que representa o bloco anterior e o hash exclusivo do próprio bloco, garantindo a integridade da cadeia.

Além disso, o ambiente controlado do servidor viabilizou a execução de simulações específicas, como ataques DDoS do tipo HTTP Flood, nos quais um grande volume de requisições HTTP é enviado simultaneamente com o objetivo de sobrecarregar os recursos do sistema. Essa simulação foi crucial para observar como a rede Blockchain responde às condições adversárias, fornecendo dados importantes para análises de desempenho e proposições de estratégias de mitigação.

4.2.3.2 Testes em máquina com configuração de de Hardware específica

Os testes foram contínuos utilizando uma máquina equipada com 8 GB de RAM, processador Intel Core i5 e SSD de 250 GB. Esses recursos foram escolhidos para representar uma configuração interna, comum em equipamentos de uso doméstico ou corporativo, permitindo uma análise realista do desempenho do sistema Blockchain em condições práticas.

Os experimentos visaram compreender como as configurações de hardware impactam a execução de transações, a mineração de blocos e a resiliência do sistema frente a ataques simulados, como DDoS. Além disso, buscou-se avaliar a estabilidade e a eficiência do sistema sob diferentes cargas de trabalho, gerando dados relevantes para otimizações futuras.

4.2.4 Simulação de Ataques DDoS

4.2.4.1 Tipo de Ataque: HTTP Flood

A simulação do ataque DDoS foi direcionada especificamente para o tipo HTTP Flood, um dos métodos mais comuns desse tipo de ataque, no qual uma grande quantidade de requisições HTTP é enviada de forma simultânea para sobrecarregar os recursos do servidor-alvo. Esse tipo de ataque foi escolhido para sua capacidade de simular uma carga excessiva de tráfego que compromete o desempenho e a disponibilidade do sistema.

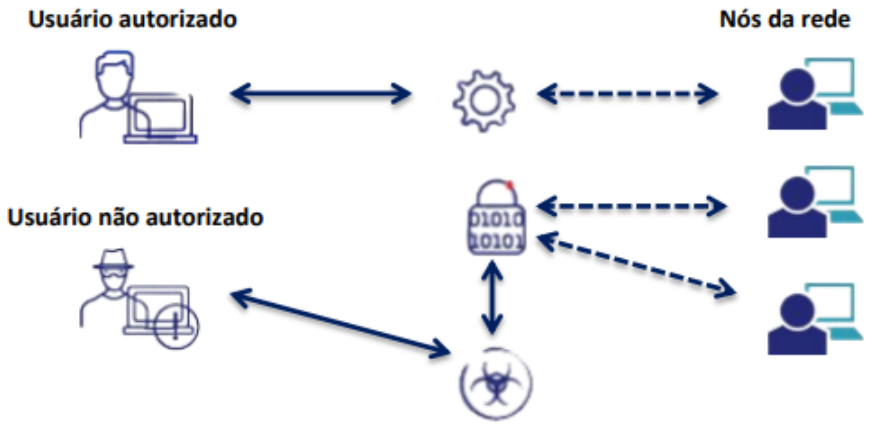
4.2.4.2 Cenários de Teste

Foram definidas configurações específicas para analisar a funcionalidade, segurança e disponibilidade da rede frente a ataques excessivos, frequentemente relacionados a ataques DDoS. Cada nível de requisição simulada reflete intensidades diferentes de ataque DDoS, permitindo avaliar o comportamento da rede Blockchain sob cenários variados, desde ataques sutis até tentativas diversas de paralisação. Os cenários explorados foram baseados em volumes progressivos de requisições, simulando diferentes intensidades de tráfego

malicioso. As cargas simuladas incluíam os seguintes níveis de requisições simultâneas: 100.000, 250.000, 500.000 e 1.000.000 de transações/blocos.

O diagrama abaixo ilustra a arquitetura simulada, mostrando as interações entre os usuários e a rede Blockchain desenvolvida. Ele visualiza as simulações feitas em diferentes condições de acesso dos usuários, destacando a diferença entre acessos legítimos e tentativas de ataque. Enquanto os usuários autorizados têm acesso direto à rede, os não autorizados precisam passar pela Blockchain na tentativa de obter acesso. Caso seja identificado um comportamento de invasão ou tentativa de ataque, a rede aciona mecanismos de segurança que bloqueiam o acesso suspeito, registram o evento para posterior análise e ajustam as regras de detecção para mitigar novos riscos de forma proativa.

Figura 17 – Arquitetura do cenário de teste executado



Fonte: (Autor, 2024)

No cenário de 100.000 requisições simultâneas , o impacto esperado é uma manipulação leve no desempenho da rede, com um aumento quase imperceptível na latência ou no tempo de resposta. Essa simulação teve como objetivo testar as defesas do sistema e identificar possíveis vulnerabilidades, podendo passar despercebidos pelos mecanismos tradicionais de detecção. Nesse caso, foi realizado um ataque de baixa intensidade contra a rede Blockchain criada para estudar seu comportamento, buscando informações sobre como melhor explorá-la futuramente. Além disso, cenários de baixa intensidade, como este, podem representar casos reais em que caçadores tentam camuflar suas ações em meio ao tráfego legítimo. Por exemplo, um hacker experiente poderia enviar requisições aparentemente normais para explorar vulnerabilidades enquanto evita suspeitas. Nas redes Blockchain, onde a transparência e a segurança são cruciais, essa etapa inicial de reconhecimento pode ser usada para preparar ataques mais severos no futuro.

Com 250.000 requisições simultâneas, observa-se um aumento significativo na carga do servidor, o que pode afetar tanto o tempo de resposta quanto a latência de maneira mais notável. Essa simulação forçou a rede a redirecionar recursos para lidar com a sobrecarga,

comprometendo parcialmente sua eficiência. Em um contexto real, ataques dessa magnitude podem não apenas prejudicar temporariamente o desempenho do sistema, mas também explorar vulnerabilidades específicas que só se tornam evidentes sob condições de maior carga. Além disso, esse cenário também destaca como o redirecionamento de recursos para lidar com o ataque pode comprometer outras funções da rede. A necessidade de alocar mais processamento para tratar requisições maliciosas pode reduzir a capacidade do sistema de lidar com tráfego legítimo, prejudicando diretamente a experiência dos usuários finais.

No cenário de 500.000 requisições simultâneas , o impacto na rede é substancial, resultando em uma queda acentuada no desempenho e aumentando significativamente a probabilidade de interrupções temporárias nos serviços. Nesse nível, a capacidade do sistema de resposta é eficiente e severamente comprometida, uma vez que a sobrecarga atinge aspectos críticos, exigindo recursos computacionais e de rede muito além das condições normais de operação. Essa simulação é especialmente relevante para representar ataques organizados e sustentados, frequentemente realizados por redes de bots (botnets). Essas redes consistem em dispositivos comprometidos que operam de forma coordenada, enviando grandes volumes de requisições maliciosas com o objetivo de sobrecarregar ou alvo por longos períodos. Esse cenário foi projetado não apenas para interromper os serviços temporariamente, mas também para explorar a exaustão dos recursos do sistema, como memória e CPU. Além disso, ataques dessa magnitude podem expor limitações no design da rede, como gargalos em algoritmos de consenso ou ineficiências na comunicação entre nós. Esses pontos fracos, quando explorados, podem levar a falhas em cascata, afetando tanto a disponibilidade quanto a integridade do sistema.

