UNIVERSIDADE FEDERAL DO AMAZONAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA - PPGEE
CENTRO DE PD EM TECNOLOGIA ELETRÔNICA DA INFORMAÇÃO – CETELI

JONATHAS TAVARES NEVES

DESENVOLVIMENTO DE UMA MICRO-BLOCKCHAIN PRIVADA PARA COLETA DE DADOS DE DISPOSITIVOS IIOT

Manaus
2024

JONATHAS TAVARES NEVES

DESENVOLVIMENTO DE UMA MICRO-BLOCKCHAIN PRIVADA PARA COLETA DE DADOS DE DISPOSITIVOS IIOT

Projeto de dissertação apresentado ao Curso de Mestrado em Engenharia Elétrica, área de concentração Sistemas Inteligentes e Microeletrônica e linha de pesquisa Blockchain e Criptomoedas do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas.

Versão corrigida contendo as alterações solicitadas pela comissão julgadora em 14 de dezembro de 2023.

Orientador: Prof. Dr. Carlos Augusto de Moraes Cruz

Manaus

2024

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Neves, Jonathas Tavares
N518d Desenvolvimento de uma micro-blockchain privada para coleta de dados de dispositivos IIoT / Jonathas Tavares Neves . 2024
109 f.: il. color; 31 cm.

Orientador: Carlos Augusto de Moraes Cruz
Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Amazonas.

1. Micro-blockchain. 2. Internet industrial das coisas. 3. Protocolo mqtt. 4. Bitcoin Satoshi Vision. I. Cruz, Carlos Augusto de Moraes. II. Universidade Federal do Amazonas III. Título

Poder Executivo
Ministério da Educação
Universidade Federal do Amazonas
Faculdade de Tecnologia
Programa de Pós-graduação em Engenharia Elétrica

JONATHAS TAVARES NEVES

DESENVOLVIMENTO DE UMA MICRO-BLOCKCHAIN PRIVADA PARA COLETA DE DADOS DE DISPOSITIVOS IIOT

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Engenharia Elétrica na área de concentração Controle e Automação de Sistemas.

Aprovada em 28 de março de 2024.

BANCA EXAMINADORA

Prof. Dr. Carlos Augusto de Moraes Cruz
Presidente
Universidade Federal do Amazonas

Documento assinado digitalmente
gov.br MARIO SALVATIERRA JUNIOR
Data: 10/05/2024 16:46:41-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Mário Salvatierra Júnior, Membro
Universidade Federal do Amazonas

Documento assinado digitalmente
gov.br CELSO BARBOSA CARVALHO
Data: 16/05/2024 13:20:53-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Celso Barbosa Carvalho, Membro
Universidade Federal do Amazonas

PPGEE
Programa de Pós-Graduação em Engenharia Elétrica - UFAM

Pós-Graduação em Engenharia Elétrica.
Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Campus Universitário, Setor Norte - Coroado, Pavilhão do CETELI.
Fone/Fax (92) 99271-8954 Ramal:2607. E-mail: ppgee@ufam.edu.br

Aos meus pais Cleilton e Telma, minha namorada Jarlene e a todas as pessoas que, de alguma forma, tornaram esta jornada mais fácil e enriquecedora.

Agradecimentos

Agradeço inicialmente a D'us por conceder o fôlego de vida e a oportunidade de realizar esta jornada. Expresso minha gratidão à minha namorada Jarlene e aos meus pais, cujo apoio e estímulo foram fundamentais para que eu seguisse adiante. Reconheço o professor Dr. Carlos Augusto e todos os membros do grupo de pesquisa em blockchain pelo valioso suporte e orientação ao longo deste trabalho. Também sou grato ao Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) e ao Centro de P&D em Tecnologia Eletrônica da Informação (CETELI) pela disponibilização dos laboratórios e demais recursos essenciais para a realização desta pesquisa.

Resumo

NEVES, Jonathas Tavares. **Desenvolvimento de uma micro-blockchain privada para coleta de dados de dispositivos IIoT** 2024. 109 f. Dissertação (Mestrado em Engenharia Elétrica) – Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Amazonas, Manaus, 2024.

Este estudo aborda o desenvolvimento de uma micro-blockchain privada para a coleta de dados de dispositivos da Internet Industrial das Coisas (IIoT) utilizando microeletrônicos com funcionalidades similares. O DHT11 foi empregado como sensor de temperatura, enquanto o ESP32 WROOM foi utilizado como microcontrolador IIoT, demonstrando um desempenho superior ao Arduino Nano 33 IoT em aplicações IIoT. A pesquisa concentrou-se na segurança da comunicação de dados em ambientes fabris na camada de aplicação, levando em consideração a prevalência de ataques cibernéticos. Foi proposto um método que, apesar da necessidade de implementação manual de dados, apresentou resultados significativos em termos de funcionalidade e aplicabilidade. A transmissão de dados do protocolo MQTT em uma rede blockchain web3 provou ser segura contra ataques Man-in-the-Middle e DDoS. É importante ressaltar que as transações realizadas na micro-blockchain não envolvem o gasto de bitcoins. O estudo também explorou o uso do Proof of Work (PoW) na micro-blockchain para produzir o carimbo de data/hora da criação da chave privada. Foram identificadas limitações e sugeridas pesquisas futuras para automatizar o processo de implementação de dados. Diretrizes para trabalhos futuros foram propostas, incluindo a comunicação física cabeada e a restrição da troca de informação ao acesso de chaves privada e pública. Este estudo contribuiu para a literatura existente e abriu novas possibilidades para pesquisas futuras na integração segura de dispositivos IIoT em ambientes fabris.

Palavras-chaves: Micro-blockchain. Internet Industrial das Coisas (IIoT). Protocolo MQTT.

Abstract

NEVES, Jonathas Tavares. **Development of a private micro-blockchain for data collection from IIoT devices** 2024. 109 p. Dissertation (Master's in Electrical Engineering) – Graduate Program in Electrical Engineering, Federal University of Amazonas, Manaus, 2024.

This study addresses the development of a private micro-blockchain for data collection from Industrial Internet of Things (IIoT) devices using microelectronics with similar functionalities. The DHT11 was employed as a temperature sensor, while the ESP32 WROOM was used as an IIoT microcontroller, demonstrating superior performance to the Arduino Nano 33 IoT in IIoT applications. The research focused on the security of data communication in factory environments at the application layer, taking into account the prevalence of cyber attacks. A method was proposed that, despite the need for manual data implementation, showed significant results in terms of functionality and applicability. The transmission of MQTT protocol data on a web3 blockchain network proved to be secure against Man-in-the-Middle and DDoS attacks. It is important to note that transactions carried out on the micro-blockchain do not involve the expenditure of bitcoins. The study also explored the use of Proof of Work (PoW) in the micro-blockchain to produce the timestamp of the creation of the private key. Limitations were identified and future research was suggested to automate the data implementation process. Guidelines for future work were proposed, including wired physical communication and the restriction of information exchange to access to private and public keys. This study contributed to the existing literature and opened new possibilities for future research on the secure integration of IIoT devices in factory environments.

Keywords: Micro-blockchain. Industrial Internet of Things (IIoT). MQTT Protocol.

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

AGV	Automated Guided Vehicle
AMQP	Advanced Message Queuing Protocol
ARPANET	Advanced Research Projects Agency Network
BFT	Byzantine Fault Tolerance
Bitcoin-cli	Bitcoin Command Line Interface
CLPs	Controladores Lógicos Programáveis
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
DAG	Directed Acyclic Graph
DC	Direct Current
DApps	Decentralized Applications
DDoS	Distributed Denial of Service
DHT11	Digital Humidity and Temperature Sensor Module
DPoS	Delegated Proof of Stake
ECDSA	Elliptic Curve Digital Signature Algorithm
E-Ciber	Estratégia Nacional de Segurança Cibernética do Brasil
ELF	Executable and Linkable Format
ESP32 WROOM	ESP32 Wireless Real-time Onboard Operating Module
GE	General Electric
GND	Ground (or Ground Reference)
HTTP	Hypertext Transfer Protocol

IIC	Industrial Internet Consortium
IDE	Integrated Development Environment
IIoT	Industrial Internet of Things
IOTA	Internet of Things Application
IPCs	Industrial Personal Computers
LoRa	Long Range
MDIoTSP	Mobile Device Internet of Things Security Protocol
MITM	Man-in-the-Middle
Modbus	Modicon Communication Protocol
MQTT	Message Queuing Telemetry Transport
MTConnect	Manufacturing Technology Protocol
NIST	National Institute of Standards and Technology
OPC-UA	Open Platform Communications Unified Architecture
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoB	Proof of Burn
PoC	Proof of Capacity
PoI	Proof of Importance
PoS	Proof of Stake
PoSpace	Proof of Space
PoW	Proof of Work
PROFINET	Process Field Network
RPC	Remote Procedure Call

SHA-256	Secure Hash Algorithm 256-bit
SoC	Sistemas em Chip
TCP/IP	Transmission Control Protocol/Internet Protocol
TPS	Transactions Per Second
TTP	Trusted Third Party
TxID	Transaction ID
UTXOs	Unspent Transaction Outputs
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WiFi	Wireless Fidelity
WIF	Wallet Import Format
WSL2	Windows Subsystem for Linux 2

Sumário

[1] De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

1 INTRODUÇÃO

Na era digital contemporânea, a Internet das Coisas Industrial (IIoT) representa uma mudança substancial na operação de fábricas e sistemas industriais. A IIoT, simplificadamente, engloba a interconexão de maquinários e dispositivos industriais à internet, facilitando a comunicação mútua e com sistemas gerenciais. Essa interligação possibilita a coleta e análise de dados em tempo real, promovendo a otimização da eficiência e produtividade. No entanto, apesar dos benefícios evidentes, a IIoT também enfrenta desafios consideráveis, especialmente no que diz respeito à segurança dos dados transmitidos.

A comunicação interna na IIoT demanda equipamentos de hardware compatíveis com diversas topologias de redes de comunicação, destacando-se aquelas que utilizam transmissão sem fio. A implementação dessa metodologia proporciona a vantagem de monitorar e controlar múltiplos ambientes. Nesse contexto, o hardware local, englobando máquinas, sensores, atuadores, computadores e outros dispositivos eletrônicos, emite um sinal para o hardware responsável pela topologia de comunicação, que por sua vez o retransmite para um hardware de destino. Esse processo contribui para mitigar situações em que ambientes específicos possam representar riscos à saúde do operador.

Em relação aos hardwares de diferentes níveis da pirâmide da automação, diversas estruturas são empregadas para a transmissão de dados coletados em campo para os demais níveis. Mesmo quando a transmissão é realizada sem cabos, são aplicados diversos protocolos e interfaces. Dessa forma, a segurança dos dados fica condicionada ao nível de proteção do hardware em questão, evidenciando que a segurança está limitada à capacidade do dispositivo intermediário de resistir à exposição.

A proteção de dados contra ataques cibernéticos figura como um dos desafios mais significativos na era digital, sendo crucial assegurar o acesso apenas a indivíduos autorizados. Em ambientes industriais, onde todas as máquinas estão interligadas, a presença de um único ponto vulnerável na segurança pode comprometer a integridade do sistema como um todo.

Nesse contexto, a tecnologia blockchain emerge como uma solução inovadora, reconhecida por sua capacidade de garantir a segurança e integridade dos dados. Operando por meio de um sistema de registros distribuídos e criptografados, a blockchain oferece

uma robusta barreira contra invasões e manipulações não autorizadas, representando assim um avanço significativo na proteção de dados contra ameaças cibernéticas.

Uma das principais abordagens do uso de blockchains em sistemas industriais foi relatada por Gimenez-Aguilar et al.(1) (2021) em seu artigo "*Achieving cybersecurity in blockchain-based systems: A survey*". Nesse trabalho, foram avaliados manuscritos acadêmicos ao longo de 8 anos quanto a abordagens industriais existentes. Foi evidenciado que a blockchain é uma tecnologia habilitadora que está pavimentando o caminho para serviços mais inteligentes e enriquecidos. Como resultado, alguns locais de pesquisa que permanecem inexplorados foram identificados. Além disso, foi constatado que as propostas industriais geralmente omitem detalhes críticos em suas abordagens. Outro fato preocupante é que há uma fração de trabalhos acadêmicos que estão usando blockchain desconsiderando (ou pelo menos não fornecendo evidências de satisfação de) todos os princípios que justificam seu uso. Para fomentar trabalhos futuros nesta direção, um conjunto de questões em aberto foi identificado, muitos desses trabalhos só observam uma aplicação específica de blockchain (Etherum) não abordando outras características como a escalabilidade de blockchains mais tradicionais (Bitcoin Satoshi Vision).

Em outro estudo que aborda a aplicação de blockchain com dispositivos IIoT, Li et al.(2) (2018) apresentaram "*A Blockchain-Based Authentication and Security Mechanism for IoT*". Neste artigo, são analisadas as desvantagens do IoT tradicional na autenticação de identidade e proteção de segurança. Propõe-se um modelo baseado em blockchain para autenticação IoT e proteção de segurança. Esse modelo tem como objetivo prevenir a intrusão de nós maliciosos, resistir a ataques DDoS e prevenir a porta dos fundos do firmware. Contudo, não aborda aspectos de protocolos mais viciosos como o MQTT (*Message Queuing Telemetry Transport*). Em suma, a blockchain é um sistema de registro distribuído que armazena dados em blocos encadeados, que são protegidos por criptografia e validados por consenso. A blockchain é um sistema descentralizado, que não depende de uma autoridade central, mas de uma rede de participantes que mantêm uma cópia do registro completo. A blockchain é um sistema imutável, que torna virtualmente impossível alterar ou adulterar as transações passadas. A blockchain é um sistema transparente, que permite a verificação e o compartilhamento de dados entre os participantes. A blockchain é um sistema confiável, que garante a segurança e a integridade dos dados. A blockchain é um sistema versátil, que pode ser aplicado em diferentes domínios e contextos, como a IIoT.

A blockchain é uma tecnologia inovadora, que tem o potencial de transformar diversos setores e indústrias. A presente dissertação de mestrado tem como objetivo a investigação da combinação da Internet das Coisas Industrial (IIoT) com uma modalidade específica de blockchain, denominada micro-blockchain privada. Esta combinação é proposta como uma solução para os desafios de segurança de dados enfrentados pelo setor industrial. Para tanto, será realizada uma análise minuciosa dos desafios existentes e das soluções propostas, bem como a proposição de um sistema baseado em micro-blockchain privada para a coleta de dados de dispositivos IIoT. Este estudo tem como meta contribuir para o entendimento e o desenvolvimento de estratégias robustas e adaptáveis que permitam a implementação segura e eficiente da IIoT com o suporte da blockchain. Adicionalmente, busca-se investigar os benefícios e as limitações das blockchains privadas em cenários industriais, fornecendo insights valiosos para profissionais e pesquisadores que buscam aprimorar as operações da IIoT. Através desta pesquisa, espera-se contribuir significativamente para o campo de estudo, auxiliando na superação dos desafios de segurança de dados na indústria.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver e avaliar um sistema de segurança para a transmissão de dados de temperatura e umidade em uma rede de dispositivos da Internet Industrial das Coisas (IIoT) utilizando o protocolo MQTT e a tecnologia de micro-blockchain para garantir a integridade e a confiabilidade dos dados transmitidos.

1.1.2 Objetivos Específicos

- Realizar uma revisão abrangente da literatura sobre as ameaças cibernéticas que a IIoT enfrenta e as soluções de segurança propostas;
- Avaliar a funcionalidade da tecnologia blockchain privada e sua aplicabilidade na mitigação de ameaças cibernéticas em sistemas IIoT;

- Projetar e implementar um ambiente de teste que simule uma rede IIoT integrada com uma blockchain privada, a fim de avaliar a eficácia da solução proposta;
- Coletar dados e métricas relevantes durante os experimentos para quantificar as melhorias na segurança e confiabilidade obtidas pela integração da blockchain privada;
- Analisar os resultados dos experimentos e fornecer insights sobre os benefícios e as limitações do uso da blockchain privada em cenários industriais IIoT;
- Propor diretrizes e recomendações para a implementação segura e eficiente de sistemas IIoT com o apoio da tecnologia blockchain privada, visando contribuir para o avanço nesta área de pesquisa e sua aplicação prática em ambientes industriais.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em seis capítulos, conforme descrito a seguir:

- Capítulo 1: Introdução;
- Capítulo 2: Revisão da Literatura;
- Capítulo 3: Referencial Teórico;
- Capítulo 4: Materiais e Métodos;
- Capítulo 5: Resultados preliminares;
- Capítulo 6: Conclusão;
- Capítulo 7: Trabalhos Futuros.

O Capítulo 1 introduz o contexto e a motivação da pesquisa, discutindo a demanda crescente por dispositivos da Internet das Coisas (IoT) na indústria, categorizados como Internet Industrial das Coisas (IIoT). Aborda-se os riscos potenciais de ataques cibernéticos aos quais esses dispositivos podem estar sujeitos, as estratégias para estabelecer uma arquitetura mais segura e os objetivos gerais e específicos desta pesquisa.

O Capítulo 2 oferece uma revisão sistemática da literatura, focando em estudos que se relacionam com a aplicação de IIoT e Cibersegurança, bem como pesquisas que utilizam blockchains privadas para garantir a segurança em seus sistemas. Realiza-se uma análise criteriosa dos métodos existentes na literatura, destacando suas forças, fraquezas, limitações e desafios.

O Capítulo 3 introduz os fundamentos teóricos das técnicas empregadas nesta pesquisa, incluindo blockchain privada, IIoT e computação em névoa. Clarifica-se os conceitos, as características distintivas, os benefícios e os desafios associados a cada técnica. Além disso, discutem-se suas aplicações práticas e fornecem-se exemplos ilustrativos.

O Capítulo 4 detalha os materiais e métodos empregados nesta pesquisa, abordando as características do hardware mínimo necessário e os detalhes da metodologia proposta. Apresentam-se os cenários, parâmetros, métricas e ferramentas utilizadas nos experimentos. Adicionalmente, fornece-se o modelo do trabalho proposto ilustrando o processo de coleta, processamento e análise dos dados.

O Capítulo 5 apresenta os resultados obtidos e promove uma discussão aprofundada sobre eles. Exibem-se tabelas comparativas e imagens que demonstram o progresso da presente pesquisa em sua área específica. Além disso, realiza-se uma análise desses dados, empregando técnicas de avaliação qualitativa comparativa.

O Capítulo 6 descreve as principais conclusões obtidas no desenvolvimento e análise simulada comparativa da presente pesquisa para a proposta do tema. Abordam-se os desafios superados e as percepções para outras aplicações.

O Capítulo 7 aborda os trabalhos futuros relacionados ao tema, apresentando melhorias com aspectos da automação da coleta e tratamento dos dados.

2 REVISÃO DA LITERATURA

Neste capítulo, realiza-se uma revisão abrangente e meticulosa da literatura que serve como base teórica e metodológica para a proposta deste trabalho de dissertação. A literatura é organizada em três grupos temáticos, de acordo com os focos das soluções apresentadas.

No primeiro grupo, examinam-se os artigos dedicados à avaliação de ataques (ameaças) e riscos cibernéticos associados aos ambientes IIoT. Esta análise prova ser essencial para identificar pontos críticos que exigem melhorias na pesquisa, bem como para delimitar o problema e os objetivos do estudo.

No segundo grupo, exploram-se as possíveis aplicações da tecnologia blockchain em ambientes industriais que contam com componentes IoT. Neste contexto, investiga-se como a tecnologia blockchain pode ser implementada de forma eficiente e segura, considerando as hipóteses propostas no Capítulo 1, que são: (A) a utilização de uma blockchain privada para garantir a integridade e a confidencialidade dos dados gerados pelos dispositivos IIoT; (B) a utilização de uma computação em névoa para distribuir e processar os dados de forma descentralizada e escalável; (C) a utilização de um protocolo de consenso adaptativo para manter a sincronização e a validação dos blocos na rede. Além disso, analisam-se as vantagens e desvantagens de diferentes tipos de blockchain, como pública, privada e híbrida, para a gestão de dados em ambientes IIoT. Uma blockchain pública é aquela que permite a participação de qualquer pessoa na rede, sem a necessidade de autorização ou identificação. Uma blockchain privada é aquela que restringe o acesso à rede a um grupo limitado de participantes, que devem ser autorizados e identificados. Uma blockchain híbrida é aquela que combina elementos de ambos os tipos, permitindo a interoperabilidade entre redes públicas e privadas.

No terceiro grupo, define-se o conceito de micro-blockchain, que é a base da proposta de solução para as ameaças cibernéticas em ambientes IIoT. Uma micro-blockchain é uma blockchain privada que opera em um nível local, conectando um conjunto de dispositivos IIoT que compartilham dados e recursos. As principais características de uma micro-blockchain são: (A) a utilização de um algoritmo de consenso leve e eficiente, que não depende de alto poder computacional ou de incentivos econômicos; (B) a utilização de um mecanismo de autenticação e criptografia robusto, que garante a segurança e a privacidade

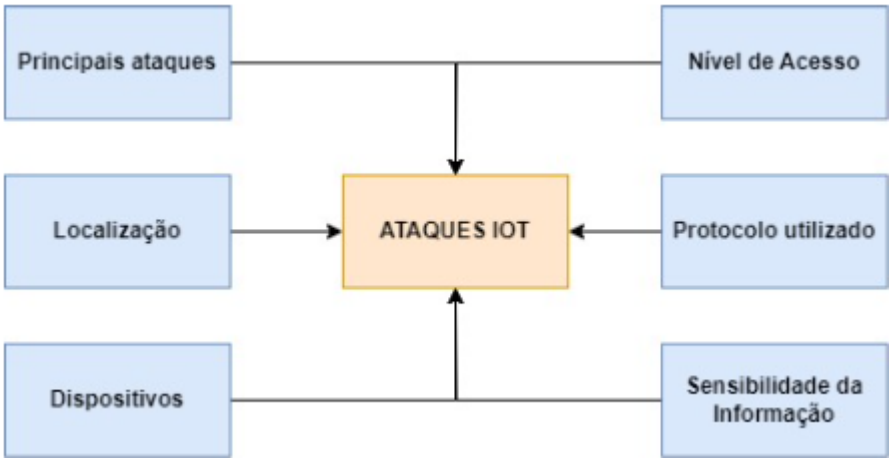
dos dados; (C) a utilização de um protocolo de comunicação flexível e dinâmico, que permite a adaptação às mudanças de topologia e de demanda da rede. As principais vantagens de uma micro-blockchain são: (A) a redução da latência e do consumo de energia, ao evitar a transmissão de dados desnecessários ou redundantes; (B) o aumento da confiabilidade e da disponibilidade, ao evitar a dependência de um servidor central ou de uma rede externa; (C) o aumento da escalabilidade e da modularidade, ao permitir a criação e a integração de múltiplas micro-blockchains. As principais desafios de uma micro-blockchain são: (A) a garantia da consistência e da integridade dos dados, ao lidar com possíveis conflitos ou falhas na rede; (B) a garantia da segurança e da privacidade dos dados, ao lidar com possíveis ataques ou intrusões na rede; (C) a garantia da interoperabilidade e da compatibilidade dos dados, ao lidar com possíveis diferenças ou incompatibilidades entre as micro-blockchains. As aplicações e exemplos de micro-blockchain na literatura são: (A) o trabalho de Zhang, Wu e Wang(3) (2020), que propõe uma micro-blockchain para a gestão de energia em uma rede de veículos elétricos; (B) o trabalho de Antoniadis, Kontsas e Spinthiropoulos(4) (2019), que propõe uma micro-blockchain para a rastreabilidade de alimentos em uma cadeia de suprimentos; (C) o trabalho de Chang e Chen(5) (2020), que propõe uma micro-blockchain para a monitorização de saúde em uma rede de sensores corporais.

Essa organização meticulosa da literatura fornece uma base sólida e consistente para a construção do conhecimento e o suporte da pesquisa desenvolvida no contexto da investigação sobre micro-blockchain e IIoT.

2.1 ANÁLISE DOS TRABALHOS DO GRUPO 1

2.1.1 *Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics*

Figura 1 – Arquitetura e taxonomia da cibersegurança IoT



Fonte: Jonathas Neves, 2024

O artigo de Lu e Xu(6) (2018) explora o panorama da cibersegurança no contexto da Internet das Coisas (IoT), tecnologia emergente que proporciona benefícios significativos para diversos setores e aplicações, incluindo indústria, saúde, transporte e agricultura. Contudo, a implementação da IoT apresenta desafios de segurança substanciais, uma vez que os dispositivos e as comunicações estão expostos a ataques cibernéticos, comprometendo potencialmente a confidencialidade, integridade, disponibilidade, escalabilidade e interoperabilidade dos dados e serviços. Nesse sentido, o estudo em questão oferece uma revisão sistemática e abrangente da cibersegurança na IoT. Para tanto, discutem-se as principais vulnerabilidades, ameaças e riscos que afetam os dispositivos IoT, as diferentes tecnologias de comunicação sem fio empregadas para a transmissão de dados, as melhores práticas e recomendações para assegurar a segurança dos sistemas IoT e as aplicações industriais mais relevantes que utilizam a IoT, como a indústria 4.0, a saúde inteligente e a cidade inteligente. As camadas de sensoriamento (física e enlace de dados), rede, intermediária (sessão e transporte) e aplicação são suscetíveis a diversos tipos de ataques, conforme descritos a seguir:

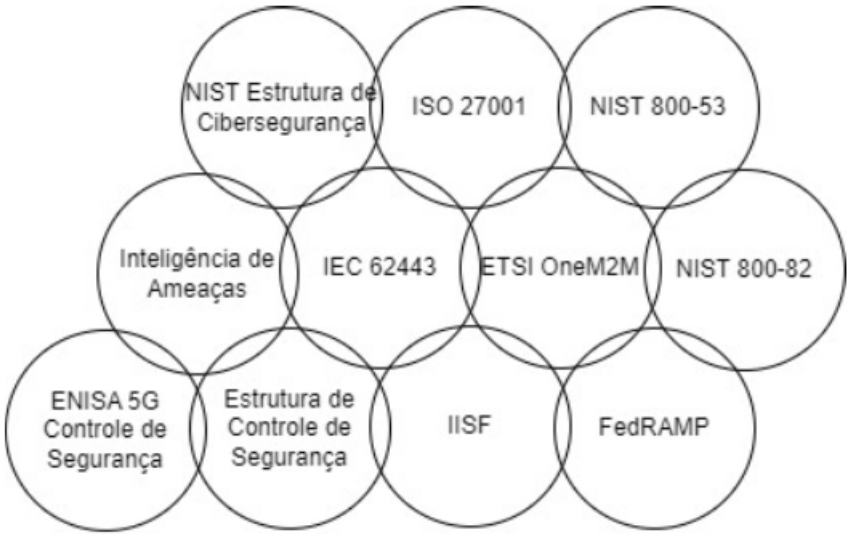
- Camada de sensoriamento: repetição, temporais, captura de nó e canal lateral;

- Camada de rede: homem-no-meio, *spoofing*, modificação, repetição e *Sybil*;
- Camada intermediária: ataques maliciosos internos, ataques subjacentes e ataques de relacionamento com terceiros;
- Camada de aplicação: *phishing*, injeção de *malware* e acesso não autorizado.

