UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)

UNIDADE ACADÊMICA DE GRADUAÇÃO

CURSO DE ENGENHARIA DA COMPUTAÇÃO

GUILHERME ZANINI DA SILVA

AUMENTO DA SEGURANÇA EM REDES IOT UTILIZANDO A BLOCKCHAIN E O PROTOCOLO LORAWAN:

Estudo de Caso com a Rede Helium

São Leopoldo

2024

GUILHERME ZANINI DA SILVA

AUMENTO DA SEGURANÇA EM REDES IOT UTILIZANDO A BLOCKCHAIN E O PROTOCOLO LORAWAN:

Estudo de Caso com a Rede Helium

Trabalho de Conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Engenharia da Computação, pelo curso de Engenharia da Computação da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof.ª Me. Janaina Conceição Sutil Lemos

São Leopoldo

2024

AGRADECIMENTOS

Agradeço aos meus pais e a toda minha família pelo suporte incondicional e apoio ao longo dessa caminhada. Sou grato aos amigos, pela parceria e pelos aprendizados compartilhados durante os desafios enfrentados na graduação. Agradeço também a todos os professores desta universidade, pelos ensinamentos e pela dedicação em transmitir seu conhecimento. Em especial, agradeço à professora Me. Janaina Conceição Sutil Lemos, cuja orientação foi fundamental para o desenvolvimento deste trabalho.

RESUMO

O avanço da Internet das Coisas (IoT) tem impulsionado o uso de dispositivos conectados em diversos setores, incluindo ambientes sensíveis como infraestrutura crítica e aplicações militares. Contudo, a segurança dos dados transmitidos por esses dispositivos continua sendo um dos maiores desafios enfrentados, devido à vulnerabilidade das redes IoT a ataques cibernéticos e a capacidade limitada de muitos dispositivos para implementar medidas de segurança robustas. Neste contexto, este trabalho investiga como a combinação do protocolo LoRaWAN, com suas características de baixo consumo de energia e longo alcance, e a tecnologia *Blockchain*, especificamente a *Blockchain* Helium, pode ser utilizada para aumentar a segurança em redes IoT. A proposta inclui o desenvolvimento de uma aplicação prática para testar a rede, avaliando a eficiência da arquitetura em termos de autenticação descentralizada e integridade dos dados. A revisão de literatura aborda os principais desafios de segurança em IoT, as características do protocolo LoRaWAN, e os benefícios da integração de *Blockchain*, que oferece autenticação sem a necessidade de autoridades centrais, imutabilidade dos dados e resistência a ataques. Além disso, discute-se o impacto da escalabilidade e do desempenho das soluções propostas em ambientes críticos. O estudo conclui que a implementação conjunta de LoRaWAN e *Blockchain* Helium pode proporcionar uma arquitetura de rede IoT mais segura e eficiente, especialmente em cenários onde a proteção dos dados é crucial.

Palavras-chave: Internet das Coisas (IoT); *Blockchain*; LoRaWAN; Helium *Blockchain*; Autenticação Descentralizada; Proteção de Dados; Segurança de Redes.

ABSTRACT

The rapid growth of the Internet of Things (IoT) has expanded the use of connected devices across various sectors, including sensitive environments such as critical infrastructure and military applications. However, the security of data transmitted by IoT devices remains a significant challenge due to the vulnerability of IoT networks to cyberattacks and the limited capacity of many devices to implement robust security measures. This work explores how the combination of the LoRaWAN protocol, known for its low energy consumption and long-range communication capabilities, with Blockchain technology, specifically the Helium Blockchain, can be used to enhance the security of IoT networks. The proposed solution involves the development of a practical application to test the network, evaluating the efficiency of the architecture in terms of decentralized authentication and data integrity. The literature review addresses key IoT security challenges, the characteristics of the LoRaWAN protocol, and the benefits of integrating Blockchain, which offers authentication without the need for central authorities, data immutability, and resistance to attacks. Additionally, the scalability and performance of the proposed solution in critical environments are discussed. The study concludes that the joint implementation of LoRaWAN and Helium Blockchain can provide a more secure and efficient IoT network architecture, especially in scenarios where data protection is crucial.

Keywords: *Internet of Things (IoT); Blockchain; LoRaWAN; Helium Blockchain; Decentralized Authentication; Data Protection; Network Security.*