No cenário de 1.000.000 de requisições simultâneas , a rede enfrenta uma paralisação quase completa, expondo as limitações de hardware. Esse nível de ataque reflete uma sobrecarga, em que todos os recursos disponíveis, como processamento e memória, são consumidos rapidamente, resultando na incapacidade do sistema de atender a qualquer requisição, seja ela legítima ou maliciosa. Essa simulação não apenas testa a capacidade da rede de lidar com cargas excessivas, mas também evidencia vulnerabilidades críticas que podem ser exploradas em cenários reais.

Cada cenário foi projetado para simular diferentes comportamentos de um ataque DDoS, abrangendo desde tentativas leves e quase imperceptíveis até sobrecargas massivas que poderiam paralisar completamente a rede. Essa abordagem progressiva permitiu compreender como a rede Blockchain reage a diferentes intensidades de tráfego malicioso, além de identificar os pontos críticos de falha e as oportunidades de melhoria. Ao projetar esses cenários, buscou-se refletir sobre situações reais enfrentadas por redes Blockchain em ambientes de produção. Cada cenário, portanto, oferece uma oportunidade para testar e avaliar não apenas a capacidade da rede de lidar com o ataque, mas também a eficácia de diferentes estratégias de mitigação, como balanceamento de carga, bloqueio automático de

IPs maliciosos, uso de proxies e escalabilidade horizontal. Essa progressão controlada de panorama oferece uma visão do espectro de desafios que os sistemas Blockchain podem enfrentar, permitindo a construção de soluções mais robustas e resilientes para proteger a integridade, a disponibilidade e o desempenho dessas redes, mesmo diante de ataques intensos e sofisticados.

4.3 Considerações finais sobre o capítulo

Os resultados mostraram que a solução proposta foi eficaz em manter a estabilidade da rede Blockchain em diferentes cenários de ataque. A pesquisa demonstrou que redes Blockchain, quando combinadas com estratégias adequadas de mitigação, têm grande potencial para resistir a ataques DDoS. Essas descobertas foram feitas para uma melhor compreensão das vulnerabilidades e das possibilidades de aprimoramento na cibersegurança de sistemas distribuídos.

5 Resultados e Discussão

5.1 Considerações iniciais sobre o capítulo

Este capítulo apresenta os resultados obtidos na simulação de ataques DDoS na rede Blockchain desenvolvida, bem como a análise de sua eficiência e resiliência. O estudo incluiu experimentos realizados em uma máquina de uso doméstico, onde diferentes cenários foram testados para avaliar a resposta da rede a diferentes cargas de transações e condições de ataque.

Os principais aspectos analisados foram o padrão de transação, o volume de dados trafegados e a disponibilidade dos serviços da rede Blockchain. Os testes foram conduzidos com diferentes quantidades de blocos processados, permitindo uma avaliação sobre o comportamento da rede em condições normais e sob ataques.

Os resultados foram organizados em tabelas e discutidos detalhadamente para compreender melhor a capacidade da rede Blockchain de lidar com cargas crescentes de processamento e resistir a ataques maliciosos. A análise estatística permitiu identificar padrões de desempenho e limitações do sistema em relação à segurança e eficiência computacional.

5.1.1 Resultados obtidos

Os dados coletados durante a execução da simulação foram organizados e sistematizados nas Tabelas a seguir, apresentando uma visão sobre o comportamento da rede Blockchain sob diferentes cargas e condições, o que permite uma análise da eficiência e da resistência da rede em face de ataques maliciosos.

Inicialmente, foi realizado um levantamento estatístico referente à execução da rede Blockchain, levando em consideração aspectos fundamentais como a criação, validação e descarte dos blocos. A criação de blocos está diretamente associada à capacidade da rede de gerar novas unidades de dados, enquanto a validação diz respeito ao processo de verificação da integridade e autenticidade dos blocos antes de sua inclusão no livro-razão distribuído. Por outro lado, o descarte de blocos é um indicativo da eficácia do sistema em filtrar transações inválidas ou malformadas, garantindo a segurança e o bom funcionamento da rede.

Tabela 5 – Estatísticas para a Execução de Blocos

Estatística/Nº de blocos	**100.000**	**250.000**	**500.000**	**1.000.000**
Blocos criados	100.000	250.000	500.000	1.000.000
Blocos validados	99.137	249.069	499.028	998.215
Blocos descartados	863	931	972	1.785
Taxa de hash - por minuto	137	152	161	208

Fonte: Autor (2024)

A tabela mostra o comportamento da rede Blockchain sob diferentes escalas de execução, com um aumento no número de blocos processados, mas também com uma leve redução na quantidade de blocos validados e um pequeno aumento nos blocos descartados, o que pode ser associado a limitações de capacidade e recursos durante o aumento da carga de trabalho. Nela, observamos diferentes parâmetros, incluindo o número de blocos criados, validados, descartados e a taxa de hash por minuto, para quatro diferentes quantidades de blocos processados.

A primeira linha da tabela mostra o número de blocos criados, ou seja, a quantidade de novos blocos gerados pela rede, que aumenta linearmente com a quantidade de blocos processados, como esperado. Para cada quantidade de blocos, o número de blocos criados é igual ao número especificado, o que indica que a rede foi capaz de gerar a totalidade dos blocos solicitados durante o experimento.

A segunda linha exibe os blocos validados, que são os blocos aceitos e verificados pela rede. A diferença entre os blocos criados e os validados reflete o número de blocos que, por alguma razão, não passaram na validação, como falhas na criação ou problemas de integridade. Essa diferença, que é relativamente pequena, mostra que a maior parte dos blocos criados foi validada, mas que um número reduzido foi descartado.

A terceira linha, que mostra os blocos descartados, revela que esse número variou entre 863 e 972 blocos, indicando uma certa instabilidade no processo de validação à medida que o número de blocos aumentava. O aumento dos blocos processados pode ter levado a uma maior incidência de falhas ou erros, refletindo a necessidade de mais recursos computacionais para garantir a integridade dos blocos.

Por fim, a quarta linha da tabela apresenta a taxa de hash por minuto, que mede a quantidade de funções de hash executadas pela rede a cada minuto. O valor da taxa de hash por minuto aumentou com o número de blocos processados, o que é esperado, pois mais blocos geram maior carga para a rede. A taxa variou entre 137 e 161 hashes por minuto, o que sugere que a rede foi capaz de se ajustar e se tornar mais eficiente à medida que a carga aumentava.

Após a criação da rede Blockchain, foi realizada uma simulação de ataque DDoS, com o objetivo de testar a resiliência e o desempenho da rede em um cenário adverso. O

ataque DDoS foi implementado enviando uma grande quantidade de solicitações simultâneas para a rede, sobrecarregando seus recursos e tentando exaurir a capacidade de processamento da rede Blockchain.