Ademais, destacam-se as tendências atuais de pesquisa e os desafios emergentes neste campo em rápida evolução. Por fim, apresenta-se a proposta do autor para uma arquitetura e taxonomia da cibersegurança da IoT, conforme ilustrado na 1.

2.1.2 *Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap*

Figura 2 – Roteiro unificado de padrões IIoT



Fonte: Jonathas Neves, 2024

O estudo desenvolvido por Dhirani, Armstrong e Newe(7) (2021) enfatiza a importância da crescente implementação da Internet Industrial das Coisas (IIoT) na otimização dos processos de fabricação. A IIoT, uma abordagem inovadora, envolve a conexão de dispositivos, máquinas, sensores e sistemas industriais por meio de redes sem fio, permitindo a coleta, processamento e análise de dados em tempo real. No entanto, como uma tecnologia emergente, a transição para um modelo vertical totalmente conectado apresenta desafios significativos em termos de segurança cibernética e interoperabilidade.

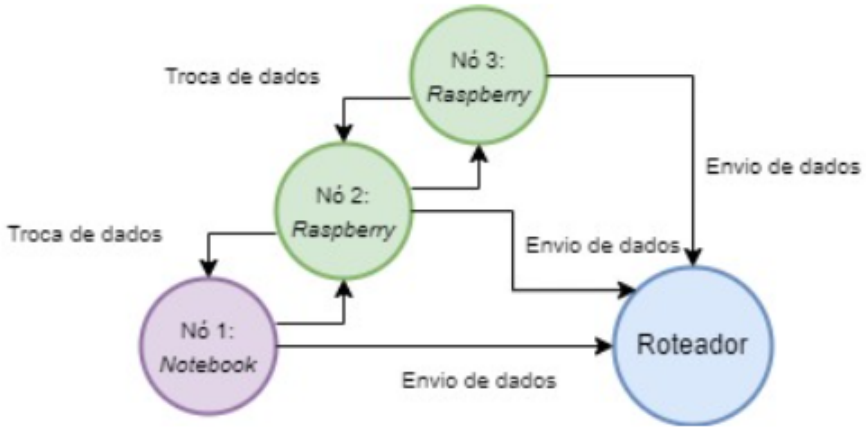
A ausência de métodos para avaliar o impacto das vulnerabilidades que podem ser exploradas por atores maliciosos é uma preocupação notável. Portanto, este estudo aborda o desenvolvimento de um projeto de cibersegurança para a Indústria 4.0. São compartilhados insights sobre a compreensão de padrões de cibersegurança que integram diferentes domínios e camadas da IIoT, revisão das melhores práticas e o fornecimento de um roteiro para a implementação de padrões e estratégias de cibersegurança adequados para garantir as comunicações entre os dispositivos e as máquinas na IIoT.

Assim, a pesquisa contribui para o aprimoramento da segurança, eficiência e competitividade dos sistemas industriais que se baseiam na IIoT. Isso é evidenciado pelo uso de medidas de segurança robustas, como a criptografia, na proteção da comunicação de dados. Finalmente, propõe-se um roteiro unificado para a implementação de padrões de segurança na IIoT, conforme ilustrado na 2.

2.2 ANÁLISE DOS TRABALHOS DO GRUPO 2

2.2.1 *An experimental study on performance of private blockchain in IoT applications*

Figura 3 – Blockchain privada integrada com dispositivos IoT



Fonte: Jonathas Neves, 2024

O artigo de Chen, Nguyen e Sekiya(8) (2021) tem como objetivo investigar o desempenho da tecnologia blockchain, com ênfase na plataforma Ethereum, em cenários de Internet das Coisas (IoT) que empregam redes privadas para assegurar a integridade dos

dados. A blockchain é uma tecnologia que viabiliza a criação de um registro distribuído e imutável de transações, as quais são agrupadas em blocos e validadas por meio de um protocolo de consenso. A plataforma Ethereum, por sua vez, é reconhecida por suportar a execução de contratos inteligentes, os quais consistem em programas autônomos que estabelecem as regras e condições das transações.

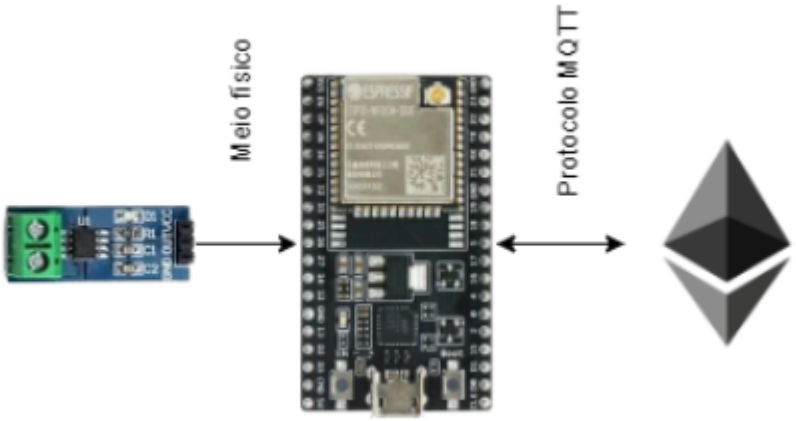
A IoT representa uma tecnologia que possibilita a interconexão de dispositivos, sensores e sistemas por meio da internet, permitindo a geração e troca de dados em tempo real. Diante desse contexto, este estudo experimental propõe-se a investigar uma variedade de parâmetros de desempenho em redes privadas baseadas na Ethereum. São detalhados os processos de latência de acordo com o ciclo de vida da transação, incluindo o tempo necessário para o envio, recebimento, processamento e confirmação de uma transação na rede. A latência é categorizada em dois tipos: a latência orientada à transação, que refere-se ao tempo necessário para a confirmação de uma transação individual, e a latência orientada ao bloco, que diz respeito ao tempo necessário para a confirmação de um bloco inteiro de transações.

Além disso, o estudo monitora e relata o desempenho dos nós da blockchain durante os processos de utilização da transação. Os nós da blockchain são os participantes da rede responsáveis por armazenar, validar e propagar os blocos e as transações. As redes utilizadas neste estudo experimental incluem uma rede interna de blockchain IoT, composta por um laptop e diversos computadores de placa única Raspberry Pi 3b+ (RPI 3b+), e uma blockchain privada hospedada na nuvem. Em ambos os casos, é desenvolvido e implantado um contrato inteligente para leitura e escrita de dados na blockchain, sendo o desempenho medido em diversos cenários.

Os resultados obtidos no experimento revelam não apenas o desempenho dos nós da blockchain, mas também a correlação entre latências e o número de saltos (hops), bem como a relação entre as latências em diferentes cargas de trabalho. Assim, este estudo contribui para a avaliação e otimização da tecnologia blockchain em aplicações de IoT que exigem segurança e eficiência. Uma das recomendações destacadas pelo estudo é que a implantação de blockchain mostra-se consideravelmente demandante para dispositivos IoT. Por fim, é apresentada a proposta para uma rede de blockchain privada integrada com dispositivos IoT, conforme ilustrado na 3.

2.2.2 *Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol*

Figura 4 – Blockchain privada com ESP32 IoT



Fonte: Jonathas Neves, 2024

O estudo desenvolvido por Baig et al.(9) (2021) introduz uma plataforma de negociação de energia *peer-to-peer* (P2P) baseada em código aberto, concebida para facilitar a troca de energia entre pares. A plataforma proposta é capaz de adquirir, monitorar e controlar energia autogerada em locais remotos em tempo real.

As transações são conduzidas através de uma interface web que emprega uma blockchain Ethereum privada. Um contrato inteligente é implantado nesta blockchain para registrar as atividades de negociação executadas na interface web, garantindo a integridade e a imutabilidade das transações.

A plataforma utiliza a tecnologia da Internet das Coisas (IoT) para monitorar e controlar a energia autogerada. Os dados de energia são coletados e processados por microcontroladores ESP32-S2, que estão conectados à fonte de tensão e à carga através de dispositivos de instrumentação de campo.

O sistema proposto, que incorpora uma arquitetura de blockchain e IoT, implementa um sistema de negociação de energia P2P descentralizado. A configuração de hardware inclui um relé, um sensor de corrente, um sensor de tensão, um roteador Wi-Fi e um microcontrolador ESP32-S2.

A transferência de dados é realizada utilizando o protocolo *Message Queuing Telemetry Transport* (MQTT) em uma rede local. O ESP32-S2 é configurado como cliente MQTT, enquanto o servidor IoT Node-Red atua como corretor MQTT.

Métodos de solicitação HTTP são implementados para conectar o servidor Node-Red à interface web, que foi desenvolvida usando a biblioteca React.JS. A 4 ilustra a composição básica e resumida dos sistemas de comunicação.

2.3 ANÁLISE DOS TRABALHOS DO GRUPO 3

2.3.1 *IoT Micro-Blockchain Fundamentals*

O trabalho de Anagnostakis et al.(10) (2021) aborda a funcionalidade mínima essencial de uma blockchain autônoma, bem como o hardware e software necessários para apoiá-la em microescala no contexto da Internet das Coisas (IoT). A blockchain é uma tecnologia que possibilita a criação de um registro distribuído e imutável de transações, agrupadas em blocos e validadas por meio de um protocolo de consenso. O IoT é uma tecnologia que facilita a conexão de dispositivos, sensores e sistemas através da internet, permitindo a geração e troca de dados em tempo real.

O estudo destaca a aplicação de operações profundas de blockchain na atividade de nível inferior do ecossistema IoT. Para isso, são discutidas a configuração e operação de mecanismos de blockchain de nível de bit em elementos mínimos de IoT, como interruptores inteligentes e sensores ativos. Um protocolo denominado "Testemunha" é empregado para estabelecer a funcionalidade mínima essencial do micro-blockchain. Este protocolo consiste em um algoritmo que permite aos dispositivos IoT testemunharem e validarem as transações uns dos outros, sem a necessidade de uma autoridade central ou de uma rede externa.

Dessa forma, o protocolo foi desenvolvido e instalado em uma rede autônoma ad-hoc de microdispositivos IoT, especificamente, Arduino Nano 33 IoT. Estes são pequenos computadores de baixo custo e alto desempenho. A configuração foi testada e avaliada em termos de necessidades computacionais, eficiência e resistência contra ataques maliciosos.

Os resultados deste trabalho indicam que as redes de micro-blockchain totalmente autônomas e privadas são viáveis no mundo do *smart dust*. Este termo se refere a dispositivos

IoT extremamente pequenos e dispersos, que podem formar redes sem fio e interagir com o ambiente, utilizando as capacidades dos dispositivos IoT de baixo custo existentes.

Por fim, o autor apresenta uma proposta para a comunicação do protocolo Testemunha.

2.3.2 *A Hierarchical Sharding Protocol for multi-domain IoT Blockchains*

O artigo de Tong et al.(11) (2019) apresenta um protocolo denominado MDIoTSP, concebido para blockchains de Internet das Coisas (IoT) multi-domínio. O estudo inicia-se com a ênfase na relevância do IoT em diversas indústrias e como a tecnologia blockchain pode abordar desafios, tais como gerenciamento de dados e segurança em sistemas IoT multi-domínio. O artigo discute as limitações dos sistemas de blockchain existentes em lidar com a taxa de transações necessária por sistemas IoT multi-domínio e propõe o MDIoTSP como uma solução. O protocolo MDIoTSP divide a blockchain em shards menores, cada um correspondendo a um domínio no sistema IoT. Utiliza-se um mecanismo de consenso baseado no protocolo *Practical Byzantine Fault Tolerance* (PBFT) para alcançar o consenso dentro de cada *shard* e no *shard* principal. O artigo compara o MDIoTSP com outros protocolos de *shard* existentes, destacando suas vantagens em termos de escalabilidade e adequação para sistemas IoT com recursos limitados. Adicionalmente, é apresentado um estudo de caso de implementação do MDIoTSP em um aplicativo IoT específico e é descrita a arquitetura do sistema *MicrothingsChains*, que implementa o protocolo MDIoTSP. O artigo detalha o design do MDIoTSP, incluindo formação de *shards*, configuração de overlay para shards, consenso intra-shard usando PBFT e transmissão de consenso final para mesclar sub-blocos em uma blockchain completa. Também são discutidos experimentos e resultados, comparando o desempenho do *MicrothingsChains* com o protocolo Elástico em termos de taxa de consenso de transações. Em suma, o MDIoTSP visa abordar os requisitos específicos e desafios dos sistemas IoT multi-domínio, aproveitando técnicas de *shard* e mecanismos de consenso adaptados ao ambiente IoT. A taxa de transferência de consenso de transação aumenta quase linearmente com o número de fragmentos.

Tabela 1 – Síntese da revisão bibliográfica apresentada no capítulo 2

Artigo	**Foco da área de pesquisa**	**Principal conclusão**	**Aplicação no presente trabalho de dissertação**	**Ponto a explorar no presente trabalho de dissertação**
Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics	Sistemas de segurança cibernética para dispositivos IoT	Identificação dos Tópicos de Pesquisa Atuais	Embasamento Teórico sobre Segurança Cibernética em Sistemas IoT	Aplicação de blockchain como sistema de cibersegurança
Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap	Sistemas de segurança cibernética para dispositivos IoT	Avaliação do Panorama de Ameaças e Normas	Diretrizes para Implementação de Padrões de Segurança em Sistemas IoT	Aplicação de blockchain como sistema de cibersegurança
An experimental study on performance of private blockchain in IoT applications	Aplicação de blockchain para segurança cibernética de dispositivos IoT	Análise do Desempenho de Blockchain Privado em Aplicações IoT	Avaliar a Eficácia da Implementação de Blockchain Privado em Dispositivos IoT	Aplicação de blockchain específica (privada) para IIoT
Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol	Aplicação de blockchain para segurança cibernética de dispositivos IoT	Desenvolvimento de uma Plataforma de Negociação de Energia Peer-to-Peer Baseada em IoT e Blockchain de Código Aberto	Implementação Prática de Blockchain em Transações que utilizam o Protocolo MQTT	Aplicação de blockchain específica para IIoT combinada ao protocolo MQTT
IoT Micro-Blockchain Fundamentals	Blockchains dedicadas à aplicações IoT	Exploração dos Fundamentos de Micro-Blockchains para IoT	Investigação de Protocolos de Consenso e Estruturas de Dados Específicas para Implementações em Ambientes IoT	Aplicação de micro-blockchains específicas para IIoT
A Hierarchical Sharding Protocol for multi-domain IoT Blockchains	Blockchains dedicadas à aplicações IoT	Proposta de Protocolo de Shard Hierárquico para Blockchains IoT Multidomínio	Implementação de Sharding em Blockchains IoT para Escalonamento e Eficiência	Aplicação de micro-blockchains específicas para IIoT

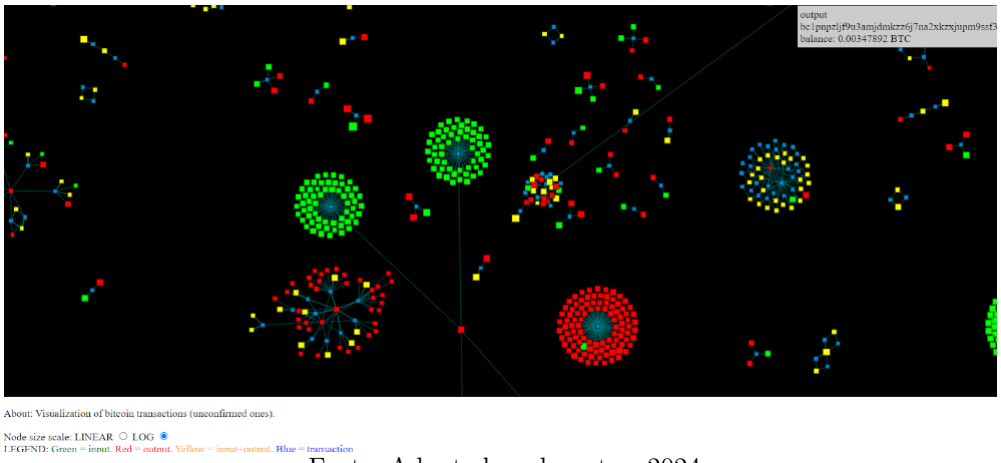
Fonte: Autor, 2024.

3 REFERENCIAL TEÓRICO

3.1 BLOCKCHAIN: CONCEITOS

A blockchain é uma tecnologia revolucionária que teve sua origem com a proposta do Bitcoin em 2008, conforme descrito em um artigo intitulado “Bitcoin: A peer-to-peer electronic cash system” por um autor anônimo conhecido como Satoshi Nakamoto. Esta tecnologia é essencialmente um registro distribuído que emprega criptografia e consenso para validar transações em uma rede descentralizada. Embora o Bitcoin, a primeira criptomoeda baseada em blockchain, tenha enfrentado desafios devido à sua volatilidade e complexidade, o potencial da blockchain como uma plataforma para outras aplicações rapidamente chamou a atenção de vários setores Laurence(12) (2023).

Figura 5 – Estrutura da rede de comunicação descentralizada de uma blockchain



Fonte: Adaptada pelo autor, 2024

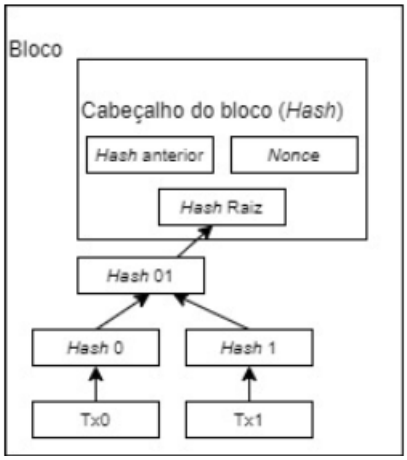
3.1.1 Conceitos básicos de blockchain

A arquitetura da blockchain é uma solução robusta que possibilita a gestão e o armazenamento descentralizados de dados. Essa arquitetura é composta por vários elementos, sendo o bloco o seu componente básico. Um bloco é formado por um cabeçalho e um conjunto de dados. O cabeçalho contém metadados sobre o bloco, tais como o número do bloco, o carimbo de tempo, o hash do bloco anterior e o hash do bloco atual, que são essenciais para garantir a integridade e a ordem dos dados, funcionando como identificadores únicos. Na seção de dados, há espaço para armazenar informações específicas,

que dependem da aplicação da blockchain, podendo incluir transações financeiras, contratos inteligentes ou outros tipos de registros.

a) Bloco

Figura 6 – Representação da arquitetura de um bloco de uma blockchain

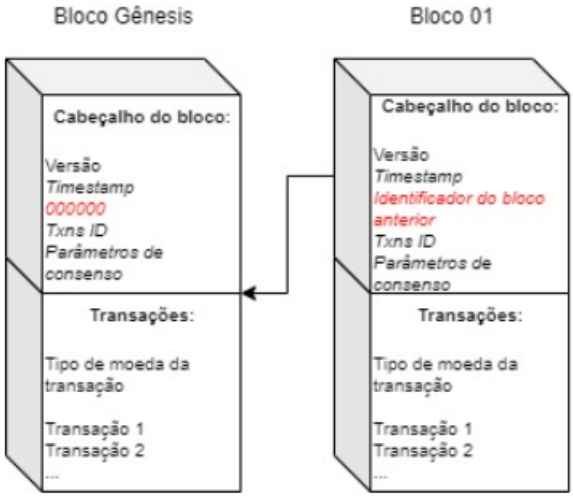


Fonte: Adaptada pelo autor, 2024

O conceito de blocos encadeados é fundamental para a segurança e imutabilidade da blockchain. Cada novo bloco é conectado ao anterior por meio de seu hash, criando uma sequência linear e contínua de informações. Isso significa que qualquer alteração feita em um bloco anterior resultaria na mudança de seu hash, afetando os hashes subsequentes e tornando facilmente perceptível qualquer tipo de adulteração nos dados. Assim, a estrutura em bloco garante que uma vez que os dados são registrados na blockchain, eles se tornam praticamente imutáveis, promovendo a confiança e a transparência nas transações registradas Gupta e Sadoghi(13) (2021).

b) Bloco gênesis

Figura 7 – Representação da arquitetura de um bloco de uma blockchain identificado o bloco gênesis



Fonte: Adaptada pelo autor, 2024

O bloco gênesis, também conhecido como o bloco inicial, é o alicerce de uma blockchain, sendo o primeiro bloco em uma cadeia de blocos interligados. Este bloco é singular e distinto, pois simboliza o início da trajetória de toda a rede. O bloco gênesis é crucial, pois estabelece os princípios fundamentais para a estrutura e operação da blockchain Hillmann et al.(14) (2020). Normalmente, o bloco gênesis é gerado no momento do lançamento inicial da blockchain. Ele se diferencia dos blocos subsequentes de diversas maneiras: seu número de bloco pode ser zero ou um, dependendo da convenção de numeração adotada, e sua estrutura pode ser distinta em relação aos outros blocos. Por exemplo, enquanto os blocos regulares contêm dados de transações efetivas, o bloco gênesis pode conter informações específicas sobre a configuração inicial da blockchain, tais como parâmetros do sistema, o protocolo empregado, a identidade do criador e possíveis declarações iniciais ou mensagens simbólicas. Ademais, o bloco gênesis não é gerado por meio de mineração ou validação de transações, como ocorre com os demais blocos. Ele é geralmente pré-configurado ou pré-gerado antes do lançamento da blockchain. Sua principal finalidade é estabelecer um ponto de partida comum para todos os nós da rede, garantindo a consistência e a integridade dos dados desde o início Read(15) (2022).

c) Cabeçalho (*header*)

Figura 8 – Representação das informações do cabeçalho de um bloco

Fonte: BlockExplorer (acessado em: 25/11/2023 às 18:08)

O cabeçalho de um bloco na blockchain, também conhecido como header, é um componente essencial que contém informações vitais para garantir a integridade, segurança e ordenação correta dos blocos Abed et al.(16) (2021). O número do bloco, um identificador único atribuído a cada bloco na sequência da blockchain, indica a posição do bloco na cadeia, permitindo a ordenação cronológica e facilitando a referência a blocos específicos.

O timestamp, ou carimbo de data e hora, é outro elemento do cabeçalho do bloco. Ele registra o momento exato de criação do bloco, geralmente em segundos, a partir do chamado Unix epoch time. Este registro temporal é crucial para estabelecer a ordem cronológica das transações e garantir a consistência na sequência dos blocos.

O hash, uma assinatura digital única que identifica todo o conteúdo do bloco, é um elemento crucial do cabeçalho do bloco. Gerado através de um algoritmo de hash criptográfico, o hash é único para cada bloco e representa uma representação compacta de todas as informações contidas no bloco, possibilitando a verificação da integridade dos dados armazenados no bloco Abed et al.(16) (2021).

Na blockchain, o hash é uma sequência de caracteres de comprimento fixo que é gerada aplicando um algoritmo específico a uma entrada ou mensagem. Independentemente do tamanho da entrada, o hash resultante sempre terá um comprimento fixo. Este conceito é fundamental para a forma como as transações são registradas na blockchain.

Cada transação que ocorre na blockchain possui um identificador único conhecido como hash da transação ou ID da transação (TxID). Este código único é gerado quando uma transferência de criptomoedas é confirmada na blockchain. Com esse código, é possível verificar se a transferência foi de fato realizada. Isso destaca a importância do hash na rastreabilidade e transparência das transações na blockchain. Segundo GeeksforGeeks(17)

(2023), a função hash é uma função matemática que transforma qualquer entrada em uma saída de tamanho fixo. As funções de hash criptográfico possuem várias características que as tornam ideais para criptografia segura, como a baixa chance de ocorrência de colisões e a impossibilidade de engenharia reversa da saída de hash. Portanto, o hash desempenha um papel vital na manutenção da integridade, segurança e imutabilidade da blockchain. Isso reforça a confiabilidade da blockchain como um sistema de registro de transações.

O hash é gerado por diversos tipos de algoritmos, tais como: SHA-256, Scrypt, Ethash, X11, Lyra2Z, Equihash e RandomX. A principal função do hash é garantir a integridade dos dados. Qualquer modificação nos dados dentro de um bloco resultaria em um hash completamente diferente. Isso torna qualquer tentativa de manipulação de dados facilmente identificável, pois o hash do bloco seria alterado. Esta característica de imutabilidade do hash é fundamental para a segurança e a confiabilidade da blockchain.

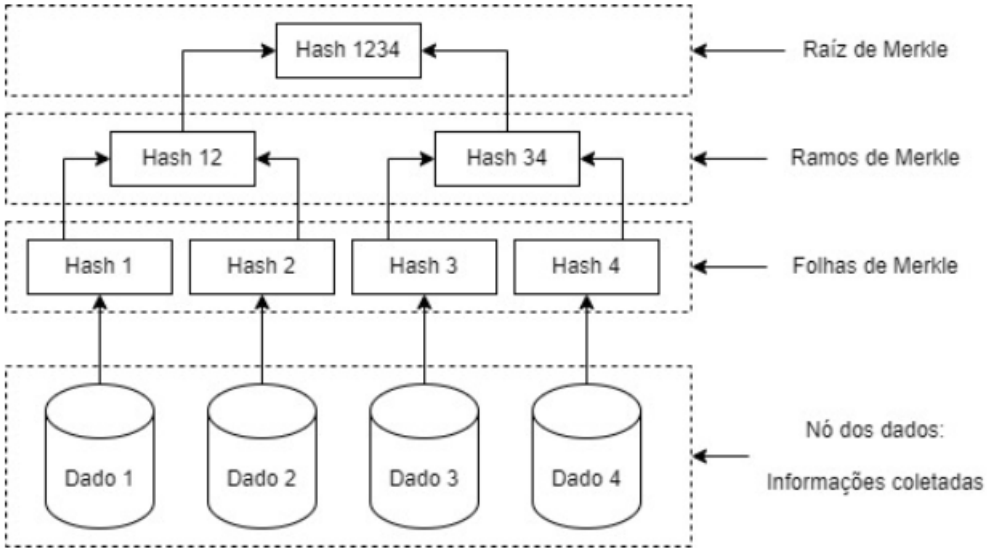
O "hash do bloco anterior" é um componente crucial do cabeçalho de um bloco na blockchain, referenciando o hash do bloco imediatamente anterior na sequência. Isso cria uma conexão linear entre os blocos, estabelecendo uma cadeia contínua e tornando a blockchain imutável. A inclusão do hash do bloco anterior é essencial para a validação de toda a sequência de blocos, pois qualquer alteração em um bloco anterior resultaria em mudanças nos hashes subsequentes, identificando rapidamente qualquer tentativa de manipulação.

O "hash do bloco atual" na blockchain é o hash que representa o conteúdo específico do bloco atual. Este hash é gerado com base em todo o conteúdo do bloco, incluindo transações, timestamp e o hash do bloco anterior. Ele atua como uma assinatura única do bloco atual. Este hash é gerado com base em todo o conteúdo do bloco, incluindo transações, timestamp e o hash do bloco anterior. Ele atua como uma assinatura única do bloco, garantindo a integridade e a autenticidade dos dados contidos no bloco. Além disso, o hash do bloco atual é usado para criar o hash do próximo bloco, estabelecendo assim a conexão entre os blocos e mantendo a integridade da blockchain.