Para realizar o ataque, foi criada localmente uma carga simulada que envolvia o envio de pacotes de dados para as diferentes partes da rede. Isso foi feito para testar como a infraestrutura da Blockchain se comportaria quando forçada a lidar com uma quantidade excessiva de requisições, o que poderia causar uma diminuição na eficiência do processo de validação de blocos ou até a falha do sistema. A ideia era criar um ambiente de teste no qual as limitações da rede fossem evidenciadas, de modo que fosse possível identificar pontos frágeis, como a capacidade de resposta da rede, o tempo de processamento e o impacto no volume de dados gerenciados pela Blockchain.

Essa fase da simulação avaliou três parâmetros fundamentais para entender o impacto do ataque DDoS sobre a rede Blockchain: padrão de transação, volume de dados e disponibilidade de serviço. Cada um desses parâmetros foi essencial para medir diferentes aspectos da performance da rede sob estresse, e os resultados estão organizados nas tabelas a seguir.

O padrão de transação foi analisado com o objetivo de verificar como os tempos máximos e mínimos das transações foram afetados pelo ataque. Esse parâmetro é crucial para entender se o ataque DDoS causou atrasos significativos nas transações ou se a rede foi capaz de manter uma performance constante, apesar da sobrecarga.

Tabela 6 – Padrão de Transação para a Execução de Blocos

Parâmetro/Nº de blocos	**100.000**	**250.000**	**500.000**	**1.000.000**
Tempo máximo de transação (em segundos)	2.3475	2.1279	2.1283	2.2471
Tempo mínimo de transação (em segundos)	2.0092	2.0038	2.0184	2.0302

Fonte: Autor (2024)

No contexto dos resultados apresentados, observa-se que à medida que o número de blocos aumenta, o tempo máximo de transação tende a diminuir ligeiramente, com valores de 2.3475 segundos para 100.000 blocos e alcançando 2.2471 segundos para 1.000.000 de blocos. Isso pode indicar uma otimização do processamento das transações à medida que mais blocos são gerados. Por outro lado, o tempo mínimo de transação permanece relativamente constante, variando entre 2.0092 segundos para 100.000 blocos e 2.0302 segundos para 1.000.000 de blocos, sugerindo que o sistema manteve um tempo de processamento mínimo estável, independentemente do aumento no volume de blocos.

Dando continuidade à análise dos parâmetros de desempenho da rede Blockchain, a tabela a seguir apresenta os dados enviados e recebidos pela rede durante a simulação de

ataque DDoS. Ao correlacionar com os tempos de transação apresentados anteriormente, é possível observar como o aumento no tráfego de dados influencia a eficiência do processamento de transações e a resiliência do sistema. A medição do tráfego total enviado e recebido fornece uma perspectiva mais ampla sobre o desempenho da rede, especialmente em cenários de sobrecarga.

Tabela 7 – Volume de Dados para a Execução de Blocos

Estatística/Nº de blocos	**100.000**	**250.000**	**500.000**	**1.000.000**
Dados enviados (bytes)	1.500	21.372	25.308	56.408
Dados recebidos (bytes)	4.600	52.108	56.762	77.321

Fonte: Autor (2024)

A tabela apresentada anteriormente detalha o volume de dados enviados e recebidos pela rede durante a execução da Blockchain, destacando as métricas de tráfego sob a simulação realizada. À medida que o número de blocos aumenta, observa-se um crescimento considerável no tráfego de dados, refletido nas colunas de dados enviados e recebidos em bytes. Por exemplo, ao passar de 100.000 para 1.000.000 de blocos, o volume de dados enviados aumenta de 1.500 bytes para 56.408 bytes, enquanto os dados recebidos também seguem uma tendência crescente, de 4.600 bytes para 77.321 bytes. Esses números são indicativos de como o tráfego de dados pode crescer à medida que o sistema se torna mais robusto, mas também de como a rede precisa gerenciar eficientemente a comunicação para evitar gargalos e manter o desempenho sob ataques.

Atrelado com os dados sobre a disponibilidade do sistema, a medição do volume de dados é essencial para entender a capacidade da rede em manter sua operação durante a sobrecarga causada por um ataque DDoS. A quantidade de transações realizadas com sucesso, o total de transações processadas e a porcentagem de disponibilidade, conforme apresentados na tabela seguinte, fornecem uma visão integrada de como o volume de dados impacta a eficiência e a resiliência da Blockchain, refletindo diretamente na manutenção do serviço, mesmo diante do tráfego excessivo gerado pelo ataque.

Tabela 8 – Disponibilidade de Serviço para a Execução de Blocos

Estatística/Nº de blocos	**100.000**	**250.000**	**500.000**	**1.000.000**
Total de transações	99.137	249.069	499.028	998.215
Transações bem-sucedidas	96.482	239.804	490.097	960.083
Disponibilidade (%)	97,34%	96,28%	98,21%	96,18%

Fonte: Autor (2024)

A tabela apresentada fornece informações detalhadas sobre a disponibilidade de serviço da rede Blockchain durante a execução dos blocos, a quantidade de blocos proces-

sados. Ela inclui três parãmetros principais: transações bem-sucedidas, total de transações e a disponibilidade percentual do sistema.

A coluna "Transações bem-sucedidas"mostra o número de transações que foram concluídas com sucesso em cada cenário, enquanto a coluna "Total de transações"registra o total de transações processadas, incluindo aquelas que não foram concluídas com sucesso. A diferença entre essas duas colunas reflete as transações que falharam devido a problemas de rede, como a sobrecarga causada pelo ataque DDoS. Por exemplo, para 100.000 blocos, 99.137 transações foram processadas, das quais 96.482 foram bem-sucedidas, o que indica um pequeno número de falhas.

A métrica "Disponibilidade (%)"expressa a porcentagem de transações bem-sucedidas em relação ao total de transações processadas. Para o caso de 100.000 blocos, a disponibilidade foi de 97,34%, o que demonstra que uma grande maioria das transações conseguiu ser realizada com sucesso, apesar da pressão do ataque DDoS. Conforme o número de blocos aumenta, a disponibilidade varia ligeiramente, com uma leve queda na disponibilidade para 250.000 blocos (96,28%) e para 1.000.000 de blocos (96,18%). No entanto, a disponibilidade do sistema continua relativamente alta, mesmo sob ataque.

Esses dados refletem a resiliência da Blockchain em manter suas operações, evidenciando sua capacidade de continuar processando transações com sucesso, apesar das dificuldades impostas por um ataque DDoS. A leve variação nos percentuais de disponibilidade em diferentes cenários sugere que, enquanto a rede pode ser impactada por um volume crescente de transações, ela ainda mantém uma performance robusta, com boa capacidade de recuperação.

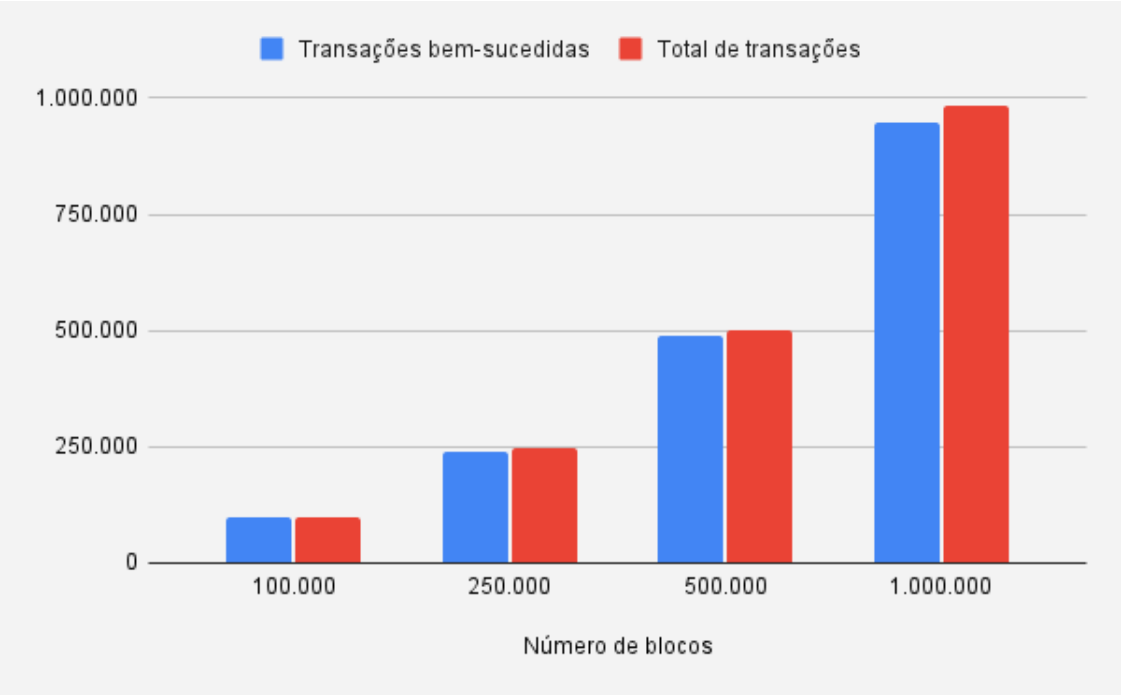
Com base nos resultados apresentados, observa-se que a rede Blockchain manteve um desempenho considerável mesmo sob a pressão de um ataque DDoS. Embora tenha ocorrido uma leve variação nas métricas de tempo de transação e disponibilidade de serviço à medida que o número de blocos aumentava, a rede conseguiu sustentar um alto nível de operação. A taxa de transações bem-sucedidas permaneceu significativa, com a disponibilidade do sistema oscilando entre 96,18% e 98,21%, indicando que a Blockchain demonstrou robustez e resiliência, mesmo diante da sobrecarga de solicitações. Esses resultados sugerem que, apesar do impacto de um ataque DDoS, o sistema de Blockchain manteve sua capacidade de validar e processar transações de forma eficiente, mostrando-se eficaz para operações em ambientes adversos.

5.1.2 Análise Comparativa

À luz dos resultados obtidos, a análise da resiliência da rede Blockchain sob ataque DDoS revelou que, em cenários com diferentes volumes de blocos, o sistema demonstrou uma excelente capacidade de processamento e manutenção de desempenho, mesmo quando

submetido a condições adversas. A disponibilidade de serviço, com taxas variando entre 96,18% e 98,%, foi um indicador claro de que a rede foi eficaz na validação e execução das transações, mesmo sob a pressão de um tráfego elevado gerado pelo ataque DDoS. Este comportamento reflete a robustez do sistema em lidar com a sobrecarga imposta por ataques, mantendo um nível de serviço elevado, como ilustrado no gráfico a seguir.

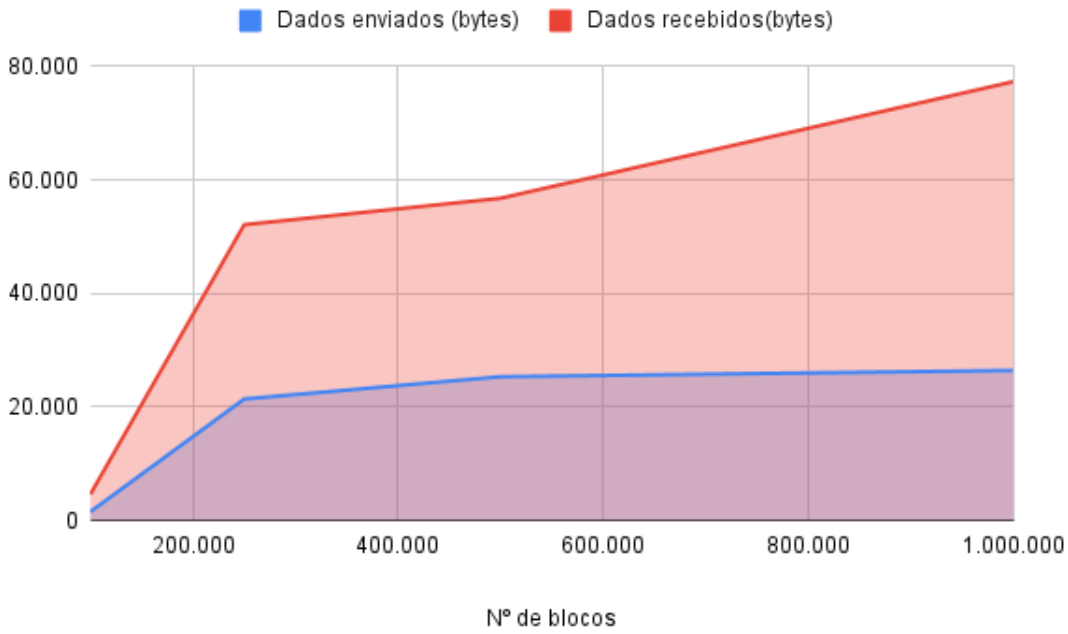
Figura 18 – Gráfico comparativo de Disponibilidade de Serviço sob Ataque DDoS



Fonte: Autor, 2024.

Além disso, as métricas de tempo de transação e volume de dados enviados e recebidos, quando observadas em conjunto, demonstraram que a rede Blockchain manteve sua eficiência operacional ao lidar com grandes volumes de blocos, mesmo diante do aumento do tráfego gerado pelo ataque DDoS. A integridade das transações foi preservada, e a rede conseguiu executar as operações de maneira eficiente, o que é fundamental para a credibilidade e funcionamento de redes descentralizadas. Essa resistência ao impacto do ataque, evidenciada nas métricas de desempenho, é crucial para garantir a continuidade das operações em um ambiente adverso, conforme mostrado no gráfico abaixo.