Outro elemento característico de uma blockchain é o nonce, um número arbitrário de 32 bits usado uma única vez. Na mineração de Bitcoin, por exemplo, o nonce é alterado repetidamente até que um hash válido seja encontrado. Este processo é crucial para a segurança da blockchain, pois garante que a mineração de blocos requer esforço computacional significativo, protegendo a rede contra ataques Murray(18) (2019).

d) Informação (*data*)

Figura 9 – Arquitetura da distribuição da informação em uma cadeia de blocos



Fonte: Adaptada pelo autor, 2024

A informação contida em um bloco é a abstração dos dados que estão sendo utilizados naquela cadeia de blocos. Esses dados podem ser valores de criptomoedas, digitalização de documentos (textos), automação e contratos inteligentes, registro de ativos reais, votação digital, entre outros. Esses dados são agregados utilizando o conceito da árvore de Merkle.

Segundo Mohan, Gladston et al.(19) (2020), a árvore de Merkle, também conhecida como árvore binária de hash, é uma estrutura de dados fundamental na blockchain. Ela é usada para codificar os dados da blockchain de maneira mais eficiente e segura. Na blockchain, cada bloco contém uma lista de transações e uma raiz de Merkle. Cada transação é processada por uma função de hash para gerar um hash, que é uma sequência de números e letras que pode ser usada para verificar que um conjunto de dados é o mesmo que o conjunto original de transações. Em seguida, cada par de transações é concatenado e processado juntas pela função de hash, e assim por diante, até que haja um único hash para todo o bloco. Este hash é chamado de raiz de Merkle e é armazenado no cabeçalho do bloco. A árvore de Merkle permite que os nós da rede verifiquem de forma eficiente se uma transação específica está contida em um bloco sem a necessidade de baixar todas as transações. Isso é possível devido à natureza das árvores de Merkle, onde pequenas mudanças nos dados originais resultam em mudanças significativas nos hashes superiores, facilitando a detecção de qualquer alteração nas informações. A informação dentro de um

bloco na blockchain pode variar dependendo do uso da blockchain. Pode ser valores de criptomoedas, digitalização de documentos (textos), automação e contratos inteligentes, registro de ativos reais, votação digital e outros. Esses dados são agregados usando o conceito da árvore de Merkle.

3.1.2 Evolução da blockchain

A tecnologia blockchain tem experimentado uma evolução notável, que pode ser categorizada em quatro gerações distintas: Blockchain 1.0, 2.0, 3.0 e a mais recente, 4.0. Cada geração trouxe consigo novas funcionalidades e aplicações, expandindo o alcance e a utilidade da tecnologia blockchain.

A Blockchain 1.0 é a primeira geração desta tecnologia, representada principalmente pelo Bitcoin. Esta fase inicial focou na criação de uma moeda digital descentralizada e na facilitação de transações *peer-to-peer* (P2P) sem a necessidade de intermediários. O Bitcoin, introduzido em 2009 por Satoshi Nakamoto, foi pioneiro nesse campo. O principal objetivo desta geração era garantir a segurança e a confiança nas transações financeiras, utilizando o consenso de Prova de Trabalho (*Proof of Work - PoW*) para validar e registrar transações na rede Nakamoto(20) (2008).

A Blockchain 2.0 marcou uma evolução significativa na tecnologia de ledger distribuído, introduzindo os chamados contratos inteligentes e expandindo as aplicações para além das simples transações financeiras. Esta fase foi impulsionada pelo Ethereum, uma plataforma que permitiu a criação de aplicativos descentralizados (DApps) e a execução de contratos inteligentes. Contratos inteligentes são códigos autoexecutáveis que facilitam e automatizam acordos entre partes, sem a necessidade de intermediários. O Ethereum, lançado em 2015 e criado por Vitalik Buterin, se diferencia do Bitcoin não apenas por sua moeda nativa, o Ether, mas também por sua capacidade de suportar contratos inteligentes Buterin et al.(21) (2014). Apesar das vantagens proporcionadas pela Blockchain 2.0, como a automação de processos, a descentralização e a expansão das aplicações, ela também enfrenta desafios. Questões de segurança, escalabilidade e regulamentação continuam a ser áreas de preocupação e desenvolvimento dentro deste ecossistema, motivando ainda mais avanços para a Blockchain 3.0 Buterin et al.(21) (2014).

A Blockchain 3.0 representa a próxima fase na evolução da tecnologia blockchain, visando resolver desafios críticos enfrentados por versões anteriores. Este avanço procura abordar questões fundamentais como escalabilidade, sustentabilidade, segurança, custo e interoperabilidade, para tornar a tecnologia mais aplicável em diversos setores e resolver limitações dos estágios anteriores Buterin et al.(21) (2014). Uma das características-chave da Blockchain 3.0 é a introdução do Grafo Acíclico Direcionado (DAG). Esse modelo utiliza uma estrutura de dados de grafo direcionado que não requer blocos ou mineradores, permitindo uma sequência de transações mais eficiente e escalável. Enquanto o Bitcoin tem um tempo de bloco de 10 minutos e o Ethereum de cerca de 20 segundos, o DAG pode lidar com mais de 10.000 transações por segundo, ultrapassando até mesmo gateways de pagamento populares, como a Visa Buterin et al.(21) (2014).

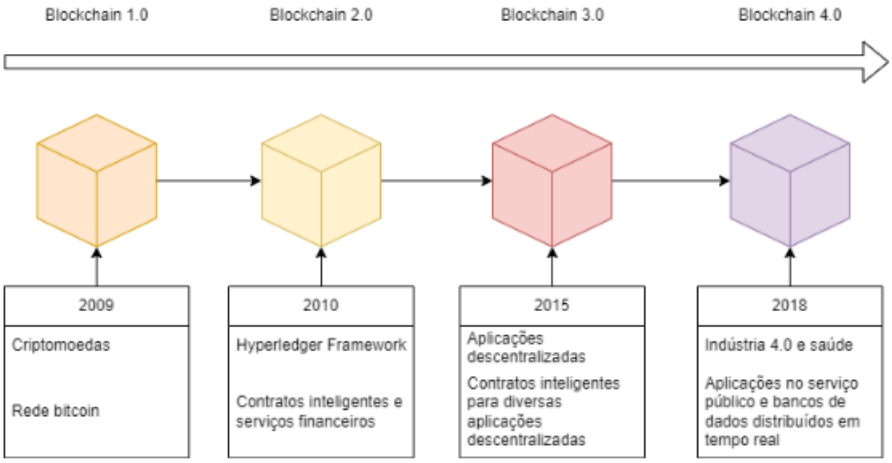
Novos projetos, como Cardano, Zilliqa, EOSIO, ArcBlock, Aion e Hyperledger Fabric, estão entre os pioneiros da Blockchain 3.0. Cada um desses projetos aborda desafios específicos Hamdi, Fourati e Ayed(22) (2023):

- Cardano: Concentra-se em escalabilidade, interoperabilidade, sustentabilidade e governança, oferecendo uma arquitetura segura para smart contracts e aplicativos descentralizados (DApps), além de sua própria criptomoeda, ADA;
- Zilliqa: Desenvolvido para execução de cálculos complexos e intensivos, utiliza a tecnologia de sharding para escalabilidade, permitindo centenas a milhares de transações por segundo com sua linguagem de programação Scilla;
- EOSIO: Facilita a criação e escalabilidade de aplicativos descentralizados, oferecendo um ambiente seguro para contratos inteligentes e DApps;
- ArcBlock: Foca em simplificar a construção e implantação de aplicativos descentralizados, visando tornar a tecnologia blockchain mais acessível e fácil de usar;
- AION: Oferece soluções para privacidade, escalabilidade e interoperabilidade, permitindo a execução de DApps em diferentes blockchains dentro da rede;
- Hyperledger: Um projeto de código aberto que visa desenvolver tecnologias blockchain para empresas, fornecendo várias plataformas de blockchain permissivas prontas para empresas.

A Blockchain 4.0 representa a mais recente geração da tecnologia blockchain, prometendo entregar blockchain como um ambiente empresarial utilizável para a criação e execução de aplicações, trazendo a tecnologia totalmente para o *mainstream*. Nesta versão

4.0, o blockchain passa de ser visto como uma plataforma para um ecossistema empresarial onde se aproveitam suas vantagens como a segurança, automatização e imutabilidade de registros e a facilidade para realizar trâmites como pagos e firmas de contratos Bodkhe et al.(23) (2020).

Figura 10 – Arquitetura da evolução da operação das blockchains e suas linhas de aplicação com o tempo



Fonte: Adaptada pelo autor, 2024

A ascensão da Web 3.0, de acordo com Lacity e Lupien(24) (2022), representa uma evolução significativa na arquitetura da internet, caracterizando-se pela descentralização, segurança avançada e a capacidade de facilitar transações diretas entre pares. Nesse contexto, a tecnologia blockchain emerge como um pilar fundamental na construção dessa nova era da internet.

A blockchain oferece um sistema de registro distribuído e imutável, promovendo a descentralização ao eliminar a necessidade de intermediários centralizados, garantindo maior transparência e confiabilidade na troca de informações e ativos digitais. A segurança inerente à blockchain, proveniente da criptografia avançada e do consenso distribuído, é um elemento crucial para a Web 3.0. Essa tecnologia proporciona uma estrutura imutável que dificulta a adulteração de dados por agentes mal-intencionados, contribuindo para a construção de um ambiente online mais seguro e resiliente.

Outro aspecto central da relação entre blockchain e Web 3.0 é a autonomia e controle de dados conferidos aos usuários. Por meio de identidades digitais descentralizadas e sistemas de gerenciamento de dados, os usuários ganham maior autonomia sobre suas informações pessoais, decidindo quem pode acessá-las e como são utilizadas, alinhando-se com os princípios de uma internet mais centrada no usuário.

A interoperabilidade proporcionada pela blockchain é também um elemento-chave na Web 3.0, permitindo a comunicação entre diferentes blockchains e sistemas. Essa capacidade viabiliza o desenvolvimento de novas aplicações descentralizadas e ecossistemas complexos, possibilitando o compartilhamento de informações e funcionalidades de maneira mais ampla e eficiente.

Em síntese, a integração da tecnologia blockchain na estrutura da Web 3.0 oferece as bases para uma internet mais descentralizada, segura e centrada no usuário. Essa evolução representa não apenas um avanço na tecnologia, mas também a criação de um ambiente online mais confiável e inclusivo para usuários e desenvolvedores Lacity e Lupien(24) (2022).

Tabela 2 – Representação da evolução da web

Fases da Internet	**Datas aproximadas**	**Composição das inovações**
Internet Primitiva	1960s - 1990	Conexões máquina a máquina, Exemplos: 1969 ARPANET, 1982 TCP/IP, 1983 DNS
Web 1.0	1991 - 2004	Pesquisa fácil, Troca de valor facilitada por TTP, Exemplos: 1989 Discada, 1990 HTML, 1991 WWW, 1993 navegadores WWW
Web 2.0	2004 até os dias atuais	Geração fácil de conteúdo, Pesquisa fácil, Exemplos: 1994 Amazon, 1995 Ebay, 1995 Netflix, 1999 Napster, 2003 MySpace, 2005 Facebook, 2006 Youtube, 2010 Instagram, 2016 Tik Tok
Web 3.0	2009 até os dias atuais	Geração fácil de conteúdo, Troca de valor ponto a ponto, Exemplos: 2009 Bitcoin, 2012 Ripple, 2015 Ethereum
Web 4.0	2019 até os dias atuais	Integração entre o mundo físico e o virtual, interação entre seres humanos e máquinas, uso de tecnologias como realidade estendida (XR), inteligência artificial, Internet das Coisas (IoT), blockchain e computação de borda, Exemplos: Meta Quest (2019), Apple Vision Pro (2023)

Fonte: Adaptada pelo autor, 2024.

3.1.3 Topologias de blockchain

Existem três tipos principais de blockchain, cada um com suas próprias características distintas Paul et al.(25) (2021):

a) Blockchains Públicas

Um blockchain público é um sistema de registro distribuído e não restritivo que não requer permissão, e qualquer pessoa com acesso pode ser autorizada a obter os dados ou parte do blockchain. Este tipo de blockchain também dá autorização para a verificação de registros atuais e passados. Além disso, ele é usado para mineração e troca de criptomoedas. Os exemplos mais comuns neste segmento são Bitcoin e Litecoin. Ele é principalmente seguro ao seguir regras e métodos de segurança rigorosos. Todavia, ao não seguir os protocolos de segurança, pode ser arriscado. Alguns exemplos deste tipo de blockchain são Bitcoin, Ethereum e Litecoin Paul et al.(25) (2021).

Os blockchains públicos são confiáveis e, ao contrário dos blockchains privados, os participantes não precisam pensar na autenticidade. Neste tipo de blockchain público, eles não precisam conhecer outros nós, e portanto não há fraude nas transações. Nesta categoria, os nós podem se contatar cegamente sem sentir a necessidade de confiar em nós individuais.

No blockchain público, há oportunidades de se conectar com outros participantes e nós na mesma rede pública, e isso resulta em uma comunicação e participação segura, maior e maior. Devido a esse recurso, é difícil para os invasores entrarem nos sistemas e aqui cada nó fará as verificações e transações conforme as normas. Aqui, métodos de criptografia cuidadosos são usados e, portanto, é muito mais seguro do que o blockchain privado, de acordo com alguns especialistas.

O blockchain público também tem os recursos de abertura e aqui os dados são basicamente transparentes para todos os nós e neste mecanismo, um registro de blockchain é normalmente disponível para todos os nós autorizados. Portanto, aqui todos os nós se tornam abertos e transparentes e não há transações falsas ou ocultação de informações.

Embora haja muitas vantagens e benefícios, também há diferentes tipos de desvantagens e fraquezas, e algumas delas são mencionadas abaixo.

Baixa transação por segundo: No sistema de blockchain público, a taxa de transação por segundo é muito baixa, e isso se deve ao grande número de nós e à grande rede. Aqui,

cada nó tem que verificar a transação e também fazer a prova de trabalho é demorado. Aqui, em sistemas públicos, sete transações acontecem por segundo e, além disso, aqui a rede Ethereum tem uma taxa de TPS de cerca de 15.

Problemas de escalabilidade: Semelhante ao problema mencionado anteriormente sobre uma transação mais baixa por segundo no blockchain público, outro problema é a escalabilidade de acordo com os especialistas. O enorme tamanho basicamente cria a escalabilidade a esse respeito e aqui as redes de iluminação de bitcoins são consideradas importantes para superar o problema de acordo com os especialistas Paul et al.(25) (2021).

b) Blockchains Privadas

De acordo com Gupta e Sadoghi(26) (2021), um blockchain privado é um sistema de registro restrito e não aberto que possui recursos de acesso controlados. Este tipo de blockchain permite a permissão para a transação com o apoio do administrador do sistema. As soluções de blockchain privado são desenvolvidas com os seguintes recursos: privacidade total, alta eficiência, transações mais rápidas, melhor escalabilidade e velocidade.

Este tipo de blockchain opera apenas em sistemas e redes fechados e é geralmente útil em organizações e empresas das quais apenas membros selecionados podem participar. Este tipo de blockchain oferece segurança adequada, autorizações, permissões e acessibilidade. De acordo com especialistas, blockchains privados são implementados para votação, gerenciamento de cadeia de suprimentos, busca e gerenciamento de identidade digital, propriedade de ativos, entre outros. Existem certos blockchains privados populares como Multichain, projetos Hyperledger, Corda, etc Gupta e Sadoghi(26) (2021).

Os blockchains privados são operados com nós autorizados; portanto, ninguém fora da rede privada é capaz de acessar informações e dados relacionados à transação trocados entre dois nós. Os blockchains privados também possuem vários tipos de vantagens e desvantagens em relação aos blockchains públicos Gupta e Sadoghi(26) (2021).

De acordo com os especialistas, as seguintes são consideradas como vantagens e benefícios importantes do Blockchain Privado: Velocidade: Blockchains privados operam com maior velocidade do que um blockchain público e, portanto, aqui pode-se observar uma taxa mais alta de TPS (ou seja, transação por segundo). Além disso, aqui apenas um número limitado de nós pode ser visto, portanto, vem com maior velocidade. Aqui todos os nós têm capacidade de verificação de processo e, portanto, a taxa de adição de novas transações em um bloco é rápida. Aqui, cerca de milhares ou cem mil TPS são possíveis de

uma vez Gupta e Sadoghi(26) (2021). Escalabilidade: Em comparação com um blockchain público, um blockchain privado é mais rápido e, portanto, oferece maior escalabilidade. Aqui, adicionar nós aos existentes se torna fácil e rápido. Assim, torna os blockchains privados muito escaláveis e flexíveis. E aqui, adicionar ou remover nós não afeta como tal nos sistemas existentes.

Embora haja muitas vantagens e benefícios, também há diferentes tipos de desvantagens e fraquezas, e algumas delas são mencionadas abaixo. Requer construção de confiança: O blockchain público é um tipo de livro-razão aberto e, portanto, está preocupado com a segurança e legitimidade de cada usuário individual, contudo, no blockchain privado, como apenas usuários de acesso limitado, portanto, requer construção de confiança Gupta e Sadoghi(26) (2021). Segurança mais baixa: O blockchain privado é fraco quando um terceiro obtém acesso ao sistema de gerenciamento central; portanto, aqui é mais fácil para um nó hackear todo o sistema de blockchain privado Gupta e Sadoghi(26) (2021).

c) Blockchains Híbridas

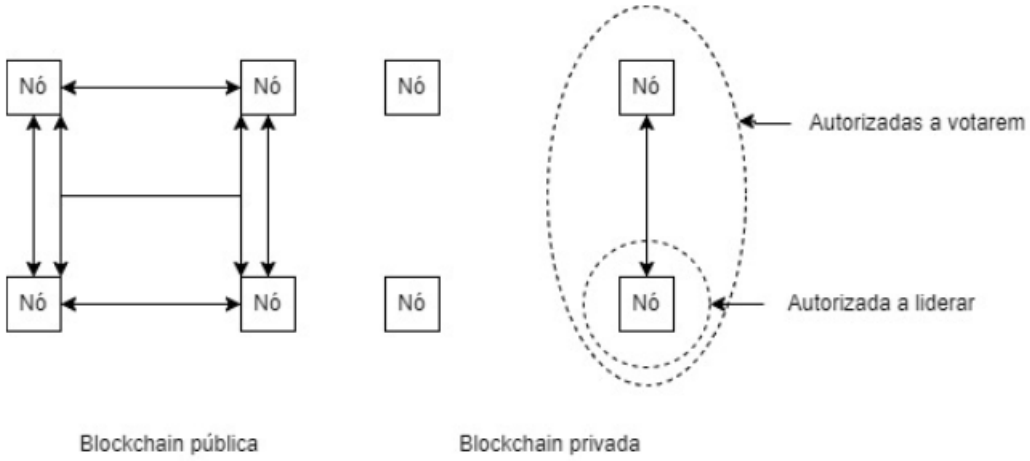
De acordo com Lamounier(27) (2020), um blockchain híbrido é uma combinação de blockchain público e privado, necessário para um controle mais eficaz na busca por metas mais elevadas. Este tipo de blockchain lida com sistemas centralizados e descentralizados. Embora não seja aberto, possui características de integridade, transparência e segurança. Ele apresenta várias vantagens em relação aos blockchains tradicionais. No blockchain híbrido, a personalização máxima é considerada o principal benefício, com um sistema baseado em permissão privada e um sistema público sem permissão. Nesses sistemas de blockchain, os usuários podem acessar seções selecionadas, enquanto o restante pode ser registrado ou mantido seguro, graças aos benefícios dos registros do livro-razão. Os blockchains híbridos são flexíveis o suficiente para permitir que os usuários se juntem facilmente como em um blockchain privado. Este tipo de blockchain é capaz de melhorar a segurança e a transparência da rede blockchain.

O blockchain de consórcio é outro tipo de blockchain semi-descentralizado, capaz de permitir que uma organização gerencie a rede blockchain. Este tipo de blockchain pode realizar atividades mesmo a partir de uma única organização. Aqui, o blockchain é capaz de trocar informações ou realizar mineração e é usado em áreas como bancos, organizações governamentais, etc. Alguns exemplos deste tipo de consórcio são Energy Web Foundation, R3, etc Lamounier(27) (2020).

As blockchains com requisição de autorização, também conhecidas como blockchains permissionadas, são um tipo de blockchain onde o acesso é restrito a determinados usuários. Diferentemente das blockchains públicas, onde qualquer pessoa pode participar e ter acesso aos dados, as blockchains permissionadas exigem que os usuários sejam autorizados para participar da rede e ter acesso aos dados.

Essas blockchains são comumente usadas em ambientes corporativos ou governamentais, onde a privacidade e o controle sobre os dados são de extrema importância. Elas oferecem maior privacidade, eficiência e escalabilidade em comparação com as blockchains públicas Moura, Brauner e Janissek-Muniz(28) (2020).

Figura 11 – Topologias de blockchain



Fonte: Adaptada pelo autor, 2024

3.1.4 Mecanismos de consenso

Um mecanismo de consenso em uma blockchain ou em qualquer sistema distribuído serve para resolver o problema da confiança entre múltiplos participantes que não necessariamente confiam uns nos outros. Sua função principal é garantir que todos concordem sobre o estado atual do sistema, como as transações válidas, a ordem em que foram registradas e a criação de novos blocos na blockchain. Isso é fundamental para manter a integridade e a segurança do sistema, garantindo que todas as partes envolvidas cheguem a um acordo sem depender de uma autoridade central Zhang, Wu e Wang(29) (2020).

Em uma rede descentralizada, onde os nós (ou participantes) podem ter interesses próprios ou maliciosos, um mecanismo de consenso estabelece regras que os participantes devem seguir para validar transações e manter a consistência na rede. Ele oferece um

método para resolver disputas, decidir quais transações são válidas e prevenir fraudes ou gastos duplicados Zhang, Wu e Wang(29) (2020).

Além disso, um mecanismo de consenso também determina como novos blocos de transações são adicionados à blockchain, definindo o processo pelo qual os participantes podem criar blocos, validar transações e ser recompensados por seu trabalho (como no caso do Proof of Work). Em essência, ele permite que uma rede descentralizada alcance um consenso global, mesmo que alguns participantes possam tentar agir de forma maliciosa Zhang, Wu e Wang(29) (2020).

Os principais mecanismos de consenso utilizados em redes blockchain podem ser classificados em quatro categorias: baseados em recursos, baseados em votação, baseados em reputação e baseados em identidade Zhang, Wu e Wang(29) (2020). A seguir, apresenta-se uma breve descrição de cada categoria e seus respectivos exemplos.

Mecanismos baseados em recursos: Esses mecanismos exigem que os participantes da rede consumam ou provem possuir algum recurso escasso, como poder computacional, espaço de armazenamento ou moedas, para validar transações e gerar novos blocos. O objetivo é desencorajar comportamentos maliciosos e garantir a segurança e a integridade da rede. Alguns exemplos de mecanismos baseados em recursos são:

- *Proof of Work (PoW)*: O primeiro e mais conhecido mecanismo de consenso, introduzido por Nakamoto(20) (2008) no *whitepaper* do Bitcoin. O PoW requer que os mineradores resolvam problemas criptográficos complexos, que demandam alto consumo de energia, para alcançar o consenso. O PoW oferece um alto nível de descentralização, mas tem como desvantagens a baixa velocidade de transação e a dificuldade de escalabilidade em redes públicas Nakamoto(20) (2008);
- *Proof of Stake (PoS)*: Uma alternativa ao PoW, proposta por King e Nadal(30) (2012) como parte do Peercoin. O PoS atribui o poder de validação aos participantes de acordo com a quantidade de moedas que eles possuem ou apostam na rede. O PoS reduz o consumo de energia, aumenta a velocidade de transação e previne ataques de 51%. Entretanto, o PoS também apresenta alguns problemas, como a tendência à centralização, a vulnerabilidade a ataques de longa distância e a falta de incentivos para os participantes King e Nadal(30) (2012);
- Outros mecanismos: Existem outros mecanismos baseados em recursos, como o *Proof of Space (PoSpace)*, o *Proof of Burn (PoB)* e o *Proof of Capacity (PoC)*, que utilizam

diferentes tipos de recursos, como espaço de armazenamento ou moedas queimadas, como prova de trabalho. Esses mecanismos são mais eficientes em termos energéticos do que o PoW, mas ainda estão em fase experimental e enfrentam desafios como a segurança, a escalabilidade e a sustentabilidade Lashkari e Musilek(31) (2021).

Mecanismos baseados em votação: Esses mecanismos utilizam um sistema de eleição ou delegação para escolher os validadores ou produtores de blocos, que são responsáveis por validar transações e gerar novos blocos. O objetivo é aumentar a eficiência e a escalabilidade da rede, reduzindo o número de participantes envolvidos no consenso. Alguns exemplos de mecanismos baseados em votação são:

- *Delegated Proof of Stake (DPoS)*: Um mecanismo de consenso proposto por Larimer(32) (2014) como parte do BitShares, uma plataforma de troca de ativos digitais. No DPoS, os detentores de tokens votam em representantes, chamados de delegados, para validar transações e produzir blocos. O DPoS é mais rápido e escalável do que o PoW e o PoS, mas é criticado pela centralização, pois os votantes elegem um número limitado de delegados para a validação. Segundo Larimer (2014, p. 2), o DPoS visa "maximizar a utilidade de todos os participantes";
- *Byzantine Fault Tolerance (BFT)*: Um conjunto de algoritmos que permitem que um grupo de nós chegue a um acordo sobre o estado da rede, mesmo na presença de nós maliciosos ou defeituosos, que podem enviar informações falsas ou inconsistentes. Existem diferentes variações de BFT, como o *Practical Byzantine Fault Tolerance (PBFT)* , o *Federated Byzantine Agreement (FBA)* e o *Tendermint* . Esses algoritmos são mais eficientes e escaláveis do que o PoW e o PoS, mas são menos descentralizados e mais vulneráveis a ataques de censura. Para Castro, Liskov et al.(33) (1999) o PBFT é "o primeiro algoritmo prático que permite que sistemas distribuídos tolerem falhas bizantinas".

Mecanismos baseados em reputação: Esses mecanismos utilizam um sistema de pontuação ou classificação para atribuir confiança aos participantes da rede. Os critérios para essa atribuição incluem a quantidade de moedas que um participante possui, sua atividade na rede e seu histórico de transações. O objetivo desses mecanismos é incentivar a participação e a contribuição dos usuários e prevenir comportamentos maliciosos. Alguns exemplos de mecanismos baseados em reputação são:

- *Proof of Importance (PoI)*: Este é um mecanismo de consenso, uma plataforma de serviços blockchain. O PoI leva em consideração não apenas a quantidade de moedas que um participante possui, mas também sua atividade na rede, como o número de transações que ele envia e recebe. O PoI visa incentivar a participação e a contribuição dos usuários, mas pode ser manipulado por atores mal-intencionados. O PoI é "um algoritmo que calcula a importância de cada conta na rede";
- *Proof of Activity (PoA)*: Este é um mecanismo de consenso que combina o *Proof of Work (PoW)* e o *Proof of Stake (PoS)*. O PoA requer que os mineradores resolvam problemas criptográficos, como no PoW, mas também que eles apostem moedas, como no PoS, para validar transações e gerar novos blocos. O PoA busca equilibrar os benefícios do PoW e do PoS, mas também herda seus problemas. O PoA é "uma forma de estender o PoW via PoS".

Mecanismos baseados em identidade: Esses mecanismos utilizam um sistema de verificação ou autenticação para atribuir identidades únicas aos participantes da rede. O objetivo desses mecanismos é garantir a responsabilidade e a transparência dos usuários, bem como prevenir ataques de Sybil, que ocorrem quando um participante cria múltiplas identidades falsas para influenciar o consenso. Um exemplo de mecanismo baseado em identidade é:

- *Proof of Authority (PoA)*: Este é um mecanismo de consenso proposto pela Parity Technologies, uma empresa de software blockchain. O PoA utiliza um conjunto de validadores pré-aprovados, que são escolhidos com base em sua identidade e reputação, para validar transações e gerar novos blocos. O PoA é mais rápido e escalável do que o PoW e o PoS, mas é altamente centralizado e depende da confiança nos validadores. O PoA é "um algoritmo de consenso que oferece uma alternativa de baixo custo e baixa latência ao PoW".

3.2 INTERNET INDUSTRIAL DAS COISAS (IIoT)

3.2.1 Conceitos básicos de IIoT

A Internet Industrial das Coisas (IIoT) é uma aplicação da tecnologia da Internet das Coisas (IoT) em ambientes industriais, como manufatura, energia, transporte e saúde. A IIoT tem como objetivo aumentar a eficiência, a produtividade, a qualidade e a sustentabilidade dos processos industriais, por meio da integração de sensores, dispositivos, máquinas e sistemas de informação conectados à Internet. A IIoT também é um dos pilares da chamada Indústria 4.0, que representa a quarta revolução industrial baseada na digitalização e na inteligência artificial.

Para entender melhor o conceito e os benefícios da IIoT, é preciso conhecer alguns elementos que compõem essa tecnologia, tais como:

- Arquitetura de referência: é um modelo que define os componentes, as relações, os padrões e as diretrizes para projetar e implementar sistemas de IIoT. Existem várias propostas de arquitetura de referência para a IIoT, como a do Consórcio de Internet Industrial (IIC), a do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) e a do Consórcio World Wide Web (W3C). Essas propostas buscam facilitar a interoperabilidade, a segurança, a escalabilidade e a confiabilidade dos sistemas de IIoT;
- Os protocolos de comunicação são as regras e os formatos que permitem a troca de dados entre os dispositivos e os sistemas da Internet das Coisas Industrial (IIoT). Alguns exemplos de protocolos de comunicação para a IIoT são o Protocolo de Transferência de Hipertexto (HTTP), o Protocolo de Telemetria de Enfileiramento de Mensagens (MQTT) e o Protocolo de Aplicação Restrita (CoAP). Esses protocolos são baseados em padrões abertos e oferecem diferentes características e vantagens, como a simplicidade, a eficiência, a confiabilidade e a adaptabilidade;
- Análise de dados: é o processo de extrair informações úteis e relevantes dos dados coletados pelos dispositivos e sensores de IIoT. A análise de dados pode ser realizada de forma centralizada, distribuída ou híbrida, dependendo da arquitetura e dos requisitos do sistema de IIoT. A análise de dados pode envolver técnicas de inteligência

Tabela 3 – Principais diferenças entre IoT e IIoT

Características	**IoT**	**IIoT**
Aplicação	Amplamente aplicada em diversos setores como saúde, casa inteligente, automação residencial, entretenimento, etc.	Especificamente aplicada em ambientes industriais como fábricas, sistemas de produção, logística, manufatura, etc.
Objetivo	Melhorar a qualidade de vida, aumentar a eficiência, oferecer conveniência, coletar dados para análise e tomada de decisões.	Aumentar a eficiência operacional, otimizar processos industriais, monitorar ativos e condições ambientais, prever falhas e realizar manutenção preditiva.
Requisitos	Ênfase na conectividade, interoperabilidade, segurança da informação, consumo de energia eficiente, custo acessível e facilidade de uso.	Ênfase na robustez, confiabilidade, escalabilidade, integridade dos dados, latência mínima, segurança industrial, integração com sistemas legados e resiliência.
Protocolos	Utiliza uma variedade de protocolos de comunicação como Wi-Fi, Bluetooth, Zigbee, LoRa, MQTT, HTTP, entre outros.	Utiliza protocolos específicos para ambientes industriais como OPC-UA, Modbus, PROFINET, EtherNet/IP, entre outros, além de protocolos padrão da IoT.
Dispositivos	Uma ampla gama de dispositivos inteligentes desde eletrodomésticos até dispositivos vestíveis e sensores ambientais.	Dispositivos robustos e industriais como sensores de temperatura, atuadores, controladores lógicos programáveis (CLPs), gateways industriais, etc.
Ambiente	Ambientes domésticos, urbanos, de escritório e públicos, com menor ênfase em condições ambientais extremas ou adversas.	Ambientes industriais adversos, com altas temperaturas, umidade, vibrações, poeira, produtos químicos agressivos, etc.
Segurança	A segurança é uma preocupação, mas geralmente é mais voltada para a privacidade dos dados do usuário.	A segurança é uma prioridade crítica devido aos riscos de danos físicos, perda de produção, violações regulatórias e ameaças cibernéticas.
Padrões de Dados	Diversidade de padrões e formatos de dados, muitas vezes com ênfase em interfaces amigáveis para o usuário final.	Utiliza padrões de dados específicos da indústria como ISA-95, MTConnect, OPC-UA, bem como formatos padronizados para interoperabilidade e integração de sistemas.

Fonte: Adaptada pelo autor, 2024.

artificial e aprendizado de máquina para gerar insights e ações automatizadas, como a manutenção preditiva, a otimização de processos e a detecção de anomalias.

A IIoT é uma tecnologia em constante evolução e com grandes desafios, como a integração de sistemas legados, a proteção de dados e a privacidade, a gestão de energia e a governança. No entanto, a IIoT também oferece grandes oportunidades e benefícios para as indústrias e para a sociedade, como a redução de custos e de emissões, o aumento da segurança e da qualidade, a melhoria da experiência do cliente e a criação de novos modelos de negócio e de inovação.

3.2.2 Aplicações de IIoT

Segundo Larimer(32) (2014), a Internet das Coisas Industrial (IIoT) é uma rede de dispositivos inteligentes que coletam, processam e compartilham dados em tempo real, permitindo a análise preditiva e a manutenção preventiva dos equipamentos industriais. Entre as aplicações da IIoT, destacam-se:

- Monitoramento e controle remoto: a IIoT permite que os operadores e gestores acompanhem e controlem os processos industriais à distância, por meio de dispositivos móveis ou computadores. Isso facilita a tomada de decisão, a resolução de problemas e a otimização de recursos. Por exemplo, a Siemens usa a IIoT para monitorar e controlar remotamente suas turbinas eólicas, reduzindo os custos de operação e manutenção;
- Manutenção preditiva: a IIoT possibilita que os equipamentos industriais sejam monitorados em tempo real, gerando dados sobre seu desempenho, seu estado e suas necessidades de manutenção. Com o uso de técnicas de inteligência artificial e aprendizado de máquina, é possível prever falhas, evitar paradas e prolongar a vida útil dos equipamentos . Por exemplo, a GE usa a IIoT para prever e prevenir falhas em seus motores de avião, aumentando a segurança e a eficiência dos voos;
- Rastreabilidade e logística: a IIoT permite que os produtos e materiais sejam identificados, localizados e rastreados ao longo de toda a cadeia de suprimentos, desde a produção até a entrega ao cliente. Isso melhora a qualidade, a segurança, a transparência e a eficiência do fluxo de produtos e informações . Por exemplo, a

IBM usa a IIoT para rastrear e gerenciar seus contêineres de transporte, otimizando o uso do espaço e o tempo de entrega.

3.2.3 Desafios de IIoT

A comunicação IIoT - Computação em Névoa é um tema que aborda a utilização de uma arquitetura computacional descentralizada para processar e armazenar dados gerados por dispositivos conectados à Internet das Coisas (IoT). A computação em névoa (*fog computing*) é definida como uma infraestrutura que distribui dados, computação, armazenamento e aplicações em um local mais apropriado entre a fonte de dados e a nuvem, fazendo uma interconexão entre esses dois ambientes. O termo névoa se refere a uma nuvem mais próxima do solo, ou seja, mais próxima dos dispositivos que geram e coletam os dados. A computação em névoa complementa e não substitui a computação em nuvem, pois permite análises de curto prazo na borda da rede, enquanto a nuvem executa análises de longo prazo com uso intensivo de recursos.

Arquitetura: A arquitetura da computação em névoa é composta por quatro camadas principais: a camada de dispositivos, a camada de rede, a camada de plataforma e a camada de aplicação. A camada de dispositivos é formada pelos sensores, atuadores, controladores e outros dispositivos que coletam e enviam dados. A camada de rede é responsável pela comunicação entre os dispositivos e a nuvem, usando protocolos e meios físicos adequados. A camada de plataforma é onde os dados são processados, armazenados e analisados, usando serviços de computação em nuvem ou em névoa. A camada de aplicação é onde os dados são transformados em informações úteis para os usuários finais ou para os sistemas de controle.

Protocolos de comunicação: Os protocolos de comunicação são os padrões que definem como os dispositivos se comunicam entre si e com a nuvem. Eles devem garantir a interoperabilidade, a segurança, a confiabilidade e a eficiência da transmissão de dados. Alguns dos protocolos mais usados na computação em névoa são: MQTT (*Message Queuing Telemetry Transport*), CoAP (*Constrained Application Protocol*), AMQP (*Advanced Message Queuing Protocol*) e HTTP (*Hypertext Transfer Protocol*). Esses protocolos são baseados no modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*) e podem ser aplicados em diferentes camadas da arquitetura.

Meios físicos: Os meios físicos são os meios materiais que permitem a transmissão de dados entre os dispositivos e a nuvem. Eles podem ser classificados em dois tipos: meios guiados e meios não guiados. Os meios guiados são aqueles que usam cabos ou fios para conduzir os sinais elétricos ou ópticos, como o par trançado, o cabo coaxial e a fibra óptica. Os meios não guiados são aqueles que usam ondas eletromagnéticas para propagar os sinais pelo ar ou pelo espaço, como o rádio, o infravermelho, o bluetooth e o wi-fi. A escolha do meio físico depende de fatores como a distância, a velocidade, a capacidade, a segurança e o custo da comunicação.

Os hardwares de controle são os dispositivos que permitem a comunicação, o processamento e a atuação dos dados gerados pelos sensores e outros dispositivos da IIoT. Eles são responsáveis por executar as lógicas de controle, as análises de dados e as ações necessárias para o funcionamento dos sistemas industriais.

Os hardwares de controle mínimo para a IIoT dependem das características e requisitos de cada aplicação, como o tipo de sensor, o protocolo de comunicação, o meio físico, a latência, a segurança, a confiabilidade e a escalabilidade. Não há uma solução única que atenda a todas as necessidades, mas sim uma variedade de opções que devem ser avaliadas e escolhidas de acordo com o cenário.

Alguns exemplos de hardwares de controle para a IIoT são: Controladores Lógicos Programáveis (PLCs), Controladores Industriais de PC (IPCs), gateways de IoT, microcontroladores, sistemas embarcados, Sistemas em Chip (SoC), módulos de comunicação sem fio, conversores de protocolo, entre outros.

Cada hardware de controle tem suas vantagens e desvantagens, que devem ser consideradas na hora da seleção. Por exemplo, os PLCs são robustos, confiáveis e fáceis de programar, mas têm custo elevado, baixa capacidade de processamento e pouca flexibilidade. Já os IPCs são poderosos, versáteis e compatíveis com vários sistemas operacionais, mas têm custo ainda mais alto, maior consumo de energia e menor resistência a ambientes hostis. Os gateways de IoT são dispositivos intermediários que conectam os sensores e os dispositivos de borda à nuvem, realizando funções de conversão de protocolo, filtragem de dados, segurança e gerenciamento. Eles têm custo moderado, boa capacidade de processamento e alta flexibilidade, mas podem apresentar problemas de latência, confiabilidade e escalabilidade.

3.3 SEGURANÇA CIBERNÉTICA

3.3.1 Conceitos básicos de segurança cibernética

A segurança cibernética é uma prática que busca proteger sistemas essenciais e informações sensíveis contra ataques digitais. Ela envolve um conjunto de práticas, tecnologias e processos com o objetivo de proteger sistemas de computadores para evitar que dados sejam acessados, destruídos ou roubados. A estrutura da segurança cibernética geralmente envolve várias camadas de proteção distribuídas pelos sistemas de uma organização, incluindo a proteção dos dispositivos de rede, dos sistemas de informação e dos dados armazenados ou transmitidos nesses sistemas. Os mecanismos de segurança cibernética podem ser divididos em duas categorias principais: medidas preventivas e medidas reativas. As medidas preventivas, como firewalls, software antivírus e autenticação de dois fatores, são projetadas para evitar que um ataque ocorra. As medidas reativas, como programas de detecção de intrusão e planos de resposta a incidentes, são usadas para responder a um ataque que já ocorreu.

Um dos principais desafios da segurança cibernética é a rápida evolução das ameaças. Os cibercriminosos estão constantemente desenvolvendo novas técnicas para burlar as defesas e obter acesso não autorizado a sistemas e dados. Isso exige que os profissionais de segurança cibernética estejam sempre atualizados sobre as últimas tendências e desenvolvimentos no campo. Segundo o relatório da IBM *Security X-Force Threat Intelligence Index* 2023, o ano de 2022 foi marcado por um aumento de 40% nos ataques cibernéticos em relação ao ano anterior, sendo os setores de finanças, manufatura e energia os mais visados.

Além disso, a segurança cibernética não é apenas uma questão técnica, mas também uma questão de gestão de riscos. As organizações precisam avaliar os riscos associados às suas operações digitais e implementar medidas de segurança adequadas para mitigar esses riscos. Isso pode incluir a implementação de tecnologias de segurança, a formação de pessoal e a criação de políticas e procedimentos de segurança. De acordo com o Instituto Nacional de Padrões e Tecnologia (NIST), uma abordagem eficaz para a gestão de riscos cibernéticos deve seguir cinco etapas: identificar, proteger, detectar, responder e recuperar. No Brasil, a segurança cibernética ganhou destaque com a publicação do decreto 10.222 que estabeleceu a Estratégia Nacional de Segurança Cibernética do Brasil (E-Ciber). Este documento

visa proporcionar um panorama sobre o papel do Brasil na segurança cibernética, bem como os objetivos e princípios norteadores para seu desenvolvimento entre os anos de 2020 e 2023. Entre os objetivos da E-Ciber, estão: fortalecer a governança nacional de segurança cibernética, promover a cultura de segurança cibernética na sociedade, incentivar a inovação e o desenvolvimento científico e tecnológico na área, e ampliar a cooperação internacional em segurança cibernética.

3.3.2 Desafios de segurança cibernética

A segurança em ambientes industriais, especialmente no contexto da Internet das Coisas Industrial (IIoT), é uma área de pesquisa em rápido crescimento. A IIoT refere-se à aplicação de tecnologias da Internet das Coisas (IoT) em ambientes industriais, como fábricas, usinas de energia e sistemas de transporte. A IIoT visa melhorar a eficiência, a produtividade e a qualidade dos processos industriais, bem como habilitar novos modelos de negócios e serviços. No entanto, a segurança é uma preocupação primordial na IIoT devido à natureza crítica das operações industriais e ao potencial de danos significativos em caso de falha ou comprometimento do sistema. As ameaças à segurança na IIoT podem variar desde ataques cibernéticos, como *malware* e *hacking*, até falhas físicas, como danos ao equipamento ou interrupções no fornecimento de energia.

Os sistemas IIoT são frequentemente compostos por uma variedade de dispositivos, desde sensores e atuadores até gateways de rede e servidores de nuvem. Cada um desses componentes pode ser um ponto de vulnerabilidade potencial, tornando a segurança um desafio complexo e multifacetado. Além disso, os sistemas IIoT devem lidar com requisitos específicos, como baixa latência, alta confiabilidade, escalabilidade e interoperabilidade, que podem impor restrições adicionais à segurança.

As estratégias de segurança para a IIoT geralmente envolvem uma combinação de medidas preventivas e reativas. As medidas preventivas podem incluir o uso de criptografia para proteger os dados em trânsito, autenticação robusta para garantir que apenas usuários autorizados tenham acesso ao sistema e atualizações regulares de software para corrigir quaisquer vulnerabilidades conhecidas. As medidas reativas podem incluir o monitoramento contínuo do sistema para detectar qualquer atividade suspeita e a implementação de planos de resposta a incidentes para minimizar o impacto de qualquer violação de segurança.

No entanto, apesar desses esforços, a segurança na IIoT continua sendo um desafio significativo. A rápida evolução da tecnologia, a crescente sofisticação dos atacantes e a natureza intrinsecamente complexa dos sistemas IIoT significam que a segurança é uma área de pesquisa ativa e em constante evolução. A colaboração entre a indústria, a academia e o governo será crucial para enfrentar esses desafios e garantir a segurança dos sistemas IIoT no futuro.

A seguir, apresentou-se alguns exemplos de ataques que podem afetar a segurança da IIoT, bem como possíveis soluções e desafios para mitigá-los:

- Ataques de Negação de Serviço (DoS/DDoS): Esses ataques, também conhecidos como ataques de negação de serviço, são projetados para sobrecarregar os recursos de um sistema, tornando-o incapaz de atender às demandas legítimas. Em um ambiente IIoT, um ataque DoS/DDoS pode sobrecarregar dispositivos críticos ou sistemas de controle, causando uma interrupção na produção e potencialmente levando a danos significativos. Isso pode ser especialmente prejudicial em um ambiente industrial, onde a interrupção da produção pode ter consequências financeiras substanciais. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de detecção e filtragem de tráfego anômalo, que podem identificar e bloquear pacotes maliciosos antes que eles atinjam o destino. Contudo, essas técnicas podem ter limitações de desempenho, precisão e escalabilidade, especialmente em cenários de ataques distribuídos e dinâmicos;
- Ataques de Injeção de Código: Esses ataques exploram vulnerabilidades nos sistemas IIoT para inserir códigos maliciosos. O código malicioso pode então ser usado para manipular processos industriais de maneiras não autorizadas ou para interromper as operações. Isso pode incluir ações como alterar as configurações de um dispositivo, desligar sistemas ou até mesmo assumir o controle de um processo industrial. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de verificação e validação de código, que podem verificar a integridade e a autenticidade do código antes de executá-lo. Entretanto, essas técnicas podem ter limitações de custo, complexidade e compatibilidade, especialmente em dispositivos com recursos limitados e heterogêneos;
- Ataques *Man-in-the-Middle* (MITM): Os ataques MITM ocorrem quando um invasor consegue se posicionar entre a comunicação de dois dispositivos IIoT. O invasor

pode então interceptar e possivelmente alterar os dados que estão sendo transmitidos entre os dispositivos. Isso pode permitir ao invasor obter informações confidenciais, falsificar comandos ou comprometer a integridade dos dados. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de segurança de canal, que podem garantir a confidencialidade, a integridade e a autenticidade dos dados em trânsito. No entanto, essas técnicas podem ter limitações de sobrecarga, latência e gerenciamento de chaves, especialmente em ambientes dinâmicos e distribuídos;

- Roubo de Identidade (*Identity Theft*): O roubo de identidade em ambientes IIoT envolve a obtenção não autorizada de credenciais de autenticação ou certificados. Isso pode permitir que um invasor se passe por um dispositivo legítimo, ganhando acesso a sistemas ou dados sensíveis. Em um ambiente industrial, isso pode permitir ao invasor acessar informações confidenciais ou até mesmo assumir o controle de processos industriais. O roubo de identidade é uma das principais ameaças à segurança da IIoT, pois pode comprometer a confiança, a integridade e a disponibilidade dos sistemas industriais;
- Exploração de Vulnerabilidades de Software/Firmware: Esses ataques exploram falhas de segurança no software ou firmware de dispositivos IIoT. Isso pode incluir a exploração de brechas não corrigidas, permitindo ao invasor obter acesso não autorizado ou exercer controle indevido sobre os dispositivos. Esses ataques podem causar danos severos aos sistemas IIoT, como interrupção do serviço, perda de dados, corrupção de arquivos ou infecção por malware. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de verificação e validação de código, que podem verificar a integridade e a autenticidade do código antes de executá-lo;
- Ataques de Ransomware: Os ataques de ransomware na IIoT envolvem a infecção de sistemas ou dispositivos com um tipo de malware que impede seu funcionamento normal até que um resgate seja pago. Isso pode resultar em interrupções graves nas operações industriais e pode exigir uma resposta significativa para resolver. Os ataques de ransomware na IIoT aumentaram 35% em 2020, afetando principalmente os setores de manufatura, energia e saúde. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de detecção e filtragem de tráfego anômalo, que podem identificar e bloquear pacotes maliciosos antes que eles atinjam o destino;

- Ataques Físicos: Além dos ataques cibernéticos, os sistemas IIoT também podem ser alvo de ataques físicos. Isso pode envolver invasores que tentam danificar ou manipular fisicamente dispositivos ou componentes, o que pode afetar diretamente a operação industrial. Esses ataques podem ter motivações políticas, econômicas ou terroristas, e podem visar a destruição ou sabotagem de infraestruturas críticas. Uma possível solução para prevenir ou mitigar esses ataques é o uso de técnicas de segurança física, que podem proteger os dispositivos e componentes de danos ou interferências externas.

Esses tipos de ataques à IIoT representam apenas uma fração das ameaças enfrentadas pelos sistemas industriais interconectados. A complexidade e a diversidade desses ataques exigem estratégias abrangentes de segurança cibernética, incluindo medidas preventivas, detecção avançada de ameaças e respostas eficazes a incidentes para proteger adequadamente os ambientes IIoT.

3.3.3 Soluções de segurança cibernética

A segurança cibernética é um campo dinâmico e multidisciplinar que busca proteger sistemas, redes, dados e dispositivos contra ataques digitais. A segurança cibernética envolve a aplicação de medidas, tecnologias e políticas para prevenir, detectar, responder e recuperar de incidentes de segurança. As soluções de segurança cibernética podem variar de acordo com o contexto, o objetivo e o nível de proteção desejado. Nesta seção, apresenta-se alguns exemplos de soluções de segurança cibernética que podem ser usadas em diferentes domínios e cenários.

- Medidas de segurança cibernética: As medidas de segurança cibernética são ações ou práticas que visam reduzir os riscos de segurança e aumentar a resiliência dos sistemas e organizações. As medidas de segurança cibernética podem ser classificadas em três categorias principais: medidas preventivas, medidas reativas e medidas proativas. As medidas preventivas são aquelas que buscam evitar ou impedir que um ataque ocorra, como o uso de senhas fortes, firewalls, antivírus e criptografia. As medidas reativas são aquelas que buscam minimizar o impacto ou a propagação de um ataque que já ocorreu, como o uso de backups, planos de contingência, análise

forense e notificação de incidentes. As medidas proativas são aquelas que buscam antecipar ou identificar possíveis ataques antes que eles causem danos, como o uso de monitoramento, auditoria, testes de penetração e inteligência de ameaças;

- Tecnologias de segurança cibernética: As tecnologias de segurança cibernética são ferramentas ou sistemas que fornecem funcionalidades ou serviços para melhorar a segurança cibernética. As tecnologias de segurança cibernética podem ser classificadas em quatro categorias principais: tecnologias de proteção, tecnologias de detecção, tecnologias de resposta e tecnologias de recuperação. As tecnologias de proteção são aquelas que fornecem mecanismos para impedir ou dificultar que um ataque ocorra, como o uso de autenticação, autorização, controle de acesso e assinatura digital. As tecnologias de detecção são aquelas que fornecem mecanismos para reconhecer ou alertar sobre um ataque que está ocorrendo ou que já ocorreu, como o uso de sistemas de detecção de intrusão, sistemas de prevenção de intrusão e sistemas de gerenciamento de eventos de segurança. As tecnologias de resposta são aquelas que fornecem mecanismos para reagir ou conter um ataque que está ocorrendo ou que já ocorreu, como o uso de sistemas de isolamento, sistemas de bloqueio e sistemas de eliminação de malware. As tecnologias de recuperação são aquelas que fornecem mecanismos para restaurar ou recuperar os sistemas ou dados afetados por um ataque, como o uso de sistemas de backup, sistemas de restauração e sistemas de recuperação de desastres;
- Políticas de segurança cibernética: As políticas de segurança cibernética são normas ou diretrizes que definem os princípios, as responsabilidades, as obrigações e as sanções relacionadas à segurança cibernética. As políticas de segurança cibernética podem ser classificadas em três categorias principais: políticas internas, políticas externas e políticas globais. As políticas internas são aquelas que são estabelecidas por uma organização para regular as atividades de segurança cibernética de seus membros, como o uso de código de conduta, código de ética, código de boas práticas e código de compliance. As políticas externas são aquelas que são estabelecidas por uma entidade externa para regular as atividades de segurança cibernética de outras organizações, como o uso de leis, regulamentos, padrões e acordos. As políticas globais são aquelas que são estabelecidas por uma entidade global para regular as

atividades de segurança cibernética de todas as organizações, como o uso de tratados, convenções, resoluções e declarações.

3.4 INTEGRAÇÃO DA BLOCKCHAIN COM IIoT

A integração da tecnologia Blockchain com a Internet das Coisas Industrial (IIoT) tem sido objeto de estudo em diversos trabalhos científicos. A Blockchain, conhecida por sua natureza descentralizada e imutabilidade de dados, oferece potencial para melhorar a segurança, integridade e confiabilidade das redes IIoT. Segundo Castro, Liskov et al.(33) (1999) , a Blockchain pode trazer oportunidades para solucionar os desafios dos sistemas IoT, tais como descentralização, vulnerabilidade de segurança e privacidade, ponto único de falha e questões de confiança. Neste sentido, o presente texto visa apresentar uma revisão da literatura sobre a integração da Blockchain com o IIoT, destacando seus benefícios, desafios e soluções.

Um estudo conduzido por Alladi et al.(34) (2019) destacou a importância da Blockchain na garantia da integridade dos dados no IIoT. Eles argumentaram que a natureza distribuída e a capacidade de registro imutável da Blockchain podem mitigar riscos de ataques cibernéticos, fornecendo uma camada adicional de segurança aos dispositivos e transações na rede IIoT. Além disso, destacaram a viabilidade da Blockchain para criar um sistema de rastreabilidade eficiente na cadeia de suprimentos industrial.

Outro estudo conduzido por Yang et al.(35) (2023) explorou a aplicação da Blockchain na IIoT para melhorar a segurança e a confiabilidade das transações. Eles enfatizaram que a imutabilidade da Blockchain pode prevenir a falsificação de dados e garantir a autenticidade das informações transmitidas entre dispositivos na rede IIoT. Além disso, propuseram um modelo de consenso adaptativo que visa otimizar a eficiência e a escalabilidade da Blockchain para atender às demandas específicas da IIoT.

Já a pesquisa realizada por Leng et al.(36) (2022) concentrou-se na aplicação da Blockchain para garantir a privacidade e a confidencialidade dos dados na IIoT. Eles discutiram o uso de técnicas de criptografia na Blockchain para preservar a privacidade dos dados gerados pelos dispositivos IIoT, garantindo que apenas partes autorizadas possam acessar e validar essas informações, o que é fundamental em ambientes industriais sensíveis.