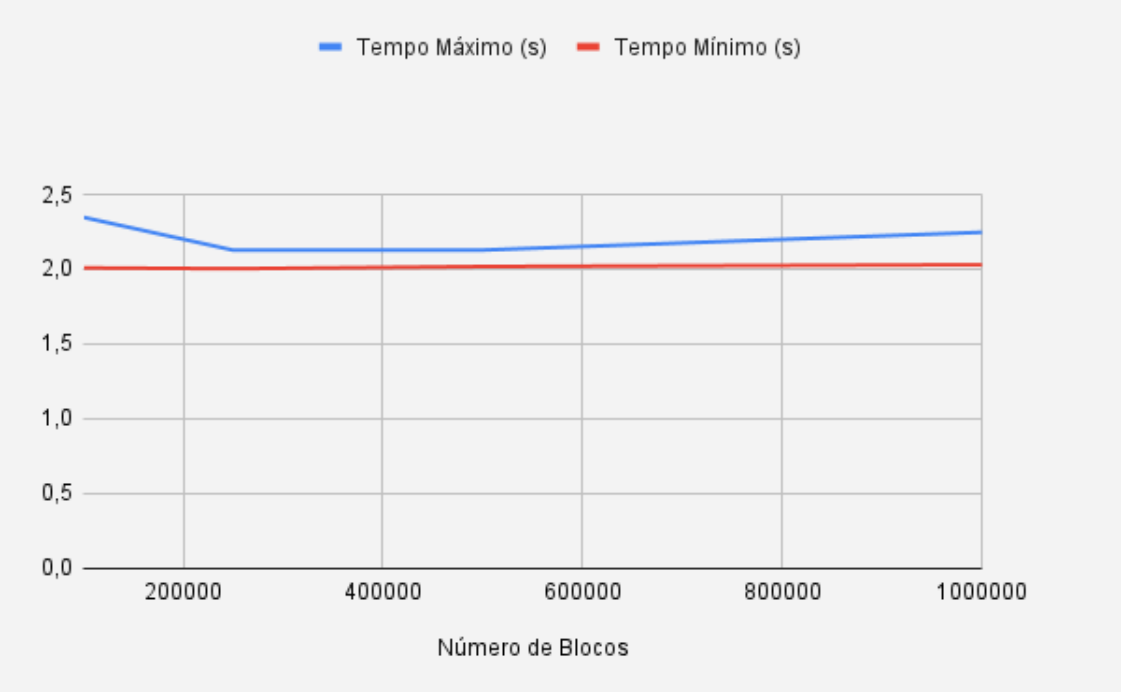
Figura 19 – Gráfico comparativo de Volume de Dados Enviados e Recebidos



Fonte: Autor, 2024.

Ao longo da simulação, as métricas de tempo de transação apresentaram variações mínimas, com exceção de uma leve flutuação observada nos cenários com volumes mais elevados de blocos. Essa variação pode ser atribuída à sobrecarga adicional imposta pela magnitude do ataque DDoS, que exigiu mais tempo para validar e processar as transações devido ao tráfego excessivo. No entanto, é importante destacar que os tempos máximos e mínimos de transação permaneceram dentro de faixas aceitáveis, o que demonstra que o sistema foi capaz de sustentar um nível considerável de desempenho, mesmo sob condições extremas. Este ponto é particularmente relevante para redes Blockchain, pois a necessidade de garantir a continuidade das transações com alta disponibilidade e baixa latência é uma das principais exigências desses sistemas. O gráfico a seguir ilustra a variação no tempo de transação ao longo dos diferentes cenários de carga.

Figura 20 – Gráfico comparativo de Tempo de Transação



Fonte: Autor, 2024.

Ademais, a análise da tabela de dados enviados e recebidos destacou claramente o impacto do aumento do volume de blocos na quantidade de tráfego gerado pela rede. Este aumento no tráfego gerado durante o ataque é um indicativo da escalabilidade da rede e de sua capacidade de gerenciar grandes volumes de dados durante eventos de tráfego intenso. A capacidade da rede em lidar com essa sobrecarga sem comprometer significativamente o desempenho é um reflexo direto da eficácia dos mecanismos de defesa implementados. Embora o tráfego tenha aumentado consideravelmente, o impacto no desempenho da rede não foi tão drástico quanto poderia ser esperado em um ataque DDoS típico, o que aponta para a eficácia das estratégias de mitigação.

Esses resultados indicam que, mesmo diante de um cenário adverso, como o ataque DDoS, a rede Blockchain foi capaz de sustentar suas operações com alta disponibilidade e baixa perda de transações. A análise dos dados sugere que a arquitetura da rede e os mecanismos de defesa implementados são robustos o suficiente para garantir a resiliência do sistema, mesmo sob estresse. A comparação entre os cenários com diferentes volumes de blocos mostrou que, embora o aumento no número de blocos tenha causado uma leve queda na disponibilidade, a rede se manteve operante, o que reforça a ideia de que a Blockchain pode ser uma solução viável em ambientes que exigem alta capacidade de processamento e resistência a ataques. Essa análise das métricas de desempenho, aliada à visualização dos gráficos comparativos, demonstra a resiliência e a eficiência da rede Blockchain em um cenário de ataque DDoS, sublinhando seu potencial para aplicações em ambientes de alta demanda e segurança.

5.2 Considerações finais sobre o capítulo

Com base nos experimentos realizados e nos resultados obtidos, conclui-se que a rede Blockchain demonstrou uma capacidade considerável de resistência a ataques DDoS, mantendo uma taxa elevada de transações bem-sucedidas e uma disponibilidade acima de 96% na maioria dos cenários testados.

Os dados obtidos reforçam a importância de soluções de segurança para mitigar os impactos de ataques DDoS em redes Blockchain, bem como a necessidade de ajustes dinâmicos na capacidade computacional para lidar com crescentes demandas transacionais. Futuros trabalhos podem explorar novos mecanismos para aprimorar ainda mais a segurança e a estabilidade de redes Blockchain diante de ameaças cibernéticas.

6 Conclusões

Este estudo apresentou uma análise sobre a resiliência de redes Blockchain diante de ataques de negação de serviço distribuídos (DDoS), com uma abordagem prática e experimental que enfatizou os impactos desses ataques na disponibilidade e desempenho do sistema. Por meio da simulação controlada que foi realizada frente a alguns cenários, foi possível perceber e documentar como o Blockchain reage sob estresse, identificando suas limitações e destacando seu potencial de adaptação quando possíveis estratégias adequadas de mitigação são aplicadas.

Os resultados desta pesquisa são altamente relevantes, pois oferecem uma compreensão mais clara de como o Blockchain - um dos pilares das tecnologias descentralizadas - se comporta frente a uma das mais persistentes e impactantes ameaças cibernéticas da atualidade. A pesquisa confirmou que, embora o Blockchain seja inerentemente robusta contra adulterações de dados, sua arquitetura, como qualquer sistema digital, permanece suscetível à saturação de recursos causada por ataques DDoS. Essa constatação não apenas valida preocupações levantadas pela literatura existente, mas também evidencia a necessidade de aprofundar o estudo sobre mecanismos específicos para assegurar a disponibilidade em sistemas distribuídos.

A importância desta pesquisa vai além da análise técnica, pois dialoga com um cenário crescente de utilização do Blockchain em aplicações críticas, como os registros de identidade. A indisponibilidade de serviços nesse contexto pode gerar consequências econômicas e sociais significativas, afetando desde o funcionamento de mercados até a segurança de informações sensíveis. Assim, ao demonstrar como estratégias de mitigação podem ser integradas para atenuar os impactos de ataques DDoS, este estudo contribui diretamente para o avanço da cibersegurança no uso prático dessa tecnologia.