Estes estudos evidenciam o potencial significativo da integração da Blockchain com o IIoT, fornecendo um ambiente mais seguro, confiável e eficiente para operações industriais. A interação dessas tecnologias pode revolucionar não apenas a segurança, mas também a confiabilidade e transparência das transações na indústria, abrindo caminho para inovações e avanços substanciais na gestão de dados e operações industriais.

3.4.1 Benefícios da integração da blockchain com IIoT

Um dos principais benefícios da integração da blockchain com o IIoT é a confiança. A blockchain permite que os dispositivos IIoT se comuniquem e interajam de forma segura e confiável, sem a necessidade de intermediários ou autoridades centrais. A blockchain utiliza mecanismos de consenso distribuído para validar as transações e os dados na rede, garantindo que todos os participantes tenham uma visão consistente e atualizada do estado do sistema. Além disso, a blockchain utiliza criptografia para proteger a identidade e a privacidade dos dispositivos e usuários, evitando ataques maliciosos e fraudes.

Outro benefício da integração da blockchain com o IIoT é a transparência. A blockchain possibilita que os dispositivos IIoT compartilhem e armazenem dados de forma transparente e auditável, criando um registro imutável e rastreável de todas as atividades e eventos na rede. A blockchain facilita a verificação e a confirmação da origem, qualidade e autenticidade dos dados, aumentando a credibilidade e a responsabilidade dos participantes. A blockchain também permite que os dispositivos IIoT sejam monitorados e controlados de forma remota e em tempo real, melhorando a eficiência e a produtividade das operações industriais.

Um terceiro benefício da integração da blockchain com o IIoT é a eficiência. A blockchain elimina a necessidade de intermediários e autoridades centrais, reduzindo os custos e os atrasos associados à comunicação e à coordenação entre os dispositivos IIoT. A blockchain também otimiza o uso dos recursos e da energia, minimizando o desperdício e o consumo excessivo. A blockchain ainda possibilita a implementação de contratos inteligentes, que são acordos auto executáveis que podem automatizar e agilizar processos industriais, tais como pagamentos, entregas, manutenções e garantias.

3.4.2 Desafios da integração da blockchain com IIoT

Apesar dos benefícios da integração da blockchain com o IIoT, existem também alguns desafios que precisam ser superados para viabilizar essa convergência. Um dos principais desafios é a escalabilidade. A blockchain enfrenta limitações de desempenho e capacidade para lidar com o grande volume e a alta velocidade dos dados gerados pelos dispositivos IIoT. A blockchain requer um alto consumo de energia e recursos computacionais para executar os algoritmos de consenso e criptografia, o que pode sobrecarregar os dispositivos IIoT, que são tipicamente restritos em termos de poder de processamento e armazenamento. Além disso, a blockchain tem um baixo rendimento e uma alta latência para processar e confirmar as transações e os dados na rede, o que pode comprometer a qualidade e a confiabilidade dos serviços IIoT.

Outro desafio da integração da blockchain com o IIoT é a interoperabilidade. A blockchain enfrenta dificuldades de compatibilidade e comunicação entre as diferentes plataformas e protocolos utilizados pelos dispositivos IIoT. A blockchain tem uma variedade de arquiteturas, modelos e padrões, que podem não ser adequados ou compatíveis com as necessidades e especificações dos dispositivos IIoT. Além disso, a blockchain tem uma complexidade de integração e coordenação com as tecnologias existentes, tais como nuvem, fog e edge computing, que são amplamente utilizadas para prover serviços IIoT. A falta de interoperabilidade pode afetar a eficiência e a funcionalidade dos dispositivos IIoT.

Um terceiro desafio da integração da blockchain com o IIoT é a governança. A blockchain enfrenta questões de regulação e padronização para estabelecer as regras e os princípios que regem o funcionamento e a gestão da rede IIoT. A blockchain tem uma natureza descentralizada e autônoma, que pode entrar em conflito com as normas e as leis existentes, que são tipicamente centralizadas e hierárquicas. Além disso, a blockchain tem uma diversidade de participantes e interesses, que podem não estar alinhados ou coordenados, gerando conflitos e disputas na rede IIoT. A falta de governança pode afetar a segurança e a confiabilidade dos dispositivos IIoT.

3.4.3 Soluções para a integração da blockchain com IIoT

Para superar os desafios da integração da blockchain com o IIoT, diversas soluções têm sido propostas e desenvolvidas na literatura. Uma das soluções é o uso de arquiteturas híbridas ou federadas, que combinam as vantagens das blockchains públicas e privadas, proporcionando um equilíbrio entre escalabilidade, segurança e privacidade. Essas arquiteturas permitem que os dispositivos IIoT se conectem e interajam com diferentes blockchains, de acordo com suas necessidades e preferências, mantendo a autonomia e a flexibilidade da rede IIoT.

Outra solução é o uso de protocolos leves e eficientes, que reduzem a sobrecarga e a latência da comunicação e do processamento na rede IIoT. Esses protocolos permitem que os dispositivos IIoT realizem transações e validações de forma rápida e econômica, sem comprometer a segurança e a confiabilidade da blockchain. Alguns exemplos de protocolos leves e eficientes são o MQTT, o CoAP e o *Internet of Things Application* (IOTA).

Uma terceira solução é o uso de plataformas integradas e padronizadas, que facilitam a interoperabilidade e a governança da rede IIoT. Essas plataformas fornecem uma interface comum e uma arquitetura modular para conectar e gerenciar os dispositivos IIoT e as blockchains, permitindo a troca e o compartilhamento de dados e serviços entre diferentes plataformas e protocolos. Alguns exemplos de plataformas integradas e padronizadas são o Hyperledger, o Ethereum e o Corda.

3.5 DESENVOLVIMENTO DE UMA MICRO-BLOCKCHAIN PARA IIoT

A implementação de uma micro-blockchain é uma abordagem inovadora e desafiadora no campo da tecnologia distribuída. Estudos como o de Berentsen, que recomenda a leitura do artigo seminal de Nakamoto sobre o Bitcoin, fornecem uma base fundamental para entender o funcionamento básico de uma Blockchain. A proposta original de Nakamoto introduziu o conceito de um sistema descentralizado que mantém um registro imutável de transações, possibilitando a criação de uma rede de confiança sem a necessidade de uma autoridade central. Este conceito fundamental continua a inspirar pesquisadores e desenvolvedores na exploração de novas iterações e adaptações da Blockchain.

Em um estudo mais recente conduzido por Anagnostakis et al.(10) (2021), a possibilidade de desenvolver uma micro-Blockchain para a Internet das Coisas (IoT) foi explorada. Eles destacaram a necessidade de uma Blockchain adaptada para dispositivos IoT devido às suas restrições de recursos, como poder de processamento e armazenamento. Propuseram uma abordagem eficiente e otimizada para implementar uma Blockchain em dispositivos com recursos limitados, enfatizando a importância de algoritmos de consenso leves e mecanismos de armazenamento de dados compactos.

Outro estudo de Lu e Xu(37) (2018) focou no desenvolvimento de uma mini-Blockchain para aplicações específicas em sistemas embarcados. Eles enfatizaram a importância de otimizar o desempenho e a eficiência da Blockchain para dispositivos com recursos computacionais restritos. Sua pesquisa propôs um novo algoritmo de consenso e estruturas de dados compactas para atender às demandas de sistemas embarcados, abrindo caminho para a aplicação da Blockchain em uma variedade de dispositivos de baixo consumo energético.

Esses estudos destacam a importância de adaptar a tecnologia Blockchain para atender às demandas de dispositivos e sistemas específicos, como IoT e sistemas embarcados. O desenvolvimento de uma micro-Blockchain representa não apenas um desafio técnico, mas também uma oportunidade para aprimorar a segurança, confiabilidade e eficiência desses dispositivos ao implementar uma camada adicional de confiança e integridade de dados. As pesquisas atuais e futuras nessa área têm o potencial de revolucionar a forma como esses dispositivos interagem e trocam informações em um ambiente cada vez mais conectado.

3.5.1 Conceito de micro-blockchain

Uma micro-Blockchain pode ser definida como uma Blockchain que é projetada para operar em dispositivos com recursos limitados, como os que compõem a Internet Industrial das Coisas (IIoT). A IIoT é uma extensão da IoT que se refere à aplicação de dispositivos inteligentes e conectados em ambientes industriais, como fábricas, minas, portos e usinas. A IIoT visa melhorar a produtividade, a qualidade, a segurança e a sustentabilidade dos processos industriais, por meio da coleta, análise e comunicação de dados em tempo real.

A motivação para o desenvolvimento de uma micro-Blockchain para IIoT surge da necessidade de superar os desafios de segurança, privacidade, confiabilidade e escalabilidade que afetam os sistemas tradicionais de IIoT. Esses sistemas geralmente dependem de uma arquitetura centralizada, que é vulnerável a ataques, falhas, adulterações e congestionamentos. Além disso, os dispositivos de IIoT são frequentemente expostos a ambientes hostis e dinâmicos, que podem comprometer seu funcionamento e sua conectividade.

Os diferenciais de uma micro-blockchain para IIoT são:

- A descentralização, que elimina o ponto único de falha e distribui o controle e a responsabilidade entre os participantes da rede;
- O consenso, que garante a validação e a sincronização das transações entre os dispositivos, sem a necessidade de intermediários ou autoridades centrais;
- A criptografia, que protege os dados e as identidades dos dispositivos, evitando acessos não autorizados ou alterações indevidas;
- Os contratos inteligentes, que permitem a execução automática de ações pré-definidas, baseadas em regras e condições lógicas.

3.5.2 Características de uma micro-blockchain

Uma micro-blockchain deve atender a alguns requisitos específicos para ser adequada para o cenário de IIoT, tais como:

- Leveza, que significa que a micro-blockchain deve consumir poucos recursos de processamento, memória, energia e largura de banda dos dispositivos;
- Flexibilidade, que significa que a micro-blockchain deve se adaptar às mudanças nas condições da rede, como a mobilidade, a heterogeneidade e a intermitência dos dispositivos;
- Interoperabilidade, que significa que a micro-blockchain deve ser capaz de se comunicar com outras redes e sistemas, como a nuvem, a névoa e a borda.

As funcionalidades de uma micro-blockchain são:

- Armazenamento de dados, que consiste em manter um registro distribuído e imutável das transações realizadas pelos dispositivos, formando uma cadeia de blocos;

- Gerenciamento de dispositivos, que consiste em registrar, autenticar, autorizar e monitorar os dispositivos que participam da rede, usando mecanismos de identidade digital;
- Execução de serviços, que consiste em prover, solicitar, negociar e entregar serviços entre os dispositivos, usando contratos inteligentes.

As vantagens de uma micro-blockchain são:

- Segurança, que é reforçada pela criptografia, pelo consenso e pelos contratos inteligentes, que impedem ataques, fraudes e violações de dados;
- Privacidade, que é preservada pela anonimização, pela pseudonimização e pela encriptação dos dados e das identidades dos dispositivos;
- Confiabilidade, que é garantida pela descentralização, pela redundância e pela tolerância a falhas, que evitam interrupções, perdas e inconsistências de dados;
- Eficiência, que é alcançada pela otimização, pela automação e pela coordenação, que reduzem os custos, os tempos e os erros de operação.

3.5.3 Implementação de uma micro-blockchain

A implementação de uma micro-blockchain envolve as seguintes etapas:

- Definição do escopo, que consiste em delimitar o problema, os objetivos, os requisitos e as restrições do projeto;
- Escolha da plataforma, que consiste em selecionar o hardware, o software, o protocolo e o algoritmo mais adequados para o desenvolvimento da micro-Blockchain;
- Desenvolvimento da solução, que consiste em projetar, codificar, testar e depurar a micro-Blockchain, usando as ferramentas escolhidas;
- Avaliação da solução, que consiste em medir, analisar e comparar o desempenho, a segurança, a privacidade e a confiabilidade da micro-Blockchain, usando indicadores e métricas apropriados.

Algumas ferramentas que podem ser utilizadas para a implementação de uma micro-Blockchain são:

- Raspberry Pi, que é um computador de placa única, de baixo custo e baixo consumo, que pode ser usado como um dispositivo de IIoT ou como um nó da micro-blockchain;
- Ethereum, que é uma plataforma de Blockchain de código aberto, que permite a criação de contratos inteligentes e aplicações descentralizadas, usando a linguagem Solidity;
- Hyperledger Fabric, que é uma plataforma de Blockchain de código aberto, que permite a criação de redes privadas e permissionadas, usando a linguagem Go;
- IOTA, que é uma plataforma de Blockchain de código aberto, que permite a criação de redes distribuídas e escaláveis, usando um protocolo baseado em grafos acíclicos direcionados, chamado Tangle;
- Bitcoin-cli, que é um cliente de linha de comando que permite enviar comandos RPC para o bitcoind, que é um daemon que implementa o protocolo Bitcoin. O bitcoin-cli pode ser usado para interagir com a micro-Blockchain, como criar, enviar e validar transações, consultar o saldo e o histórico de um endereço, gerenciar carteiras e chaves, e obter informações sobre a rede e os blocos.

Para ilustrar a implementação de uma micro-blockchain, apresenta-se um exemplo de um projeto desenvolvido por Pan et al.(38) (2018), que consiste em uma rede de sensores inteligentes para monitorar a qualidade do ar em uma cidade. Eles utilizaram o Raspberry Pi como dispositivo de IIoT, o Ethereum como plataforma de Blockchain, o Solidity como linguagem de programação e o Geth como cliente de Blockchain. Eles seguiram os seguintes passos:

- Definiu-se o escopo do projeto, que consistia em coletar, armazenar e analisar dados de qualidade do ar, como temperatura, umidade, pressão e concentração de gases, usando sensores conectados à rede de Blockchain;
- Escolheu-se a plataforma adequada, que consistia em usar o Raspberry Pi como um dispositivo de baixo custo e baixo consumo, que pode executar o Ethereum e o Geth, e se comunicar com outros dispositivos por meio de Wi-Fi ou Bluetooth;
- Desenvolveu-se a solução, que consistia em projetar e codificar os contratos inteligentes que definiam as regras e as funções da rede, como o registro, a autenticação, a autorização e a validação dos dispositivos e dos dados;
- Testou-se e depurou-se a solução, que consistia em verificar o funcionamento e a correção dos contratos inteligentes, usando ferramentas como o Remix e o Truffle;

- Avaliou-se a solução, que consistia em medir e analisar o desempenho, a segurança, a privacidade e a confiabilidade da rede, usando indicadores como o tempo de resposta, o consumo de energia, o consumo de memória e o consumo de largura de banda.

O resultado do projeto foi uma rede de sensores inteligentes que pode monitorar a qualidade do ar de forma segura, confiável e eficiente, usando uma micro-Blockchain. O projeto demonstrou a viabilidade e a utilidade de uma micro-blockchain para aplicações de IIoT, bem como os desafios e as limitações que ainda precisam ser superados.

4 MATERIAIS E MÉTODOS

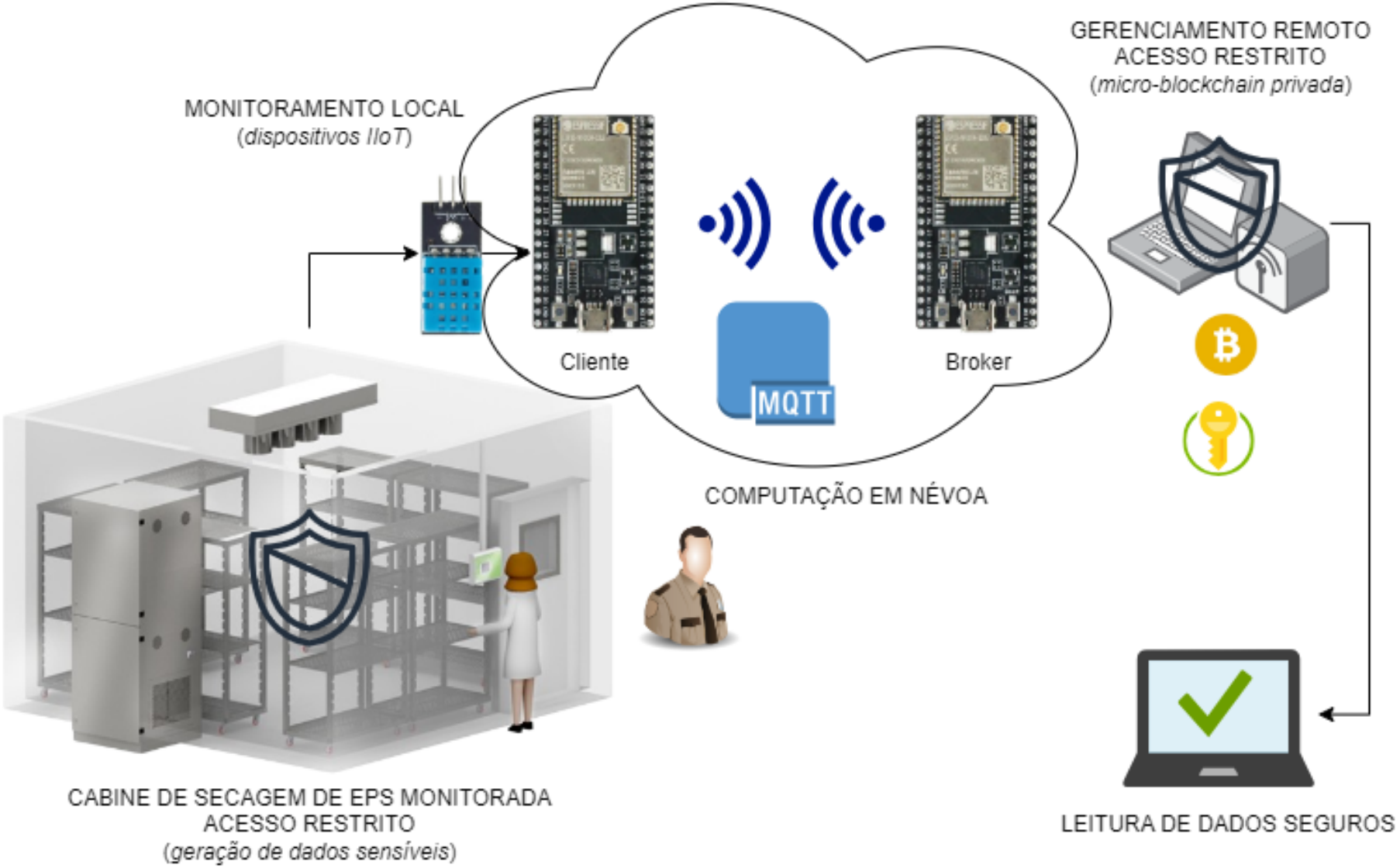
Neste capítulo, são apresentados os materiais e os métodos empregados no desenvolvimento do projeto. A escolha inicial, alinhada ao objetivo deste trabalho, é a utilização de dados referentes à leitura de temperatura de um ambiente. Tal escolha tem como objetivo simular a leitura de temperatura em um ambiente fabril, onde a mínima variação desse valor pode acarretar prejuízos materiais e físicos aos operadores. Em resumo, o presente trabalho tem como objetivo coletar, transmitir e inserir dados de sensores de temperatura e umidade na micro-blockchain privada.

O foco de análise é o ambiente fabril de um forno, devido à sua sensibilidade aos dados. Um exemplo utilizado para ilustrar essa proposta é o processo de secagem do EPS (Poliestireno Expandido, conhecido como isopor) para dispositivos eletrônicos, como televisores. Esse processo, exemplificado por uma empresa no polo industrial de Manaus, envolve a inserção do EPS não seco na sala do forno, seguido pela remoção do EPS seco para ser utilizado como suporte para eletrônicos.

Os aspectos críticos que este estudo pretende abordar em relação ao forno incluem: a temperatura do ambiente, que não pode sofrer alterações durante o processo de secagem para garantir a qualidade final do produto; a temperatura ambiente quando os operadores ou equipamentos (como o robô AGV - Automated Guided Vehicle de coleta) entram na sala para retirar o EPS final; e a umidade da sala, que não deve variar abruptamente. Portanto, os dados sensíveis tratados neste estudo se concentram principalmente na temperatura e umidade.

Além disso, este trabalho incorpora o uso de dispositivos IoT para simular um ambiente fabril. O sensor de temperatura DHT11 é empregado exclusivamente para medir a temperatura e a umidade do ambiente. Embora para aplicações industriais seja recomendado um sensor mais robusto, neste estudo, um ambiente simulado é desenvolvido para representar esses cenários. O sensor de umidade e temperatura enviará sinais para o dispositivo ESP32 WROOM, que atua como dispositivo IIoT para o caso proposto. A escolha do ESP32 se deu devido ao seu desempenho de processamento e capacidade de armazenamento superiores, conforme demonstrado em análise comparativa de hardware e da proposta do trabalho "*IoT Micro-Blockchain Fundamentals*".

Figura 12 – Proposta do desenvolvimento de uma micro-blockchain utilizando dispositivos IIoT



Fonte: Autor, 2024

4.1 CABINE DE SECAGEM DE EPS MONITORADA - ACESSO RESTRITO

Para efeitos de estudo comparativo, a cabine de segurança para o presente trabalho de dissertação de mestrado consiste em uma sala de laboratório do CETELI, na qual a temperatura está sendo avaliada ao longo de um período estimado de três horas durante três dias semanais. Este ambiente experimental foi selecionado devido à sua capacidade de proporcionar condições controladas e reprodutíveis, essenciais para a realização de análises precisas e confiáveis. A escolha de realizar as avaliações ao longo de um período de três dias por semana visa garantir a obtenção de dados representativos e robustos, permitindo uma análise abrangente e detalhada dos resultados obtidos.

A utilização da cabine de segurança como cenário experimental proporciona um ambiente controlado que minimiza a interferência de variáveis externas, garantindo assim a confiabilidade dos resultados obtidos. Além disso, a padronização das condições experimentais contribui para a consistência dos dados coletados ao longo do estudo. Desta forma, torna-se possível realizar uma análise comparativa precisa entre o sensor em avaliação e os sensores de referência utilizados na indústria.

No contexto específico de um ambiente fabril, tal como aquele encontrado nas empresas do Polo Industrial de Manaus, a temperatura em uma sala de secagem de poliestireno expandido (EPS) pode apresentar variações significativas. Empresas como a Samsung Eletrônica da Amazônia Ltda e Panasonic do Brasil Limitada, que operam no Polo Industrial de Manaus, podem experimentar tais variações de temperatura em suas salas de secagem, devido às condições climáticas locais e aos processos de produção específicos.

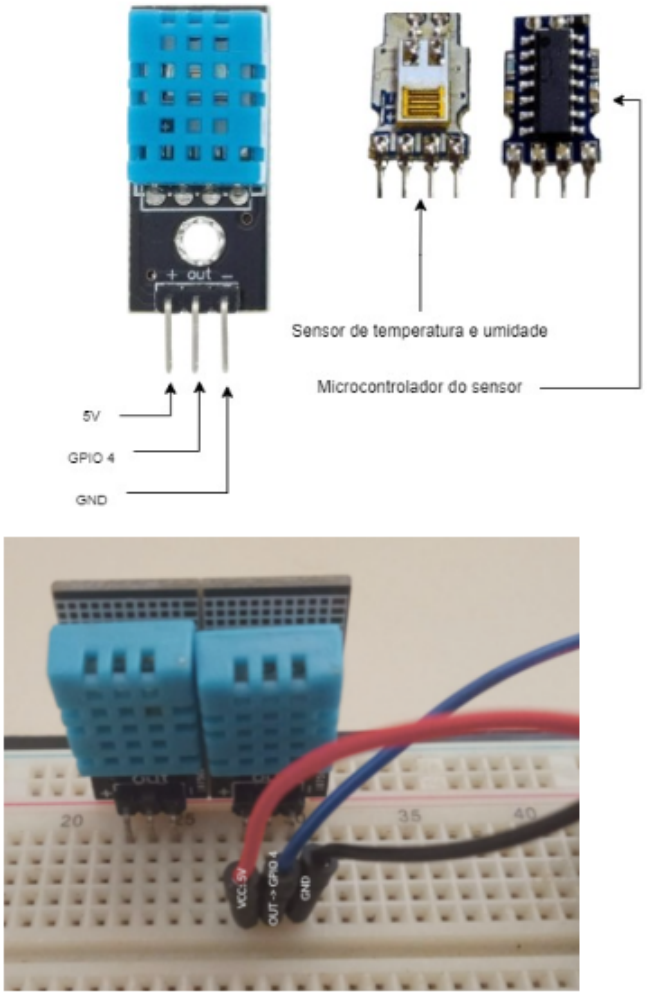
Da mesma forma, a umidade nesses ambientes pode apresentar variações consideráveis. Essas variações de temperatura e umidade são críticas para o processo de secagem do EPS e podem impactar diretamente a qualidade do produto final.

Ao delimitar o período de avaliação para três horas durante três dias semanais, busca-se capturar variações temporais significativas na temperatura, permitindo uma avaliação abrangente do desempenho dos sensores em diferentes condições ambientais. Esta abordagem permite identificar possíveis padrões ou tendências no comportamento dos sensores ao longo do tempo, possibilitando uma compreensão mais completa de suas características e limitações.

4.2 MONITORAMENTO LOCAL

4.2.1 Sensor de Temperatura

Figura 13 – Módulo sensor de temperatura DHT11



Fonte: Autor, 2024

A fonte de coleta dos dados utilizada no projeto é um sensor DHT11 (*Digital Humidity and Temperature*), que é um sensor digital de temperatura e umidade, capaz de medir valores entre 0 e 50 °C e entre 20 e 90% de umidade relativa do ar, com uma precisão de ±2 °C e ±5%. O sensor DHT11 é uma ferramenta simples, barata e de fácil utilização, sendo adequada para aplicações de monitoramento em ambientes industriais.

O sensor em análise está sendo empregado em uma simulação realizada em um ambiente de laboratório, onde está sendo comparado com sensores de temperatura amplamente utilizados na indústria, tais como os termopares tipo K, as termorresistências

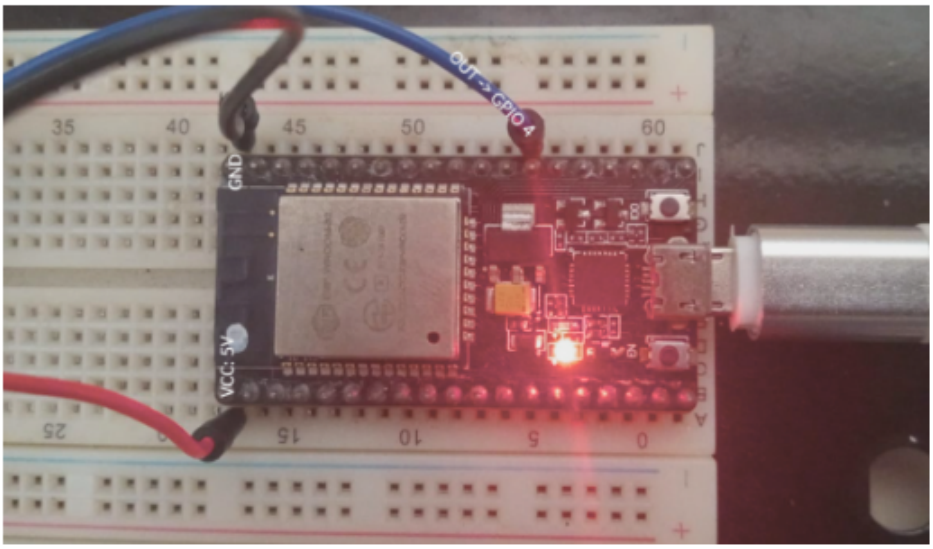
Pt100 e os termopares de isolamento mineral (MI). Estes sensores industriais possuem características distintas, como alta resistência a elevadas temperaturas, precisão e robustez em ambientes industriais rigorosos. Por outro lado, o sensor DHT11 é mais simplificado e projetado para aplicações de uso geral, podendo ser empregado, como no presente estudo, para fins puramente comparativos em relação aos sensores industriais. Diante do contexto de monitoramento de processos de secagem, como é o caso do EPS, os sensores industriais mencionados demonstram ser mais adequados para tal finalidade.