Além disso, os dados coletados apresentados foram coerentes, frutos dos experimentos realizados localmente e que permitiram mensurar, com precisão, métricas como tempo de resposta, volume de dados processados e taxas de disponibilidade do serviço durante os ataques. A replicabilidade desses experimentos reforçam a validade das conclusões e possibilitam que outras pesquisas avancem a partir deste ponto, desenvolvendo soluções ainda mais eficazes e adaptadas a diferentes arquiteturas de Blockchain.

Outrossim, a relevância da pesquisa também se destaca ao considerar seu diálogo com estudos anteriores. Trabalhos já reconhecem os ataques DDoS como uma ameaça significativa, mas poucos exploraram e detalham a aplicabilidade e impacto sobre redes Blockchain. Este estudo não apenas complementa a literatura existente, mas também introduz novas perspectivas sobre como o Blockchain pode ser configurado e protegido

em contextos reais. Ele também oferece subsídios para que a comunidade científica e tecnológica avance na criação de soluções que garantam tanto a integridade quanto a disponibilidade de redes descentralizadas.

Uma contribuição essencial desta pesquisa é a lacuna que ela preenche. Até então, havia uma escassez de estudos empíricos que combinassem simulações de ataques em Blockchain com análise quantitativa e propostas práticas de mitigação. Este trabalho fornece esse elo perdido, destacando-se como uma referência inicial para a integração de cibersegurança em sistemas Blockchain. Ele não apenas descreve os problemas, mas também oferece caminhos concretos para superá-los, servindo como um guia para futuras implementações e estudos. Ainda que os resultados apresentados sejam promissores e contribuam significativamente para a literatura, é importante reconhecer que este trabalho, como toda pesquisa pioneira, pode conter algumas pontas soltas. Certos aspectos, como a análise de cenários mais amplos, a consideração de variações em arquiteturas de Blockchain ou a implementação de estratégias de mitigação em redes em produção, podem ser aprimorados em estudos futuramente. Esses elementos, embora tangencialmente abordados, representam oportunidades para aprofundamento e refinamento, contribuindo ainda mais para a aplicabilidade da solução proposta.

6.1 Limitações e Dificuldades Encontradas

Embora este trabalho tenha alcançado avanços significativos na compreensão e análise dos impactos de ataques DDoS em redes Blockchain, é imprescindível reconhecer os desafios e limitações que permearam sua execução. Um dos aspectos mais notáveis foi a restrição imposta pela infraestrutura disponível. Os experimentos foram conduzidos em equipamento com configurações modestas o suficientes para validar os conceitos teóricos e demonstrar a viabilidade das estratégias propostas, mas insuficientes para reproduzir plenamente a complexidade e o dinamismo de redes Blockchain operando em ambientes reais, altamente escaláveis e sujeitos a condições adversas.

Essa limitação no poder computacional influenciou diretamente a capacidade de simular cenários mais amplos e detalhados, especialmente aqueles que envolvem interações simultâneas com múltiplos nós. Em redes Blockchain de grande escala, a demanda por processamento e memória pode ser exponencialmente maior, o que demanda experimentações futuras em plataformas equipadas com recursos mais robustos e tecnologias avançadas. Tal ampliação permitiria que os resultados apresentados neste trabalho fossem não apenas validados, mas também refinados em contextos mais próximos da realidade.

Ademais, é crucial observar que os experimentos foram conduzidos em um ambiente controlado, que, embora adequado para estabelecer premissas iniciais e compreender as bases do problema, não reproduz integralmente as condições encontradas em sistemas

Blockchain em produção. Ambientes reais são dinâmicos e envolvem múltiplos fatores externos, como a ocorrência simultânea de diferentes tipos de ataques, variabilidade no tráfego legítimo, limitações de infraestrutura de rede e diferenças nas políticas de segurança adotadas pelos operadores. Esses elementos podem introduzir variáveis e incertezas que escapam ao controle de um laboratório de simulação, exigindo abordagens complementares que explorem cenários de implementação prática.

Apesar desses desafios, o trabalho se posiciona como uma base essencial para futuras investigações. A análise apresentada contribui de maneira substancial para a compreensão do comportamento de redes Blockchain sob ataques de negação de serviço, fornecendo evidências relevantes e propondo soluções iniciais. No entanto, abre-se espaço para a realização de estudos subsequentes que possam superar as limitações aqui identificadas. Em particular, destaca-se a necessidade de implementar e testar as estratégias sugeridas em sistemas reais, utilizando-se de plataformas computacionais mais avançadas e abordagens metodológicas capazes de incorporar a imprevisibilidade do ambiente cibernético.

Assim, este trabalho não apenas apresenta contribuições para a área de cibersegurança, mas também sugere caminhos claros para o avanço do conhecimento. O compromisso em endereçar as limitações identificadas reforça a relevância desta pesquisa e sua capacidade de servir como alicerce para estudos futuros, possibilitando uma abordagem ainda mais robusta e prática no enfrentamento dos desafios impostos à resiliência de sistemas Blockchain diante de ataques DDoS.

6.2 Trabalhos futuros

Por fim, esta pesquisa também abre portas para novos horizontes de investigação para trabalhos futuros, propondo caminhos para o desenvolvimento de estratégias mais sofisticadas e eficazes de defesa contra ataques de negação de serviço em redes Blockchain. O fortalecimento da segurança em sistemas descentralizados continua sendo um desafio complexo e em constante evolução, exigindo abordagens inovadoras e interdisciplinares. Entre as possibilidades futuras, destaca-se a implementação de algoritmos baseados em inteligência artificial e aprendizado de máquina para a detecção de padrões anômalos de tráfego. Esses algoritmos podem aprender com dados históricos de ataques para identificar comportamentos maliciosos antes que eles comprometam a rede, contribuindo para respostas mais ágeis e eficazes.

Outro aspecto essencial para trabalhos futuros é a aplicação e avaliação das soluções propostas em ambientes reais de produção. Embora as simulações realizadas forneçam dados substanciais, um estudo empírico em redes Blockchain operacionais poderia validar ainda mais as análises realizadas, além de revelar nuances práticas que só se manifestam em cenários do mundo real. Essa transição da teoria para a prática representa um passo

crucial para consolidar a relevância e a aplicabilidade das contribuições feitas por este trabalho, fortalecendo sua conexão com a indústria e outros domínios de pesquisa.

Ao propor essas direções, esta pesquisa não apenas aponta lacunas a serem preenchidas, mas também convida à colaboração e ao avanço contínuo do conhecimento, reafirmando o compromisso com o progresso da cibersegurança. Além disso, destaca a necessidade de salvaguardar informações sensíveis que transitam na internet, considerando que a proteção da integridade e confidencialidade dos dados é um aspecto crucial para a consolidação dessa tecnologia em cenários reais.

Dessa forma, este trabalho reafirma a importância de continuar investindo na segurança do Blockchain como tecnologia central para o futuro digital, garantindo não apenas a disponibilidade dos serviços, mas também a confiança dos usuários na proteção de suas transações e registros. As evidências aqui apresentadas não apenas validam o potencial dessa tecnologia, mas também iluminam as barreiras que precisam ser superadas para assegurar sua resiliência em um ambiente cibernético cada vez mais desafiador. Assim, esta pesquisa contribui significativamente para fortalecer a base de conhecimento que permitirá à tecnologia Blockchain se estabelecer como uma solução segura e confiável para a era digital.