Os dados de temperatura e umidade coletados serão transmitidos ao microcontrolador IoT por meio da porta "*out*"do módulo do sensor de temperatura. A conexão entre o sensor e o microcontrolador será estabelecida por meio de *jumpers*. Um *jumper* será utilizado para fornecer a alimentação DC (Corrente Contínua) ao sensor, enquanto outro *jumper* utilizará o GND como terra do sensor, e o terceiro pino será responsável pelo envio dos dados.

4.3 MONITORAMENTO LOCAL E COMPUTAÇÃO EM NÉVOA

4.3.1 Microcontrolador ESP32

Figura 14 – ESP32 WROOM - Plataforma de desenvolvimento (Cliente)



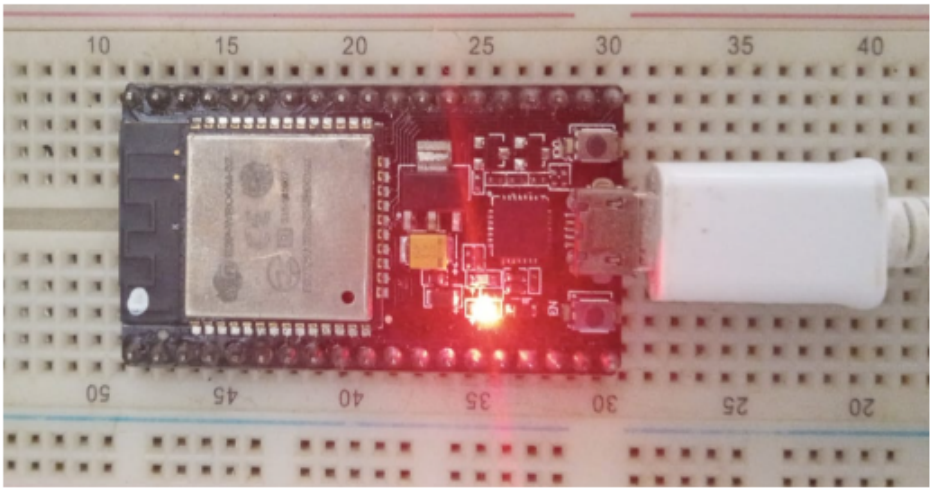
Fonte: Autor, 2024

O microcontrolador adotado no presente projeto é o ESP32 WROOM, selecionado como dispositivo IoT para a transmissão de dados. Ele desempenha igualmente o papel de

dispositivo de borda tanto na emissão quanto na recepção de informações, contribuindo para a configuração da computação em névoa. Exclusivamente um ESP32 (Publisher - Client) mantém a conexão física direta com o sensor de temperatura. Fundamentalmente, este microcontrolador provê a alimentação de 5V para o sensor, estabelece o GND e, por meio da GPIO 4, recebe os sinais provenientes do terminal "out"do sensor. A programação do ESP32 conectado ao sensor é elaborada mediante a utilização da IDE do Arduino, realizando-se ajustes nas bibliotecas para promover a comunicação entre o ESP32 e o sensor.

O outro microcontrolador ESP32 (Broker) é conectado ao servidor através da porta serial USB (*Universal Serial Bus*) de um notebook com processador Intel(R) Core(TM) i7-8565U CPU 1.80GHz 1.99 GHz. A função do cliente consiste em transmitir os dados fornecidos pelo sensor, enquanto a função do broker envolve a coleta e a gestão da rede, com os dados coletados sendo encaminhados ao servidor central. Para permitir a comunicação entre ambos os microcontroladores, são definidos os endereços IP locais (IPAddress local_IP(10, 224, 2, 32)), bem como o gateway (IPAddress gateway(10, 224, 2, 63)) e a máscara de sub-rede (IPAddress subnet(255, 255, 0, 0)). A conexão ocorre por meio de Wi-Fi (IEEE 802.11).

Figura 15 – ESP32 WROOM - Plataforma de desenvolvimento (Broker)



Fonte: Autor, 2024

É importante ressaltar que a capacidade de memória do ESP32 (*Espressif Systems 32-bit Microcontroller*) excede a proposição delineada no artigo "*IoT Micro-Blockchain Fundamentals*". Entretanto, no âmbito da cibersegurança, constata-se que nenhum dos dispositivos possui a capacidade mínima para conduzir uma transação segura. Nesse sentido,

para o propósito em foco, o hardware IIoT (*Industrial Internet of Things*) é empregado exclusivamente para a coleta de dados, sendo que a segurança cibernética desses dados será garantida por um servidor incumbido de operar uma rede blockchain.

Tabela 4 – Análise comparativa entre hardwares para comunicação IIoT

Características	**ESP32 WROOM**	**Arduino Nano 33 IoT**
Processador	Dual-core Tensilica LX6, 240 MHz	ARM Cortex-M0+, 48 MHz
Conectividade	Wi-Fi, Bluetooth de Baixa Energia	Wi-Fi, Bluetooth de Baixa Energia
Armazenamento	Flash de até 16 MB, SRAM de até 520 KB	Flash de 256 KB, SRAM de 32 KB
Memória	520 KB de SRAM	32 KB de SRAM
Transação de Dados	Alta capacidade devido ao processamento rápido e conectividade Wi-Fi	Capacidade limitada em comparação com o ESP32 devido ao processamento mais lento e capacidade de comunicação reduzida
Disponibilidade IIoT	Adequado para aplicações IIoT devido à capacidade de processamento e conectividade	Limitado devido ao processamento mais lento e menor capacidade de comunicação; adequado apenas para aplicações IIoT menos exigentes

Fonte: Autor, 2024.

Tal aspecto é determinante, pois a integração da IIoT com uma blockchain privada se dá mediante o envio de dados por intermédio do protocolo MQTT (*Message Queuing Telemetry Transport*). Para aferir a aptidão do hardware em executar uma blockchain segura, é imperativo avaliar aspectos como o tamanho da blockchain, a eficiência do protocolo, sua escalabilidade e a sensibilidade dos dados transacionados.

Adicionalmente, o tamanho mínimo de uma chave segura varia conforme o algoritmo de criptografia adotado e o modelo de ameaça inerente à aplicação em análise. Atualmente, preconiza-se o emprego de uma chave RSA (*Rivest-Shamir-Adleman*) de 2048 bits ou uma chave ECDSA (*Elliptic Curve Digital Signature Algorithm*) de 256 bits para a maioria dos contextos, a fim de assegurar um nível satisfatório de segurança, ao passo que otimiza o desempenho e a experiência do usuário. Isso corresponde a 256 bytes para RSA e 32 bytes para ECDSA. Consequentemente, a utilização dos microcontroladores se restringe

ao envio e recebimento de dados, sem que qualquer um deles incorpore um sistema de cibersegurança embutido.

4.3.2 Protocolo MQTT

Neste estudo, o protocolo MQTT foi selecionado para atender ao critério estabelecido de empregar um protocolo suscetível a ataques cibernéticos. Este protocolo é particularmente relevante no contexto de uma rede interna de dispositivos IIoT, onde cria um paradigma de "computação em névoa". Neste paradigma, a informação é restrita a uma área geográfica específica (neste caso, a empresa) e o acesso é controlado por meio de autorização. É importante notar que, entre os protocolos de comunicação IIoT, o MQTT é frequentemente o mais exposto a potenciais ameaças cibernéticas.

Tabela 5 – Análise dos tipos de ciberataque IIoT com o devido protocolo

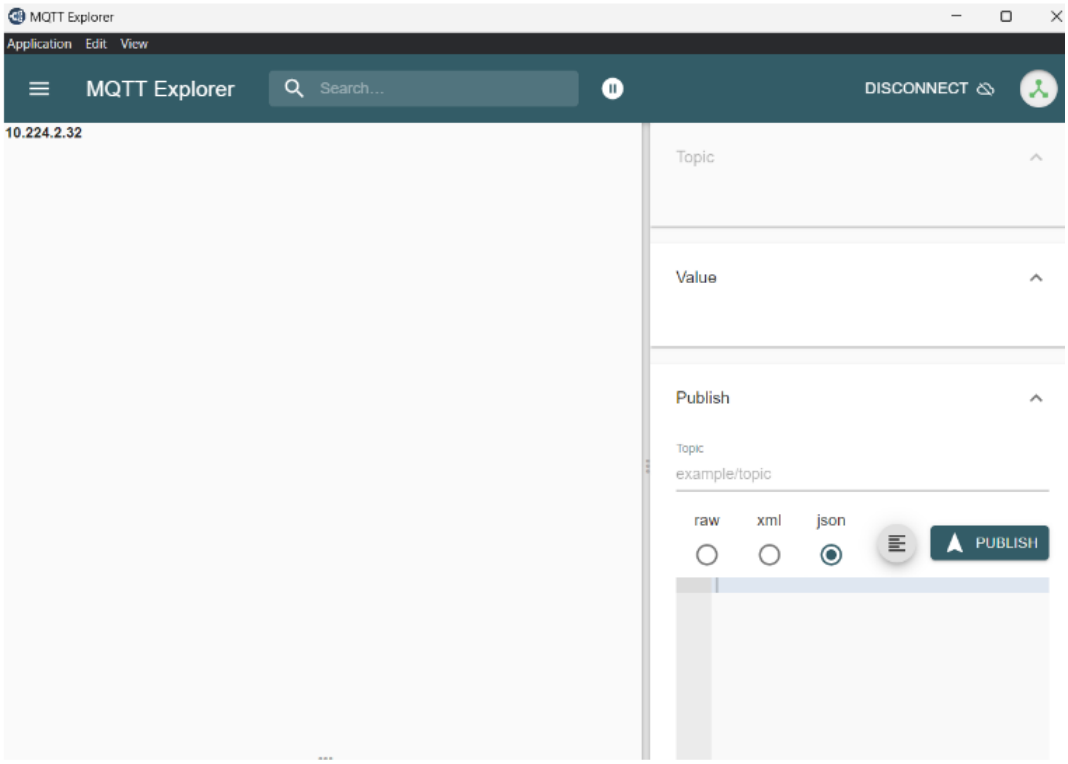
Tipo de ciberataque	**Protocolo atacado**
Ransomware	MQTT, OPC UA, CoAP, AMQP
Phishing	MQTT, OPC UA, CoAP, AMQP
Malware	MQTT, OPC UA, CoAP, AMQP
Spear Phishing	MQTT, OPC UA, CoAP, AMQP
DDoS	MQTT, OPC UA, CoAP, AMQP
Injeção SQL	MQTT, OPC UA, CoAP, AMQP
Rootkits	MQTT, OPC UA, CoAP, AMQP
Man-in-the-Middle	MQTT, OPC UA, CoAP, AMQP

Fonte: Autor, 2024.

Na configuração física do MQTT, foram utilizados dispositivos ESP32, cada um atribuído a uma função específica. Um dos dispositivos desempenhou o papel de cliente (publicador), enquanto o outro atuou como servidor (broker). Para a avaliação da rede, foi empregado o MQTT Explorer. A configuração foi realizada conforme descrito a seguir:

- Configuração do ESP32 como cliente (publicador): O ESP32 designado como cliente foi programado para publicar mensagens em um tópico específico no servidor MQTT. Isso foi realizado mediante a utilização da biblioteca PubSubClient na IDE do Arduino;
- Configuração do ESP32 como broker: O segundo ESP32 foi configurado para funcionar como broker MQTT. Para essa finalidade, foi empregada a biblioteca ESPMQTT-Broker na IDE do Arduino;
- Teste da rede com o MQTT Explorer: Para verificar a funcionalidade da rede, recorreu-se ao MQTT Explorer. Inicialmente, estabeleceu-se uma conexão com o servidor MQTT, inserindo o endereço IP, que é 10.224.2.32, e a porta padrão MQTT (1883). Após a conexão bem-sucedida, foi possível visualizar as mensagens publicadas pelo ESP32 cliente no tópico especificado.

Figura 16 – Teste MQTT Explorer



Fonte: Autor, 2024

Uma metodologia alternativa para a configuração da comunicação via protocolo MQTT, que engloba a visualização dos dados coletados pelo sensor e transmitidos aos dispositivos ESP32 por meio de um painel de controle, envolve a utilização do software

Node-Red. A implementação desta metodologia foi realizada seguindo uma sequência específica de etapas, descritas a seguir de forma detalhada:

- Instalação do Software: A primeira etapa envolveu a instalação do software Node-Red. Isso foi realizado através do prompt de comando, utilizando o comando npm install -g –unsafe-perm node-red;
- Estabelecimento da Conexão: Após a instalação do software, a conexão entre o Node-Red e os dispositivos ESP32 foi estabelecida. Isso foi feito através da interface do Node-Red, adicionando um nó de entrada MQTT e configurando-o com as informações do broker MQTT e do tópico ao qual os dispositivos ESP32 estavam publicando;
- Determinação da URL do Node-Red: Antes de prosseguir com a configuração do painel de controle, foi necessário determinar a URL do Node-Red. Para isso, o prompt de comando foi aberto e o comando node-red foi executado. Isso iniciou o servidor Node-Red e exibiu a URL na qual ele estava sendo executado.;Configuração do Painel de Controle: Com a URL do Node-Red disponível, o painel de controle no Node-Red foi configurado. Isso foi feito adicionando um nó de painel de controle na interface do Node-Red e conectando-o ao nó de entrada MQTT;
- Transmissão de Dados: Os dados coletados foram então transmitidos dos dispositivos ESP32 para o Node-Red. Isso foi feito automaticamente uma vez que o nó de entrada MQTT estava configurado corretamente e o Node-Red estava em execução;
- Visualização de Dados: Finalmente, os dados transmitidos foram visualizados no painel de controle do Node-Red. Isso foi feito acessando a URL do Node-Red em um navegador web.

4.4 GERENCIAMENTO REMOTO - ACESSO RESTRITO

O servidor de coleta, que é essencial para o recebimento dos dados, é um computador pessoal equipado com um processador Intel® Core™ i7-8565U CPU operando a 1.80GHz e capaz de atingir até 1.99 GHz. Este computador foi configurado com o Windows Subsystem for Linux (WSL2), permitindo a execução interna da aplicação micro-blockchain.

As portas seriais do computador foram empregadas de maneira específica: uma das portas foi utilizada para comunicação e alimentação com o ESP32 broker, enquanto a outra foi destinada à alimentação do ESP32 subscriber. Vale ressaltar que os dispositivos estavam dispostos a uma distância máxima de 1.5m entre si, uma configuração que se alinha ao objetivo deste projeto de estudar tais aplicações em um cenário comparativo.

Além disso, o servidor foi empregado para programar os dispositivos ESP32 por meio da IDE Arduino, demonstrando sua versatilidade e importância para o projeto.

4.4.1 Micro-blockchain Privada

Neste trabalho, o Windows Subsystem for Linux (WSL2) foi empregado como ambiente de comunicação interna para uma micro-blockchain privada. A micro-blockchain privada é definida como tal devido às suas características semelhantes às de uma blockchain privada, porém com limitações de recursos. Isso significa que a configuração é delimitada a um objetivo específico, visando evitar a perda de processamento e permitindo a execução em um computador pessoal comum.

A micro-blockchain privada deste estudo apresenta várias características alinhadas ao seu objetivo, essas características que a torna um trabalho inovador são descritas como:

- UTXOs do tipo “unspendable”: UTXO é a sigla para “Unspent Transaction Output”, ou “Saída de Transação Não Gasta” em português. São basicamente os ativos que foram recebidos mas ainda não foram gastos. Neste caso, todos os UTXOs são do tipo “unspendable”, o que significa que não podem ser gastos. Essa característica foi adotada para simplificar o modelo de transação e evitar a necessidade de gerenciar saldos e endereços na micro-blockchain;
- Ausência de competição de mineração entre os nós: A mineração é um processo que adiciona registros de transações ao livro público de transações passadas, chamado blockchain. Neste caso, não há competição de mineração entre os nós, o que significa que todos os nós cooperam entre si, em vez de competir para adicionar o próximo bloco à blockchain. Essa característica foi adotada para reduzir o consumo de recursos e o tempo de confirmação das transações na micro-blockchain;

- Baixo poder computacional necessário: A geração e manutenção dos blocos não requer grande poder computacional, tornando o sistema mais eficiente em termos de energia. Essa característica foi adotada para permitir que os dispositivos IIoT participem da micro-blockchain sem sobrecarregar suas capacidades e baterias;
- Uso de Prova de Trabalho (PoW) para produzir o carimbo de data/hora: A Prova de Trabalho é um algoritmo usado para confirmar transações e produzir novos blocos na blockchain. Neste caso, o PoW é usado para produzir o carimbo de data/hora, que é uma forma de garantir que os dados não foram adulterados. Essa característica foi adotada para aumentar a confiabilidade e a integridade dos dados na micro-blockchain;
- Armazenamento de dados na própria blockchain: Ao contrário de alguns outros sistemas, onde os dados são armazenados em um banco de dados separado, neste caso, os dados são armazenados diretamente na blockchain. Isso simplifica a arquitetura do sistema e aumenta a segurança, pois os dados estão protegidos pelas mesmas medidas de segurança que protegem a blockchain.

A configuração de acesso da micro-blockchain segue os paradigmas da segurança da informação, incluindo:

- Confidencialidade: Somente o usuário com acesso ao terminal do computador e acesso à senha poderá ler os registros e editar a micro-blockchain privada;
- Integridade: Garante que os dados não sejam alterados ou destruídos de maneira não autorizada;
- Disponibilidade: Assegura que os usuários autorizados tenham acesso aos dados quando necessário;
- Autenticidade: Confirma a identidade dos usuários, garantindo que eles sejam quem afirmam ser;
- Não-repúdio: Garante que uma operação ou evento não possa ser negado posteriormente.

Com base nas descrições apresentadas em seções anteriores deste trabalho, optou-se por utilizar a máquina virtual Linux Ubuntu dentro do ambiente *Windows Subsystem for Linux 2* (WSL2). A escolha por esta plataforma deve-se às suas funcionalidades e à sua ampla aplicação em pesquisas que envolvem a tecnologia blockchain.

Adotou-se uma blockchain privada configurada segundo as diretrizes do Bitcoin SV (Satoshi Vision). A escolha por esta modalidade de blockchain foi motivada pela sua alta capacidade de processamento de transações, quando comparada a outros modelos de blockchain.

Tabela 6 – Análise comparativa entre modelos de blockchain

Aspecto	**Bitcoin SV (BSV)**	**Bitcoin (BTC)**	**Ethereum (ETH)**
Tamanho Máximo do Bloco	Ilimitado	1 MB	N/A (Variável)
Velocidade de Transação	Rápida	Lenta	Rápida
Taxas	Reduzidas	Variável	Variável
Escalabilidade	Alta	Baixa	Alta
Algoritmo de Consenso	PoW (Proof of Work)	PoW (Proof of Work)	PoW (Proof of Work)
Contratos Inteligentes	Sim	Não	Sim

Fonte: Autor, 2024.

A configuração do servidor foi realizada no ambiente WSL2, especificamente na máquina virtual Ubuntu Linux. Este servidor foi designado para hospedar a função de Cliente de Chamada de Procedimento Remoto (RPC), que atua como uma interface de comunicação entre o agente IIoT e a micro-blockchain desenvolvida.

A função de cliente RPC adota o modelo do bitcoin-cli (com a configuração BSV), uma interface de linha de comando para o Bitcoin Core. Esta interface permite a interação com a blockchain através de comandos RPC. Através desta função, o agente IIoT tem a capacidade de enviar dados de leitura do sensor, que são inseridos manualmente na micro-blockchain. Estes dados são convertidos para o formato hexadecimal, utilizando um passo de conversão decimal para hexadecimal, que é implementado internamente no código Arduino desenvolvido e aplicado no ESP32 broker. O formato hexadecimal é compacto e seguro, minimizando a possibilidade de perda ou corrupção de dados durante a transmissão.

Além disso, a função de cliente RPC permite que o agente IIoT recupere dados da blockchain quando necessário, através de consultas RPC.

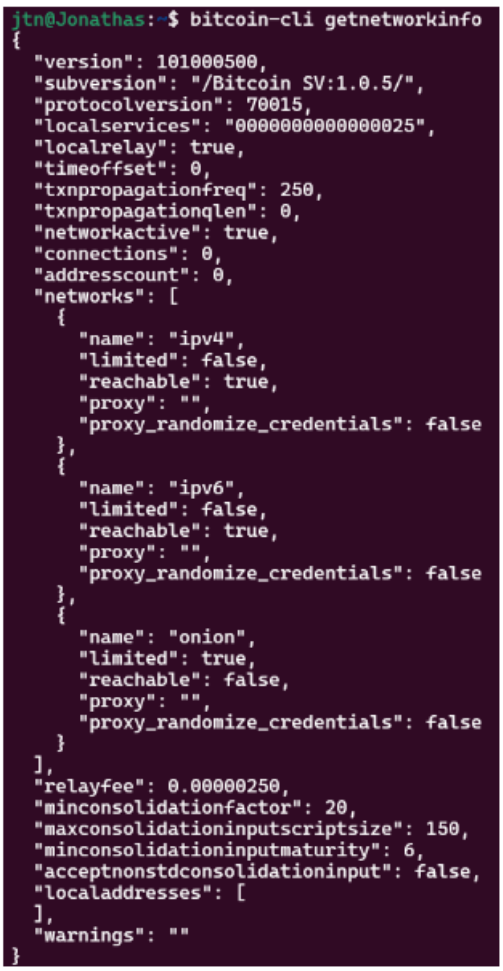
Figura 17 – Tela de informações da capacidade da micro-blockchain

Fonte: Autor, 2024

Para a análise da configuração da blockchain e das redes de comunicação interna, foram empregados os comandos bitcoin-cli (*Bitcoin Core Interface*) getblockchaininfo e bitcoin-cli getnetworkinfo, respectivamente. A execução desses comandos possibilita a visualização das configurações pertinentes ao modelo Bitcoin SV (BSV) utilizado. O comando bitcoin-cli getblockchaininfo fornece informações detalhadas sobre o estado atual da blockchain, enquanto o comando bitcoin-cli getnetworkinfo revela as configurações das redes de comunicação interna. A utilização desses comandos demonstra a aplicação do modelo BSV no contexto deste trabalho.

A micro-blockchain denominada “privbc” desempenha o papel na coleta de dados e na subsequente inserção desses dados no formato “blockchain” (formato encriptado). Após a realização dessas operações, é gerada uma chave privada que está intrinsecamente associada à informação em questão. Este processo garante a segurança e a integridade dos dados manipulados.

Figura 18 – Tela de informações da rede de comunicação da micro-blockchain



Fonte: Autor, 2024

Na estrutura da WSL2, identifica-se a presença de uma função designada como cliente RPC, a qual recebeu a denominação de “privbc”. Este termo é um acrônimo que se refere à “blockchain privada”. A escolha deste nome foi motivada pela característica intrínseca de privacidade que a blockchain apresenta, além de sua conformidade com o modelo estabelecido pelo bitcoin-cli. Esta nomenclatura foi adotada com o intuito de evidenciar tanto a natureza privada da blockchain quanto a sua aderência ao referido modelo.

4.4.2 Servidor Blockchain WEB3

Na fase denominada “blockchain web3”, emprega-se a chave privada gerada na micro-blockchain privada. Esta última é caracterizada por sua conexão exclusiva à internet

local, também conhecida como intranet, uma rede de comunicação interna cujo único dispositivo de borda com a internet externa é o servidor que utiliza a blockchain.

Após a obtenção da chave privada, é crucial proceder à conversão dos dados gerados no formato WIF para o formato hexadecimal. Esta etapa é inerente ao uso do tipo de WSL2. Para tal, recorre-se a uma das funcionalidades disponíveis no sítio "carlosam-cruz.github.io/websvmenu/", desenvolvida especificamente para atender às necessidades deste trabalho de mestrado.

Figura 19 – Página de conversão da chave privada no formato WIF para o formato Hexadecimal

Fonte: Autor, 2024

Depois de ter a chave convertida, recorre-se a um site específico para efetuar a transação dos dados já seguros. Este site opera sob a mesma configuração do modelo de blockchain SV. Para a realização das transações no modelo blockchain, utiliza-se a Testnet como ambiente de operação. Esta escolha se deve ao fato de que a Testnet não está disponível ao público em geral, o que está em conformidade com a característica de privacidade da micro-blockchain.

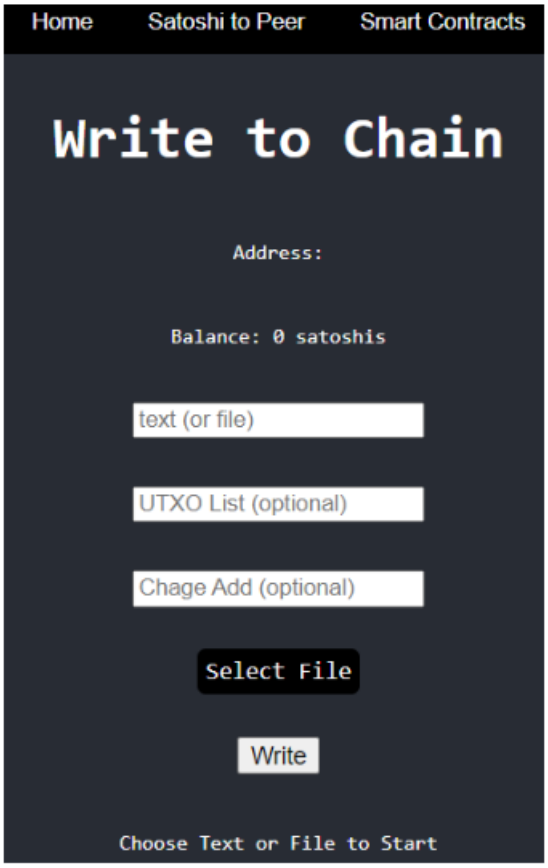
Figura 20 – Página de inserção da chave privada na rede de teste

Fonte: Autor, 2024

Com o objetivo de gerar um *faucet* para a transação dos dados associados à chave privada, recorre-se ao recurso disponível no portal eletrônico scrypt.io/faucet. Neste ambiente digital, procede-se à inserção da chave privada, que foi previamente gerada na micro-blockchain privada. Este procedimento possibilita que os dados possam ser retransmitidos em qualquer blockchain que esteja conectada, garantindo assim a integridade e a segurança das informações manipuladas.