Referências

ALMEIDA, L. C. de. *Ferramenta computacional para identificao e bloqueio de ataques de negao de servio em aplicaes web*. Tese (Doutorado) — Master Thesis in Portuguese, 2013. Citado na página 28.

BAO, J. et al. A survey of blockchain applications in the energy sector. *IEEE Systems Journal*, IEEE, v. 15, n. 3, p. 3370–3381, 2020. Citado na página 14.

BHOSALE, K. S.; NENOVA, M.; ILIEV, G. The distributed denial of service attacks (ddos) prevention mechanisms on application layer. In: IEEE. *2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*. [S.l.], 2017. p. 136–139. Citado na página 29.

BRUCE, R. A. Proposição de um modelo de blockchain para operações interbancárias. 2023. Citado na página 21.

BUTERIN, V. *A Next-Generation Smart Contract and Decentralized Application Platform*. 2014. Ethereum Whitepaper. Disponível em: <https://ethereum.org/en/whitepaper/>. Citado na página 24.

CARO, A. *Blockchain: The Beginners Guide to Understanding the Technology Behind Bitcoin & Cryptocurrency*. [S.l.]: CreateSpace Independent Publishing Platform, 2017. Citado 2 vezes nas páginas 16 e 17.

CARVALHO, I. L. K. d. Cibersegurança: um estudo comportamental de usuários da informação. 2023. Citado 2 vezes nas páginas 1 e 2.

CARVALHO, L. F. *Um ecossistema para detecção e mitigação de yearmalias em redes definidas por software*. Tese (Doutorado) — [sn], 2018. Citado na página 28.

CASTRO, M.; LISKOV, B. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, ACM New York, NY, USA, v. 20, n. 4, p. 398–461, 2002. Citado na página 24.

CATALINI, C.; GANS, J. S. Some simple economics of the blockchain. *Communications of the ACM*, ACM New York, NY, USA, v. 63, n. 7, p. 80–90, 2020. Citado na página 14.

CERIBELLI, V. O. Estudo de um ataque de negação (ddos). 004, 2020. Citado 2 vezes nas páginas 27 e 31.

CHAUM, D. Blind signatures for untraceable payments. *Advances in Cryptology: Proceedings of Crypto*, Springer, v. 82, p. 199–203, 1983. Citado na página 17.

CHICARINO, V. et al. 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*, v. 28, 2017. Citado na página 22.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. *IEEE Access*, v. 4, p. 2292–2303, 2016. Citado na página 14.

COMERT, O. *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*. [S.l.]: HeinOnline, 2020. Citado na página 18.

CONOSCENTI, M.; VETRO, A.; MARTIN, J. C. D. Blockchain for the internet of things: A systematic literature review. In: IEEE. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. [S.l.], 2016. p. 1–6. Citado 2 vezes nas páginas 23 e 26.

COSTA, W. L.; PORTELA, A. L. de C.; LOPES, G. R. Análise de características do tráfego de rede para detecção de ataques ddos em ambientes iot. *Anais do Computer on the Beach*, v. 12, p. 217–224, 2021. Citado na página 30.

CROSBY, M. et al. Blockchain technology: Beyond bitcoin. *Applied innovation*, v. 2, n. 6-10, p. 71, 2016. Citado 2 vezes nas páginas 20 e 26.

DAUMAS, Â. A. C. R. Contratos inteligentes: origens, implementações e aplicações. Universidade Federal do Rio de Janeiro, 2023. Citado na página 24.

DOURADO, L. B. M. A tecnologia de blockchain como facilitadora dos serviços cartorários brasileiros. 2020. Citado na página 24.

FIGUEIREDO, J. E. et al. Contratos inteligentes com ethereum. *Journal of innovation and Science: research and application*, v. 1, n. 1, p. 11–p, 2021. Citado na página 19.

FRANÇA, M. L. d. *Teda-guardian: detectando ataques DDOS em provedores de internet*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, 2020. Citado na página 29.

GAO, Y.; NOBUHARA, H. A decentralized trusted timestamping based on blockchains. *IEEJ Journal of Industry Applications*, The Institute of Electrical Engineers of Japan, v. 6, n. 4, p. 252–257, 2017. Citado na página 15.

GIL, F. C. P. *A implementação do Regulamento de Cibersegurança e o seu impacto para cibersegurança*. Dissertação (Dissertação de Mestrado) — ISCTE - Instituto Universitario de Lisboa (Portugal), 2021. Citado 3 vezes nas páginas 2, 5 e 7.

GIPP, B.; MEUSCHKE, N.; GERNANDT, A. Decentralized trusted timestamping using the blockchain. *arXiv preprint arXiv:1502.04015*, 2015. Citado na página 14.

GLOBO, O. *Ataques cibernéticos entram na agenda da governança*. 2021. Disponível em: <https://valor.globo.com/empresas/esg/noticia/2023/07/27/ataques-ciberneticos-entram-na-agenda-da-governanca.ghtml>. Acesso em: 1 mar. 2024. Citado na página 3.

GOUVEIA, L. D. Blockchain. Universidade Federal de Campina Grande, 2021. Citado na página 22.

GREVE, F. et al. Blockchain e a revolução do consenso sob demanda. In: *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Minicursos*. [S.l.: s.n.], 2018. Citado 2 vezes nas páginas 12 e 25.

HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. *Journal of Cryptology*, Springer, v. 3, n. 2, p. 99–111, 1991. Citado na página 17.

HOQUE, N.; BHATTACHARYYA, D. K.; KALITA, J. K. Botnet in ddos attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, IEEE, v. 17, n. 4, p. 2242–2270, 2015. Citado na página 27.

HORTA, A. *O que é Blockchain e como ela funciona?* 2022. Disponível em: <https://www.bitcointoyou.com/blog/criptomoedas/educacao-financeira/o-que-e-blockchain-como-funciona/>. Acesso em: 2 ago. 2024. Citado 2 vezes nas páginas 6 e 7.

IBP. *Número de incidentes cibernéticos significativos no mundo*. 2022. Disponível em: <https://www.ibp.org.br/observatorio-do-setor/snapshots/numero-de-incidentes-ciberneticos-significativos-no-mundo/>. Acesso em: 1 mar. 2024. Citado na página 4.

JUNIOR, J. H. G. T. *Gestão preditiva de ataques de negação de serviço em redes corporativas*. Tese (Doutorado), 2023. Citado na página 29.

KARAMITSOS, I. et al. Blockchain as a service (bcaas): a value modeling approach in the education business model. *Journal of Software Engineering and Applications*, Scientific Research Publishing, v. 15, n. 5, p. 165–182, 2022. Citado na página 15.

KUHN, A. d. S. B. P. et al. Implicações e desafios impostos à hegemonia do dólar americano pelas criptomoedas. Florianópolis, SC., 2022. Citado na página 25.

KUROSE, J. F.; ROSS, K. W. *Computer Networking: A Top-Down Approach*. Pearson Education, 2006. Disponível em: <https://www.pearson.com/store/p/computer-networking-a-top-down-approach/P100000775930>. Citado na página 16.