Seguido da liberação dos faucets, que correspondem a pequenas quantidades de criptomoedas, recorre-se ao recurso “Write to Chain” disponibilizado no portal carlosam-cruz.github.io/websvmenu/. Este recurso é utilizado para registrar os dados na blockchain privada. Com isso, inicia-se a etapa de transação, que consiste na troca de informações entre servidores autorizados. A confirmação do recebimento dos dados pode ser realizada por meio do portal test.whatsonchain.com. Este procedimento assegura a integridade e a segurança das informações transacionadas.

Figura 21 – Página para escrever o dado a ser transacionado transação dos dados utilizando a chave privada



Fonte: Autor, 2024

4.5 LEITURA DOS DADOS SEGUROS

A leitura de dados seguros será realizada no ambiente do próprio computador, porém integrada à infraestrutura da WEB3. A validação da leitura ocorrerá em um site dedicado ao processo de leitura, utilizando a chave privada gerada na micro-blockchain em conjunto com a chave pública do ambiente WEB3. Essa integração entre o ambiente local e a plataforma WEB3 garante a segurança e a autenticidade dos dados durante todo o processo de leitura e validação. Essa abordagem, ao utilizar a chave privada da micro-blockchain em conjunto com a infraestrutura da WEB3, proporciona uma camada adicional de segurança, assegurando a integridade dos dados e prevenindo potenciais violações de segurança. Assim, ao estabelecer uma conexão entre o ambiente local e a plataforma WEB3, é possível garantir a confiabilidade das operações de leitura de dados em um contexto seguro e confiável.

5 RESULTADOS E DISCUSSÕES

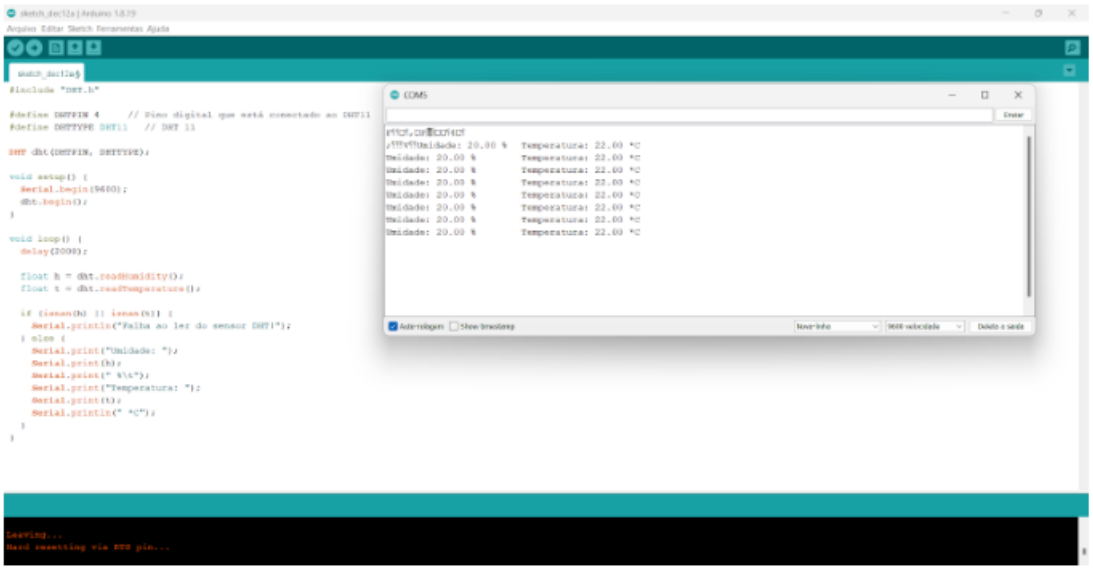
5.1 MONITORAMENTO LOCAL - SENSOR DE TEMPERATURA

Um dos principais resultados apresentados nesta pesquisa refere-se à coleta de dados por meio da leitura do sensor de temperatura e umidade. Essas leituras foram realizadas utilizando o sensor DHT11, que transmitia as informações para o ESP32. Posteriormente, o ESP32 retransmitia essas informações por meio da porta serial para a COM5, conforme visualizado no monitor serial da IDE do Arduino.

As leituras foram realizadas em intervalos de três dias por semana, com cada sessão de leitura durando aproximadamente duas horas. No ambiente simulado, a temperatura máxima registrada foi de 36 °C e a mínima foi de 19 °C, esta última obtida com o auxílio de um ar condicionado. Portanto, a taxa de variação de temperatura observada foi de 17 °C.

Quanto à umidade, a máxima registrada no ambiente controlado foi de 45%, observada próximo às janelas durante um período chuvoso. A umidade mínima registrada foi de 20%, valor este que está abaixo do que é geralmente definido como a umidade ideal para um ambiente interno. Portanto, a taxa de variação de umidade observada foi de 25%.

Figura 22 – Leitura da temperatura e da umidade feita pelo sensor DHT11 e comunicação serial COM5



Fonte: Autor, 2024

5.2 MONITORAMENTO LOCAL - COMUNICAÇÃO SERIAL DO ESP32

A interface de comunicação serial, mais especificamente a Universal Serial Bus (USB), desempenha um papel crucial na coleta e transmissão de dados em sistemas embarcados. No âmbito deste estudo, o microcontrolador ESP32 foi utilizado, empregando a mencionada interface para adquirir dados de um sensor de temperatura e umidade.

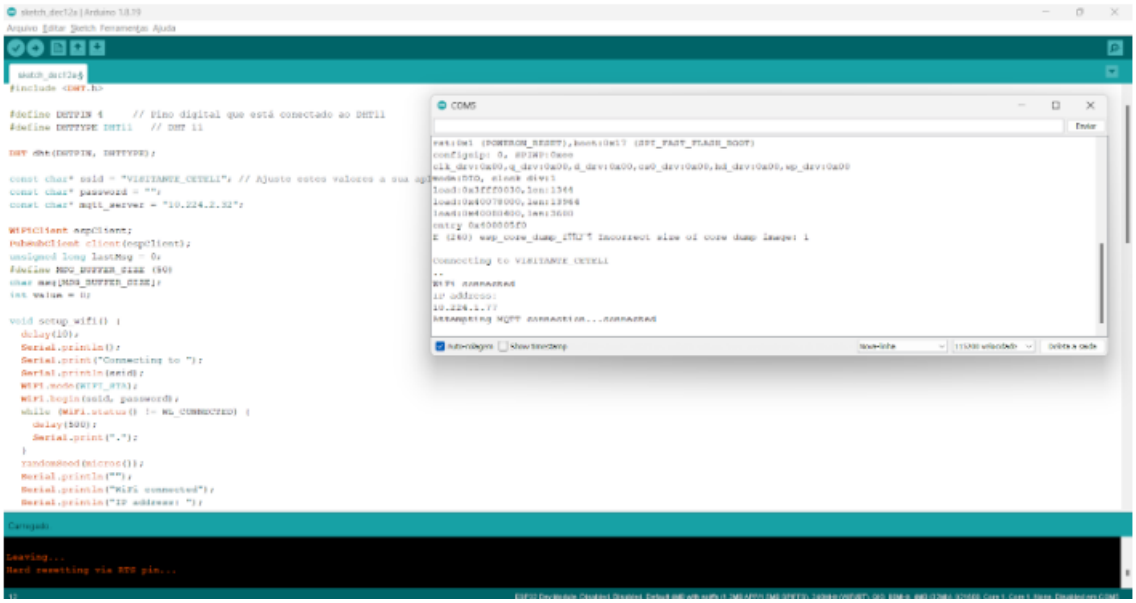
Após a coleta, os dados foram transmitidos para outro microcontrolador ESP32, que estava conectado à mesma rede. Esta metodologia possibilitou uma troca de informações eficaz entre os dispositivos, contribuindo para a precisão e confiabilidade dos dados coletados.

Adicionalmente, as portas seriais USB foram empregadas para fornecer energia aos microcontroladores ESP32. Esta funcionalidade simplifica o design do sistema, eliminando a necessidade de uma fonte de alimentação externa. Portanto, a interface de comunicação serial não apenas facilita a coleta e transmissão de dados, mas também fornece energia para os microcontroladores, destacando sua importância em sistemas embarcados.

5.3 COMPUTAÇÃO EM NÉVOA - COMUNICAÇÃO DO PROTOCOLO MQTT

A implementação do protocolo de comunicação foi conduzida em duas fases distintas, envolvendo o MQTT Explorer e o Node-RED. Na primeira fase, foi desenvolvido um código específico para o microcontrolador ESP32, com a finalidade de publicar no MQTT os valores de temperatura e umidade coletados. Na segunda fase, foi elaborado um código para o ESP32 broker, com o objetivo de receber e coletar os dados publicados pelo primeiro ESP32. Os códigos desenvolvidos para estas fases estão detalhadamente descritos no anexo do presente trabalho de dissertação. Esta abordagem estruturada possibilitou uma implementação eficaz e robusta do protocolo de comunicação.

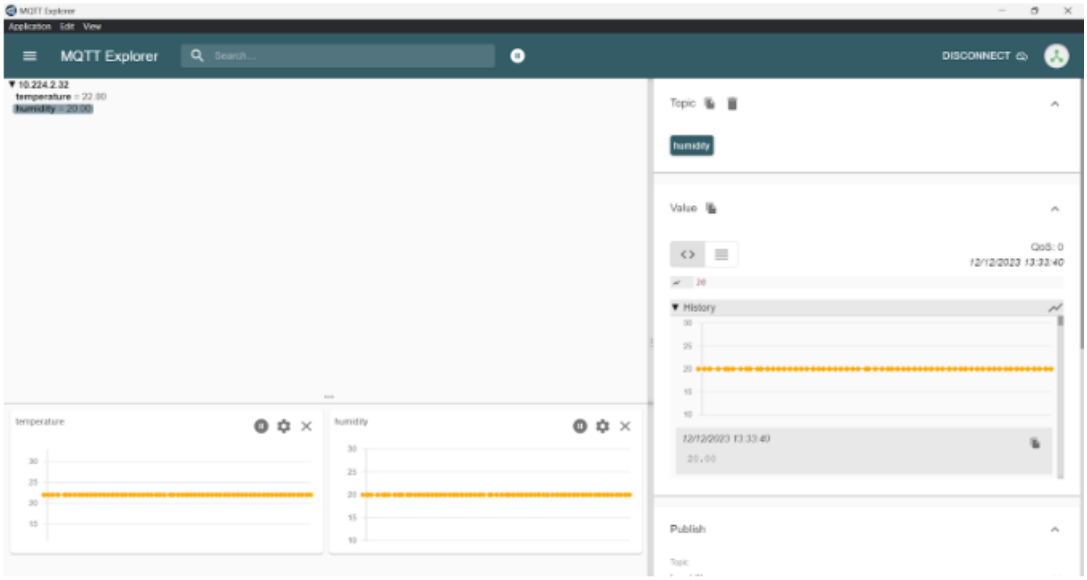
Figura 23 – Conexão do publicador com o protocolo MQTT



Fonte: Autor, 2024

A configuração do MQTT Explorer para a recepção de dados é realizada primariamente através da definição do IP do Broker. Este procedimento é essencial para estabelecer a conexão necessária para a transmissão de dados. Após a conclusão desta etapa, é realizada a verificação do recebimento dos dados enviados pelo microcontrolador ESP32 no MQTT Explorer. Esta verificação garante que a comunicação de dados foi estabelecida corretamente e que os dados estão sendo recebidos conforme o esperado. Portanto, a definição do IP do Broker e a subsequente confirmação do recebimento de dados são etapas críticas no processo de configuração do MQTT Explorer.

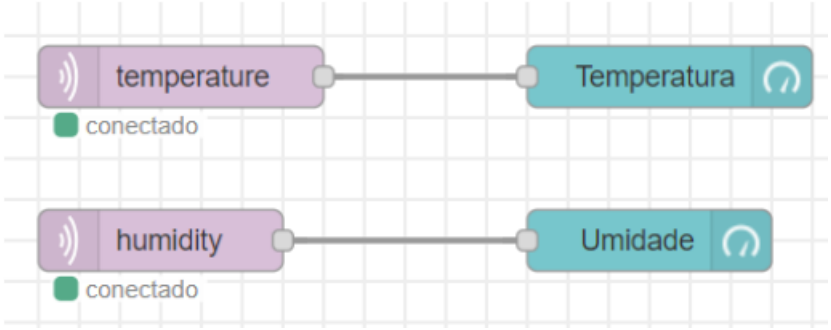
Figura 24 – Recebimento dos dados fornecidos pelo publicador



Fonte: Autor, 2024

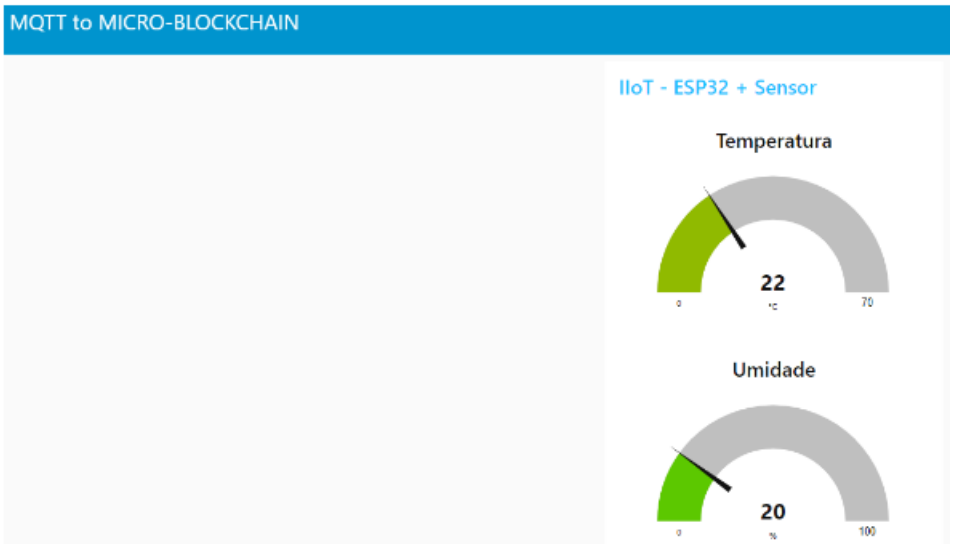
A configuração do MQTT por meio do Node-RED envolveu a construção de um painel de controle (dashboard) para exibir os dados de temperatura e umidade coletados em tempo-real.

Figura 25 – Widgets de recebimento e envio ao dashboard



Fonte: Autor, 2024

Figura 26 – Dashboard da leitura da temperatura e umidade em tempo-real



Fonte: Autor, 2024

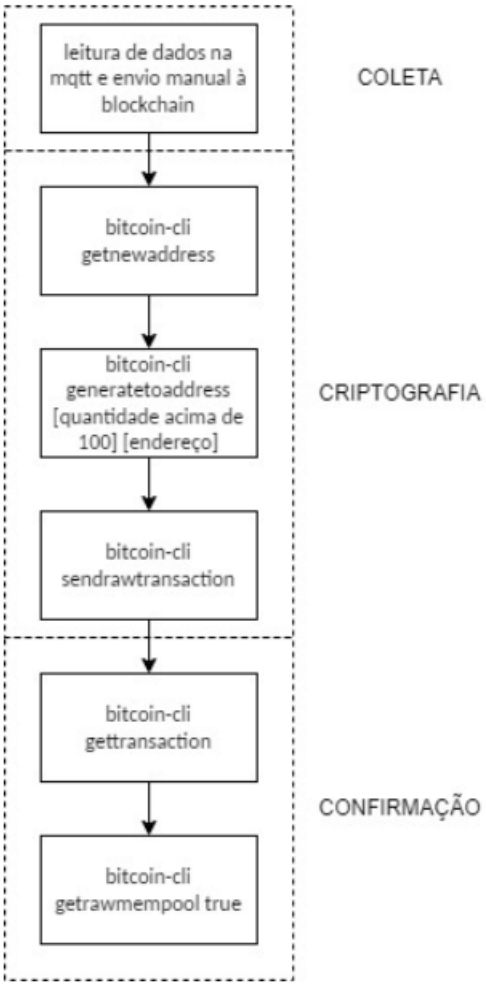
Esta integração de dados está alinhada com o conceito de computação em névoa (*Fog Computing*), no qual os dados são disponibilizados em uma rede local de sensores inteligentes. No contexto do presente trabalho, a rede de "sensores inteligentes" é constituída por microcontroladores ESP32 interoperáveis e interconectados, facilitando a troca de informações. Esta configuração permite a coleta, processamento e distribuição eficiente de dados, exemplificando a aplicação prática da computação em névoa na indústria de sensores inteligentes.

5.4 GERENCIAMENTO REMOTO - ACESSO RESTRITO

5.4.1 Operação na Micro-Blockchain Privada

A operação da micro-blockchain é conduzida por meio da manipulação dos códigos internos do servidor RPC bitcoin-cli. Após a coleta manual, leitura e inserção dos dados da rede local dos ESP32 no servidor bitcoin-cli, é executada uma sequência de comandos com o objetivo de obter a chave privada para a transação. É importante enfatizar que a chave privada na operação da micro-blockchain privada é o elemento que garante a integridade e confidencialidade dos dados. Para ter acesso ao servidor onde a micro-blockchain é executada, o usuário deve possuir a permissibilidade ao acesso, garantindo assim a segurança dos dados.

Figura 27 – Diagrama de Blocos para gerar a Chave Privada na Micro-Blockchain



Fonte: Autor, 2024

A primeira etapa executada consistiu na geração de um endereço virtual para o armazenamento dos dados. Este endereço é gerado antes da criação da chave privada. Para a criação desse endereço, é necessário executar o comando bitcoin-cli getnewaddress. Como resultado, é gerado um endereço Bitcoin, que pode variar de 26 a 35 caracteres, dependendo do tipo de endereço gerado. Este endereço representa o local virtual onde os dados serão armazenados. A geração deste endereço é um passo crucial para garantir a segurança e a integridade dos dados na micro-blockchain.

Figura 28 – Comando para gerar um novo endereço

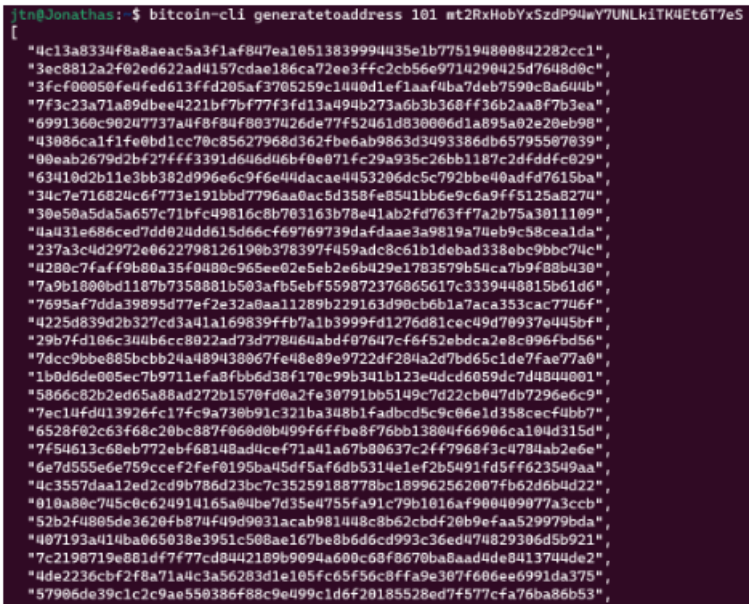
```
jtn@Jonathas:~$ bitcoin-cli getnewaddress
mt2RxHobYxSzdP94wY7UNLkiTK4Et6T7eS
```

Fonte: Autor, 2024

Após a geração do endereço “mt2RxHobYxSzdP94wY7UNLkiTK4Et6T7eS”, foi estabelecida uma quantidade específica de blocos para a distribuição da informação. No

ambiente do bitcoin-cli, para que haja uma quantidade válida de blocos, é necessário inserir no mínimo 100 blocos. O comando utilizado para inserir blocos é bitcoin-cli generatetoaddress (quantidade desejada) (endereço). No contexto do presente trabalho, o endereço utilizado para essa execução foi “mt2RxHobYxSzdP94wY7UNLkiTK4Et6T7eS”.

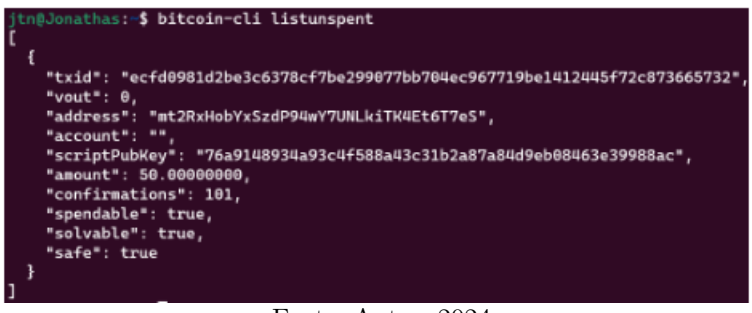
Figura 29 – Comando para gerar blocos disponíveis para o endereço criado



Fonte: Autor, 2024

A terceira etapa consiste em verificar, dentre os blocos informados, qual está disponível para realizar uma transação. Para essa verificação, é utilizado o comando bitcoin-cli listunspent. No contexto do presente trabalho, a txid e o endereço informado são utilizados para a geração da chave privada para essa transação. A chave privada não representa a transação em si, mas garante a possibilidade de sua realização. É importante ressaltar que, com a chave privada, a transação adquire a segurança inerente a uma blockchain.

Figura 30 – Comando para informar os blocos disponíveis não gastos



Fonte: Autor, 2024

A quarta etapa do processo consiste na geração da chave privada. Esta chave é gerada internamente no servidor local, que pode ser comparado a uma estação de trabalho autorizada em uma organização. Neste contexto, a micro-blockchain - uma blockchain com características específicas adaptadas às necessidades e produção do cliente - já atua como um sistema de segurança contra ataques cibernéticos. A segurança de uma blockchain em aplicações IIoT é um tema debatido por diversos autores como Sengupta, Ruj e Bit(39) (2020). No âmbito deste trabalho, a segurança no nível físico - que inclui o acesso ao hardware IIoT e ao sistema informático - é garantida pela limitação física até os terminais e componentes eletrônicos. A solução física proposta, considerando que se trata de um dispositivo não conectado à rede externa (internet pública), envolve a implementação de um agente de segurança que permita apenas a entrada autorizada de um grupo selecionado de pessoas para manipular a comunicação. No nível de redes (comunicação entre elementos), a blockchain é proposta como uma solução para combater ataques do tipo *Man-in-the-Middle* (MITM) e Ataque de Negação de Serviço (DoS). No modelo de rede proposto, o ataque *Man-in-the-Middle* seria uma opção, pois envolve dois ou mais dispositivos IIoT intercomunicáveis (dois ESP32 se comunicando). Neste cenário, um invasor consegue interceptar ou monitorar a comunicação entre dois dispositivos IoT e acessar seus dados privados. Já para o ataque de negação de serviço, os ESP32 seriam tratados como nós. Diferentemente do ataque DoS, no DDoS vários nós comprometidos atacam um alvo específico inundando mensagens ou solicitações de conexão para desacelerar ou até mesmo derrubar o recurso do servidor do sistema/rede.

Conforme observado por Sengupta, Ruj e Bit(39) (2020), a integração de tecnologias de blockchain em sistemas industriais de IoT provou ser bastante eficaz. Portanto, para a micro-blockchain proposta neste trabalho, pautada em resultados de segurança da comunicação de redes de sistemas IIoT tratados em outros trabalhos, o método para se obter a chave privada é utilizando o comando bitcoin-cli dumpprivkey, acrescentando o endereço do bloco da blockchain obtido na primeira etapa para gerar um endereço. A resposta deste comando é um código em formato WIF (*Wallet Import Format*) que auxiliará no acesso às transações seguras. Isso pode ser comparado a ter uma chave única de acesso a uma casa segura

Figura 31 – Comando para gerar a chave privada para outro endereço

Fonte: Autor, 2024

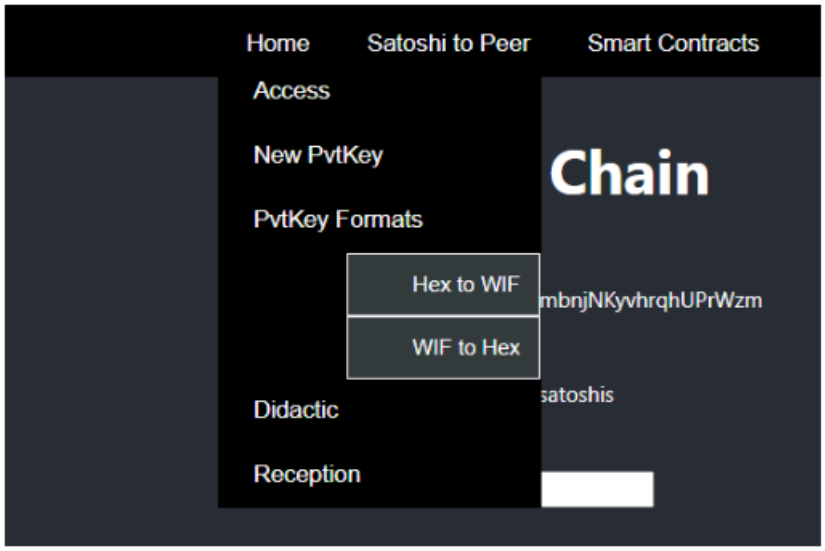
5.5 LEITURA SEGURA

5.5.1 Operação com Blockchain WEB3

A geração da chave privada resultou em uma garantia de transação segura, possibilitando a circulação da transação do dado “encapsulado” em uma blockchain. A referida chave foi gerada em uma micro-blockchain. No entanto, para a validação da chave e o teste de segurança, empregou-se uma blockchain disponível no modelo de testnet, que é uma blockchain de teste na rede. Este modelo de transação de blockchain pode ser acessado por meio de um recurso desenvolvido especificamente para a realização da transação blockchain. Quando se realiza esse tipo de operação em uma rede conectada, denomina-se “blockchain web3”, que se refere à terceira iteração da web, conhecida como Web3, construída sobre tecnologias descentralizadas como blockchain.

O procedimento inicial para a transação na rede testnet com a chave privada originada de uma micro-blockchain privada consistiu na conversão da chave do formato WIF para HEX. Essa transformação é imprescindível, visto que a blockchain na Web3 e a micro-blockchain wsl2 utilizam sintaxes distintas. A conversão de formatos é necessária para a interpretação adequada do valor da chave.

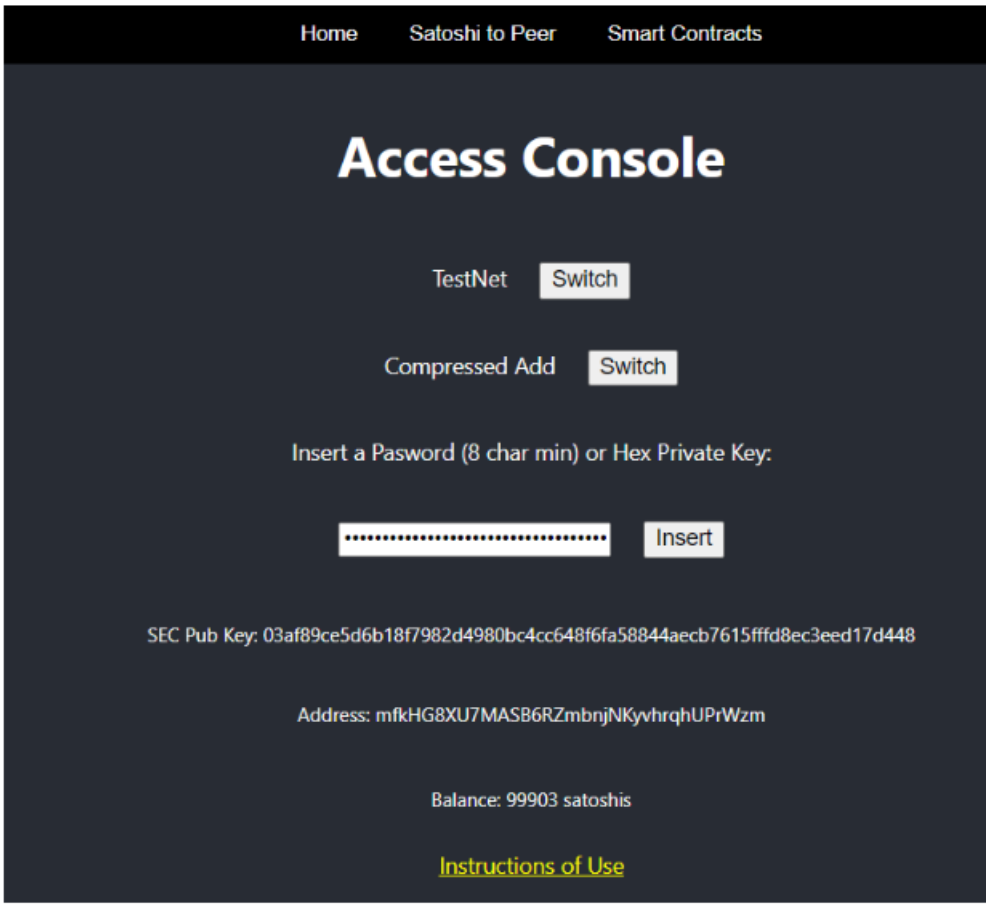
Figura 32 – Utilização da rede blockchain web3 para converter a chave em formato Hexadecimal



Fonte: Autor, 2024

O segundo procedimento realizado na Web3, após a obtenção da chave privada convertida para o formato hexadecimal, consistiu na geração da chave pública. Inicialmente, optou-se pela “testnet” como modelo de rede de transação, considerando que a testnet simula um ambiente industrial restrito, no qual apenas agentes devidamente autorizados teriam a capacidade de receber dados dessa transação. A chave privada foi inserida na caixa de texto designada para tal e, após a ação de pressionar o botão “Inserir”, obteve-se a chave pública correspondente à micro-blockchain e o endereço correspondente à micro-blockchain. Com a obtenção da chave pública, estabeleceu-se um sistema com um emissor e um receptor de informações. Com ambas as chaves, a transação do dado torna-se viável.

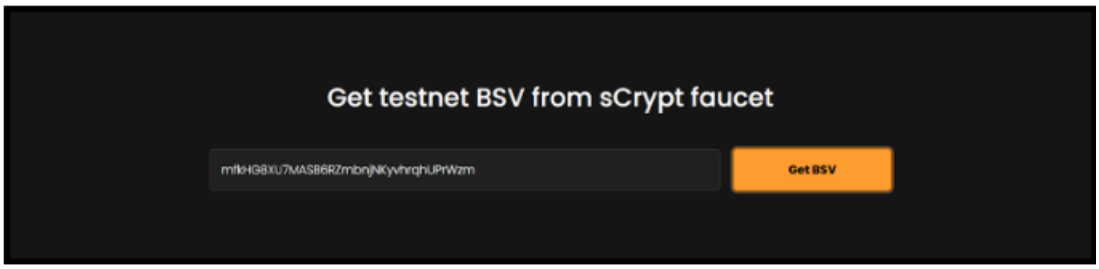
Figura 33 – Inserção da chave privada hex para obter a chave pública



Fonte: Autor, 2024

O terceiro procedimento no contexto da blockchain Web3 envolve a validação de faucets para a execução da transação. Faucets são bitcoins não utilizados para uma transação, cumprindo um dos critérios do modelo de micro-blockchain proposto nos materiais e métodos, que é o uso de UTXOs não gastos. A geração de faucets requer a inserção do endereço da blockchain após a obtenção da chave pública. Esses faucets podem ser adquiridos por meio de recursos específicos disponíveis na web.

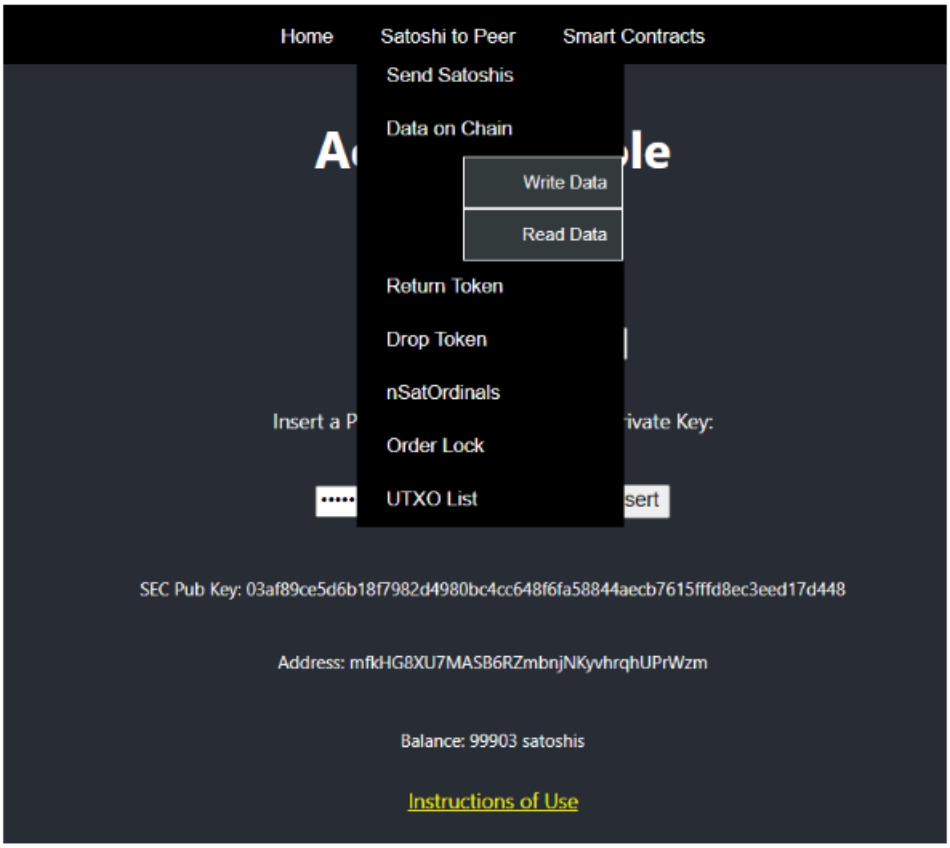
Figura 34 – Obtenção dos faucets



Fonte: Autor, 2024

Após a aquisição dos faucets (bitcoins destinados à transação na testnet), emprega-se a ferramenta “write data” da blockchain Web3 para inserir manualmente o valor fornecido pela MQTT referente à temperatura e umidade. Os valores de temperatura e umidade são inseridos isoladamente, um de cada vez. Após a inserção desses valores, aciona-se o botão “Write” para transmitir o dado, que já está seguro dentro da blockchain. Estes constituem os procedimentos para o servidor que transmite os dados dentro da blockchain Web3, utilizando a micro-blockchain para a geração da chave privada da transação.

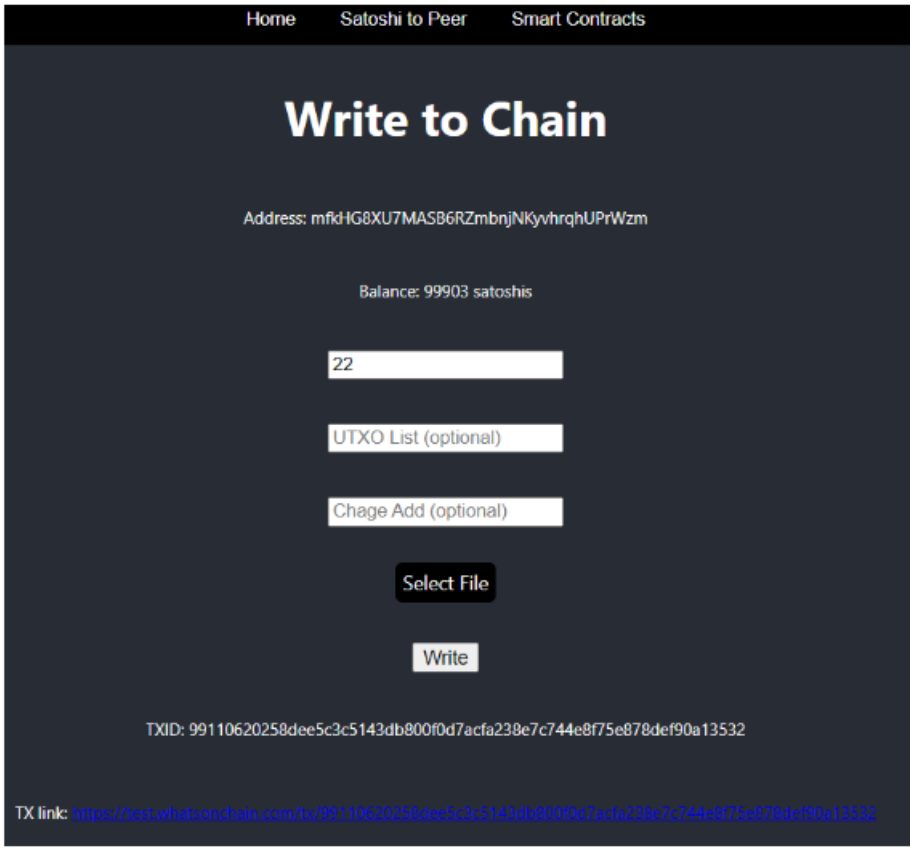
Figura 35 – Escrevendo os dados na blockchain web3



Fonte: Autor, 2024

A confirmação do envio dos dados é evidenciada pela geração de um Identificador de Transação (TXID), em formato hexadecimal, após a ação de pressionar o botão denominado “Escrever”. Esta confirmação é apresentada na parte inferior da página.

Figura 36 – Obtendo a TXID do dado enviado

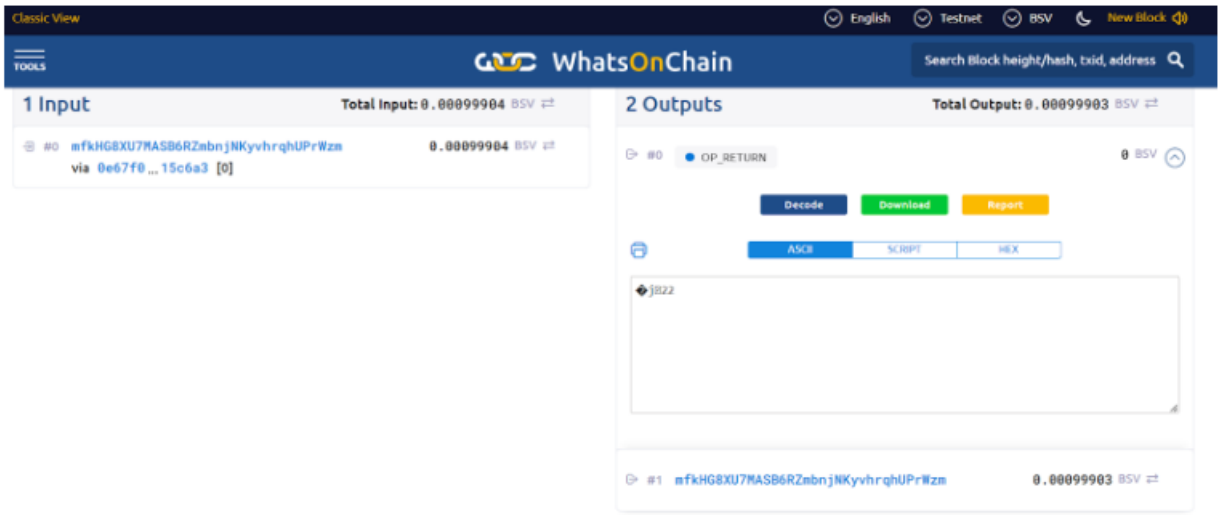


Fonte: Autor, 2024

A confirmação da integridade do envio de dados pode ser obtida por meio de verificadores de transação de dados de blockchain. No contexto deste trabalho, foi empregado o verificador “WhatsOnChain”, uma ferramenta disponível gratuitamente na rede de computadores. A verificação da transação de dados requer a inserção do endereço, tal como “mt2RxHobYxSzdP94wY7UNLkiTK4Et6T7eS”. Neste estudo, a confirmação serve para validar se o servidor de destino recebeu o dado de maneira segura.

Os aspectos descritos simulam um ambiente industrial fechado, no qual a conexão de rede é limitada e específica para a finalidade fabril. No entanto, ao expor o dado na web3, utiliza-se o conceito de testnet, que também segue a regra de uma rede interna de comunicação. O número mínimo de servidores utilizados compreende o servidor de envio e o servidor de recebimento.

Figura 37 – Validação do recebimento do dado transacionado na blockchain



Fonte: Autor, 2024

6 CONCLUSÃO

Este estudo apresentou um método inovador para a coleta de dados de dispositivos IIoT, utilizando uma micro-blockchain privada. Apesar da implementação manual de dados na rede blockchain web3 e na micro-blockchain, os resultados obtidos posicionam este trabalho no estado da arte em termos de funcionalidade, aplicabilidade na intercomunicação de dispositivos IIoT em rede e complexidade computacional.

Em um contexto de crescente demanda por dispositivos e redes seguras em ambientes fabris, devido à prevalência de ataques cibernéticos que visam reduzir ou impedir a operacionalidade de dispositivos, mecanismos e máquinas nas fábricas, a relevância deste estudo é evidente. A abordagem proposta neste trabalho é particularmente útil quando se considera que os sistemas de ciberataque estão cada vez mais utilizando inteligência artificial para quebrar as seguranças mais tradicionais.

No entanto, este estudo não está isento de limitações. A principal delas é a implementação manual de dados na rede blockchain web3 e na micro-blockchain. Pesquisas futuras poderiam explorar formas de automatizar esse processo para aumentar a eficiência e a escalabilidade do sistema.

Com base nos resultados obtidos, foram propostas duas diretrizes principais para trabalhos futuros. A primeira é a comunicação física cabeada entre os elementos da camada de aquisição de dados e dispositivos de campo, a fim de limitar o acesso à rede de alimentação de tensão e prevenir a alteração da exatidão da leitura por manipulação física do elemento. A segunda diretriz é que o protocolo MQTT se baseie em um ambiente web3, restringindo a troca de informação ao acesso de chaves privada e pública.

Em conclusão, o desenvolvimento de um servidor que gera a chave privada por meio da micro-blockchain e recebe os valores coletados pelos sensores via ambiente web3, cria um ambiente seguro que respeita os princípios da segurança da informação em um ambiente corporativo. Este trabalho representa um passo significativo para a integração segura de dispositivos IIoT em ambientes fabris, contribuindo para a literatura existente e abrindo novas possibilidades para pesquisas futuras.

7 TRABALHOS FUTUROS

Este estudo abre várias possibilidades para pesquisas futuras. Uma delas é a exploração de formas de automatizar a implementação de dados na rede blockchain web3 e na micro-blockchain. Isso poderia aumentar a eficiência e a escalabilidade do sistema, tornando-o mais adequado para aplicações industriais em larga escala.

Outra direção promissora para pesquisas futuras é a investigação de métodos avançados de limitação de acesso para melhorar a segurança dos dados. Isso poderia incluir o desenvolvimento de protocolos de autenticação mais robustos ou a implementação de medidas de segurança física para proteger os dispositivos de campo.

Além disso, seria interessante explorar a integração de outras tecnologias emergentes com a micro-blockchain privada. Por exemplo, a aplicação de técnicas de aprendizado de máquina poderia permitir a detecção precoce de anomalias ou ataques cibernéticos, melhorando ainda mais a segurança e a confiabilidade do sistema.

Por fim, pesquisas futuras poderiam se concentrar na avaliação da eficácia da solução proposta em diferentes cenários industriais. Isso poderia envolver a realização de estudos de caso em várias indústrias ou a simulação de diferentes tipos de ataques cibernéticos para avaliar a robustez do sistema.

Estas são apenas algumas das muitas direções possíveis para pesquisas futuras neste campo. À medida que a tecnologia avança, sem dúvida surgirão novas oportunidades para melhorar a segurança e a eficiência dos sistemas IIoT.

Referências[1]

1 GIMENEZ-AGUILAR, M. et al. Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, Elsevier, v. 124, p. 91–118, 2021. Citado na página 18.

2 LI, D. et al. A blockchain-based authentication and security mechanism for iot. In: IEEE. *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. [S.l.], 2018. p. 1–6. Citado na página 18.

3 ZHANG, C.; WU, C.; WANG, X. Overview of blockchain consensus mechanism. In: *Proceedings of the 2020 2nd International Conference on Big Data Engineering*. [S.l.: s.n.], 2020. p. 7–12. Citado na página 23.

4 ANTONIADIS, I.; KONTSAS, S.; SPINTHIROPOULOS, K. Blockchain applications in marketing. *The Proceedings of 7th ICCMI*, p. 124–134, 2019. Citado na página 23.

5 CHANG, S. E.; CHEN, Y. Blockchain in health care innovation: literature review and case study from a business ecosystem perspective. *Journal of medical Internet research*, JMIR Publications Toronto, Canada, v. 22, n. 8, p. e19480, 2020. Citado na página 23.

6 LU, Y.; XU, L. D. Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 2, p. 2103–2115, 2018. Citado na página 24.

7 DHIRANI, L. L.; ARMSTRONG, E.; NEWE, T. Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, MDPI, v. 21, n. 11, p. 3901, 2021. Citado na página 25.

8 CHEN, X.; NGUYEN, K.; SEKIYA, H. An experimental study on performance of private blockchain in iot applications. *Peer-to-peer networking and applications*, Springer, v. 14, p. 3075–3091, 2021. Citado na página 26.

9 BAIG, M. J. A. et al. Design and implementation of an open-source iot and blockchain-based peer-to-peer energy trading platform using esp32-s2, node-red and, mqtt protocol. *Energy reports*, Elsevier, v. 7, p. 5733–5746, 2021. Citado na página 28.

10 ANAGNOSTAKIS, A. G. et al. Iot micro-blockchain fundamentals. *Sensors*, MDPI, v. 21, n. 8, p. 2784, 2021. Citado 2 vezes nas páginas 29 e 64.

11 TONG, W. et al. A hierarchical sharding protocol for multi-domain iot blockchains. In: IEEE. *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. [S.l.], 2019. p. 1–6. Citado na página 30.

12 LAURENCE, T. *Blockchain for dummies*. [S.l.]: John Wiley & Sons, 2023. Citado na página 32.

13 GUPTA, S.; SADOGHI, M. Blockchain transaction processing. *arXiv preprint arXiv:2107.11592*, 2021. Citado na página 33.

[1] De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

14 HILLMANN, P. et al. Selective deletion in a blockchain. In: IEEE. *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. [S.l.], 2020. p. 1249–1256. Citado na página 34.

15 READ, C. L. The genesis block. In: *The Bitcoin Dilemma: Weighing the Economic and Environmental Costs and Benefits*. [S.l.]: Springer, 2022. p. 29–36. Citado na página 34.

16 ABED, S. et al. An analysis and evaluation of lightweight hash functions for blockchain-based iot devices. *Cluster computing*, Springer, v. 24, p. 3065–3084, 2021. Citado na página 35.

17 GEEKSFORGEEKS. *Blockchain Hash Function*. 2023. Acessado em: 30 nov. 2023. Disponível em: ⟨https://www.geeksforgeeks.org/blockchain-hash-function/⟩. Citado na página 35.

18 MURRAY, M. Tutorial: A descriptive introduction to the blockchain. *Communications of the Association for Information Systems*, v. 45, n. 1, p. 25, 2019. Citado na página 36.

19 MOHAN, A. P.; GLADSTON, A. et al. Merkle tree and blockchain-based cloud data auditing. *International Journal of Cloud Applications and Computing (IJCAC)*, IGI Global, v. 10, n. 3, p. 54–66, 2020. Citado na página 37.

20 NAKAMOTO, S. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, v. 9, p. 15, 2008. Citado 2 vezes nas páginas 38 e 46.

21 BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, v. 3, n. 37, p. 2–1, 2014. Citado 2 vezes nas páginas 38 e 39.

22 HAMDI, A.; FOURATI, L.; AYED, S. Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: tools, analysis and countermeasures. *International Journal of Information Security*, Springer, p. 1–45, 2023. Citado na página 39.

23 BODKHE, U. et al. Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, IEEE, v. 8, p. 79764–79800, 2020. Citado na página 40.

24 LACITY, M. C.; LUPIEN, S. C. *Blockchain Fundamentals for Web 3.0:-*. [S.l.]: University of Arkansas Press, 2022. Citado 2 vezes nas páginas 40 e 41.

25 PAUL, P. et al. Blockchain technology and its types—a short review. *International Journal of Applied Science and Engineering (IJASE)*, v. 9, n. 2, p. 189–200, 2021. Citado 2 vezes nas páginas 42 e 43.

26 GUPTA, S.; SADOGHI, M. Blockchain transaction processing. *arXiv preprint arXiv:2107.11592*, 2021. Citado 2 vezes nas páginas 43 e 44.

27 LAMOUNIER, L. Blockchain hibrida: O melhor de dois mundos. *101 Blockchains*, 2020. Disponível em: ⟨https://101blockchains.com/pt/blockchain-hibrida-explicado/⟩. Citado na página 44.

28 MOURA, L. M. F. d.; BRAUNER, D. F.; JANISSEK-MUNIZ, R. Blockchain e a perspectiva tecnológica para a administração pública: uma revisão sistemática. *Revista de Administração Contemporânea*, SciELO Brasil, v. 24, p. 259–274, 2020. Citado na página 45.

29 ZHANG, C.; WU, C.; WANG, X. Overview of blockchain consensus mechanism. In: *Proceedings of the 2020 2nd International Conference on Big Data Engineering*. [S.l.: s.n.], 2020. p. 7–12. Citado 2 vezes nas páginas 45 e 46.

30 KING, S.; NADAL, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, v. 19, n. 1, 2012. Citado na página 46.

31 LASHKARI, B.; MUSILEK, P. A comprehensive review of blockchain consensus mechanisms. *IEEE access*, IEEE, v. 9, p. 43620–43652, 2021. Citado na página 47.

32 LARIMER, D. Delegated proof-of-stake (dpos). *Bitshare whitepaper*, v. 81, p. 85, 2014. Citado 2 vezes nas páginas 47 e 51.

33 CASTRO, M.; LISKOV, B. et al. Practical byzantine fault tolerance. In: *OsDI*. [S.l.: s.n.], 1999. v. 99, n. 1999, p. 173–186. Citado 2 vezes nas páginas 47 e 60.

34 ALLADI, T. et al. Blockchain applications for industry 4.0 and industrial iot: A review. *Ieee Access*, IEEE, v. 7, p. 176935–176951, 2019. Citado na página 60.

35 YANG, X. et al. Cryptanalysis and improvement of a blockchain-based certificateless signature for iiot devices. *IEEE Transactions on Industrial Informatics*, IEEE, 2023. Citado na página 60.

36 LENG, J. et al. Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. *Machines*, MDPI, v. 10, n. 10, p. 858, 2022. Citado na página 60.

37 LU, Y.; XU, L. D. Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 2, p. 2103–2115, 2018. Citado na página 64.

38 PAN, J. et al. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 3, p. 4719–4732, 2018. Citado na página 67.

39 SENGUPTA, J.; RUJ, S.; BIT, S. D. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of network and computer applications*, Elsevier, v. 149, p. 102481, 2020. Citado na página 94.

Anexo A – Códigos aplicados à IDE Arduino

Listing A.1 – Código do MQTT Broker

```
#include <WiFi.h>
#include "sMQTTBroker.h"

sMQTTBroker broker;

IPAddress local_IP(10, 224, 2, 32); //Definindo o IP de acordo com a rede
IPAddress gateway(10, 224, 2, 63);
IPAddress subnet(255, 255, 0, 0);

void setup()
{
    Serial.begin(115200);

    if (!WiFi.config(local_IP, gateway, subnet)) {
        Serial.println("STA Failed to configure");
    }

    const char* ssid = "VISITANTE_CETELI";
    const char* password = "";

    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
        delay(1000);
    }
    Serial.println("Connection established!");
    Serial.print("IP address:\t");
    Serial.println(WiFi.localIP());

    const unsigned short mqttPort = 1883;
    broker.init(mqttPort);
    // all done
}

void loop()
{
```

```
    broker.update();
}
```

Listing A.2 – Código do MQTT Publisher

```
#include <WiFi.h>
#include <PubSubClient.h>
#include <DHT.h>

#define DHTPIN 4      // Pino digital que est  conectado ao DHT11
#define DHTTYPE DHT11    // DHT 11

DHT dht(DHTPIN, DHTTYPE);

const char* ssid = "VISITANTE_CETELI";
const char* password = "";
const char* mqtt_server = "10.224.2.32";

WiFiClient espClient;
PubSubClient client(espClient);
unsigned long lastMsg = 0;
#define MSG_BUFFER_SIZE (50)
char msg[MSG_BUFFER_SIZE];
int value = 0;

void setup_wifi() {
  delay(10);
  Serial.println();
  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.mode(WIFI_STA);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  randomSeed(micros());
  Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address: ");
```

```
  Serial.println(WiFi.localIP());
}

void callback(char* topic, byte* payload, unsigned int length) {
  Serial.print("Message arrived [");
  Serial.print(topic);
  Serial.print("] ");
  for (int i = 0; i < length; i++) {
    Serial.print((char)payload[i]);
  }
  Serial.println();
}

void reconnect() {
  while (!client.connected()) {
    Serial.print("Attempting MQTT connection...");
    String clientId = "ESP32Client";
    clientId += String(random(0xffff), HEX);
    if (client.connect(clientId.c_str())) {
      Serial.println("connected");
    } else {
      Serial.print("failed, rc=");
      Serial.print(client.state());
      Serial.println(" try again in 5 seconds");
      delay(5000);
    }
  }
}

void setup() {
  Serial.begin(115200);
  setup_wifi();
  client.setServer(mqtt_server, 1883);
  client.setCallback(callback);
  dht.begin();
}

void loop() {
  if (!client.connected()) {
```

```
    reconnect();
  }
  client.loop();
  unsigned long now = millis();
  if (now - lastMsg > 2000) {
    lastMsg = now;
    float h = dht.readHumidity();
    float t = dht.readTemperature();
    if (isnan(h) || isnan(t)) {
      Serial.println("Failed to read from DHT sensor!");
      return;
    }
    char temp[8];
    dtostrf(t, 6, 2, temp);
    client.publish("temperature", temp);
    char hum[8];
    dtostrf(h, 6, 2, hum);
    client.publish("humidity", hum);
  }
}
```