LARIMER, D. Delegated proof-of-stake (dpos). bitshare whitepaper (2014). *ed*, 2014. Citado na página 24.

LEVIS, D.; FONTANA, F.; UGHETTO, E. Uma olhada no futuro da tecnologia blockchain. *PLOS ONE*, Public Library of Science, San Francisco, CA, USA, v. 16, n. 11, p. e0258995, 2021. Citado na página 19.

LI, X. et al. An adaptive ddos detection and classification method in blockchain using an integrated multi-models. *Computers, Materials Continua*, 2023. Citado 2 vezes nas páginas 35 e 37.

LUCENA, A.; HENRIQUES, R. *Blockchain: A tecnologia que está transformando o mercado financeiro*. Editora Senac, 2016. Disponível em: <https://www.senacsp.edu.br>. Citado 2 vezes nas páginas 15 e 16.

MARTINS, D. F. G. et al. Um novo mecanismo de consenso probabilístico para blockchains públicas: A new probabilistic consensus mechanism for public blockchains. [sn], 2021. Citado na página 24.

MIRKOVIC, J.; REIHER, P. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, ACM New York, NY, USA, v. 34, n. 2, p. 39–53, 2004. Citado 2 vezes nas páginas 30 e 31.

MORAES, J. M. L. Ddshp: Um sistema para a detecção de ddos em iot baseado no parâmetro de hurst e sdn. 2023. Citado na página 28.

MOREIRA, C. V. C. *Os impactos da tecnologia Blockchain em auditorias*. Tese (Tese de Doutorado) — ISCAL, 2023. Citado 4 vezes nas páginas 1, 5, 8 e 9.

MOUGAYAR, W. *The business blockchain: promise, practice, and application of the next Internet technology*. [S.l.]: John Wiley & Sons, 2016. Citado na página 19.

MOURA, M. P. F. d. Mecanismo de detecção de ataques ddos na camada de aplicação. 2023. Citado na página 31.

MURTHY, C. V. B. et al. Cloud computing based on blockchain: architecture challenges and research. *IEEE Access*, IEEE, v. 8, p. 205190–205205, 2020. Citado 3 vezes nas páginas 19, 23 e 26.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Citado 3 vezes nas páginas 16, 17 e 24.

PEGORARO, D. R. *Blockchain*. [S.l.]: Editora Senac São Paulo, 2023. Citado na página 13.

PEREIRA, B. M. S. Dinâmica de sistemas aplicada à simulação de cenários na mineração de bitcoin. Universidade Federal de Santa Maria, 2025. Citado na página 25.

PRASEED, A.; THILAGAM, P. S. Ddos attacks at the application layer: Challenges and research perspectives for safeguarding web applications. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 1, p. 661–685, 2018. Citado 2 vezes nas páginas 31 e 32.

QURESHI, S. Denial of service (dos) attacks: Innovative cybersecurity solutions for effective attack prevention. 2024. Citado 2 vezes nas páginas 36 e 37.

RABADãO, C. M. d. S. *Cibersegurança: Programa, conteúdos e métodos de ensino-aprendizagem*. [S.l.: s.n.], 2021. Citado na página 2.

RIANDARI, F. et al. Dynamic optimization algorithms for enhancing blockchain network resilience against distribuited attacks. *Revista Internacional de Ciências Básicas e Aplicadas*, v. 13, n. 2, p. 96–111, 2024. Citado 2 vezes nas páginas 36 e 37.

RIBEIRO, M. A. Detectando e mitigando ataques ddos com a abordagem mtd com base na classificação de fluxo automatizada em redes sdn. 2022. Citado na página 29.

ROCIO, V. Microcredencial em transição e transformação digital. tecnologia blockchain: mecanismo do blockchain. 2022. Citado na página 19.

SALTIÉL, T. M. V. A tributação das criptomoedas no brasil: uma análise dos impostos. 2024. Citado na página 24.

SHAH, Z. et al. Distributed denial of service (ddos) mitigation using blockchain—a comprehensive insight. *Sensores*, MDPI, v. 22, n. 3, p. 1094, 2022. Citado 2 vezes nas páginas 35 e 37.

SILVA, A. D. O. B. da. *A implementação da tecnologia blockchain na esfera das Sociedades Comerciais*. Tese (Doutorado) — Universidade de Coimbra, 2024. Citado na página 21.

SILVEIRA, F. A. F. *Smart-IoT: um sistema de proteção contra DDoS para rede de Internet das Coisas*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, 2020. Citado na página 28.

SOUZA, G. T. et al. Aplicação da tecnologia blockchain na autenticidade de documentos. Pontifícia Universidade Católica de Goiás, 2024. Citado na página 12.

SWAN, M. *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015. Disponível em: <https://www.oreilly.com/library/view/blockchain-blueprint-for/9781491928490/>. Citado 2 vezes nas páginas 16 e 19.

TANEMBAUM, A. S. *Redes de Computadores. 3ª Edição. ed.* [S.l.]: São Paulo: Elsevier, 2003. Citado 2 vezes nas páginas 30 e 31.

TRASFERETTI, R.; MENTOR, R.; PINESCHI, C. *Blockchain para Iniciantes: desvende o mundo da blockchain em um guia prático da revolução tecnológica inovadora do século XXI*. [S.l.]: Editora Dialética, 2024. Citado na página 25.

TRIPATHI, N.; HUBBALLI, N. Application layer denial-of-service attacks and defense mechanisms: a survey. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 54, n. 4, p. 1–33, 2021. Citado 2 vezes nas páginas 31 e 32.

TSCHORSCH, F.; SCHEUERMANN, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, v. 18, n. 3, p. 2084–2123, 2016. Citado na página 22.

VAL, R. B. do. *Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT*. Tese (Doutorado) — Universidade Fernando Pessoa (Portugal), 2023. Citado na página 2.

VASCONCELOS, C. D. S. D. DetecÇÃo de ataques de negaÇÃo de serviÇo em internet das coisas com utilizaÇÃo de filtros sequenciais. 2022. Citado na página 29.

WANG, X. et al. Survey on blockchain for internet of things. *Computer Communications*, Elsevier, v. 136, p. 10–29, 2019. Citado 5 vezes nas páginas 20, 21, 26, 30 e 32.

WANI, S. et al. Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey. *Simetria*, MDPI, v. 13, n. 2, p. 227, 2021. Citado 2 vezes nas páginas 34 e 37.

ZADE, A. R.; PATIL, S. H. A survey on various defense mechanisms against application layer distributed denial of service attack. *International Journal on Computer Science and Engineering*, Citeseer, v. 3, n. 11, p. 3558, 2011. Citado na página 32.

ZARGAR, S. T.; JOSHI, J.; TIPPER, D. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE communications surveys & tutorials*, IEEE, v. 15, n. 4, p. 2046–2069, 2013. Citado na página 32.

ZHENG, Z. et al. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, v. 14, n. 4, p. 352–375, 2018. Citado na página 14.

ZHU, Y. *Classificação das carteiras na Blockchain Ethereum usando machine learning*. Dissertação (Mestrado) — Universidade de Lisboa (Portugal), 2023. Citado na página 22.