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

6LoWPAN	*IPv6 over Low-Power Wireless Personal Area Networks* (IPv6 sobre Redes de Área Pessoal Sem Fio de Baixa Potência)
AppSKey	*Application Session Key* (Chave de Sessão de Aplicação)
BLE	*Bluetooth Low Energy* (*Bluetooth* de Baixa Energia)
DDoS	*Distributed Denial of Service* (Negação de Serviço Distribuída)
HNT	*Helium Network Token*, criptomoeda usada na Rede Helium.
ICT	*Information and Communication Technology* (Tecnologia da Informação e Comunicação)
IoT	*Internet of Things* (Internet das Coisas)
IPv6	*Internet Protocol version 6* (Protocolo de Internet versão 6)
LGPD	Lei Geral de Proteção de Dados Pessoais
LoRaWAN	*Long Range Wide Area Network* (Rede de Longo Alcance de Área Ampla)
LTE	*Long-Term Evolution* (Evolução de Longo Prazo)
LTE-M	*Long-Term Evolution for Machines* (Evolução de Longo Prazo para Máquinas)
M2C	*Machine to Cloud* (Máquina para Nuvem)
M2M	*Machine to Machine* (Máquina para Máquina)
M2P	*Machine to Person* (Máquina para Pessoa)
MitM	*Man-in-the-Middle* (Ataque de Interceptação de Dados)
NB-IoT	*Narrowband Internet of Things* (Internet das Coisas de Banda Estreita)
NwkSKey	*Network Session Key* (Chave de Sessão de Rede)
PoA	*Proof of Authority* (Prova de Autoridade)
PoC	*Proof of Coverage* (Prova de Cobertura)

PoS	*Proof of Stake* (Prova de Participação)
PoW	*Proof of Work* (Prova de Trabalho)
RFID	*Radio Frequency Identification* (Identificação por Radiofrequência)
RSSF	Redes de Sensores Sem Fio
SRAM	*Static Random-Access Memory* (Memória de Acesso Aleatório Estática)
SPI	*Serial Peripheral Interface* (Interface Periférica Serial), protocolo de comunicação.
TCC1	Trabalho de Conclusão de Curso 1
TCC2	Trabalho de Conclusão de Curso 2
WSN	*Wireless Sensor Networks* (Redes de Sensores Sem Fio)

SUMÁRIO

1 INTRODUÇÃO

A Internet das Coisas (IoT) tem transformado a forma como os dispositivos interagem, promovendo conectividade em uma ampla variedade de ambientes, desde residências até setores industriais e infraestrutura urbana. No entanto, o crescimento exponencial do número de dispositivos conectados traz desafios significativos, especialmente no que diz respeito à segurança, privacidade e integridade dos dados transmitidos (REYNEKE; MULLINS; REITH, 2023). Nesse contexto, a tecnologia *blockchain* surge como uma solução promissora, oferecendo uma estrutura de registro distribuído e imutável que garante a autenticidade e transparência das transações, sem a necessidade de intermediários (SANTOS; SOUSA, 2024).

A Rede Helium destaca-se por integrar IoT e *blockchain* de maneira inovadora, utilizando o protocolo LoRaWAN para conectar dispositivos de baixa potência a longas distâncias, com um modelo descentralizado que incentiva a expansão da rede por meio do protocolo de consenso *Proof-of-Coverage* (PoC). Esse modelo permite que *hotspots* validem a cobertura e conectividade de rede, sendo recompensados com *tokens* HNT, a moeda nativa da Helium *Network* (DZHUNEV, 2022). Essa combinação de *blockchain* e IoT oferece não apenas uma infraestrutura eficiente e econômica, mas também uma camada adicional de segurança e integridade dos dados (REYNEKE; MULLINS; REITH, 2023).

Este trabalho examina o potencial da Rede Helium e sua aplicação em ambientes de IoT, com ênfase nas questões de segurança e nos mecanismos de defesa implementados para proteger a integridade dos dados. Além disso, serão discutidos os desafios regulatórios e as preocupações com a privacidade dos dados em redes distribuídas e descentralizadas. A pesquisa visa oferecer uma análise aprofundada da viabilidade e das limitações dessa tecnologia no cenário atual, com foco na proteção de dados e na eficiência em ambientes de IoT.

1.1 TEMA

O tema deste trabalho é a segurança de redes IoT utilizando *Blockchain* e LoRaWAN. Especificamente, busca-se explorar como a *Blockchain* Helium pode ser integrada ao protocolo LoRaWAN para proporcionar uma rede IoT mais segura e descentralizada, adequada para ambientes sensíveis e críticos.

1.2 DELIMITAÇÃO DO TEMA

Este estudo está delimitado à análise da segurança em redes IoT utilizando a integração do protocolo LoRaWAN com a *Blockchain* Helium. O foco será o desenvolvimento de uma aplicação simples para testar essa arquitetura, sem a pretensão de realizar um levantamento detalhado sobre a eficácia em grandes redes ou um estudo de caso complexo.

1.3 PROBLEMA

Investigar de que forma a integração da *Blockchain* Helium com o protocolo LoRaWAN pode aumentar a segurança de redes IoT, garantindo a autenticidade, integridade dos dados e resistência a ataques cibernéticos.

1.4 OBJETIVOS

1.4.1 OBJETIVO GERAL

O objetivo geral deste trabalho é avaliar como a *Blockchain* Helium, integrada ao protocolo LoRaWAN, pode aumentar a segurança de redes IoT em ambientes sensíveis, garantindo autenticação descentralizada, integridade dos dados e proteção contra ataques cibernéticos.

1.4.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são divididos em quatro itens:

1) Analisar os desafios de segurança em redes IoT e as principais vulnerabilidades.

2) Explorar as vantagens do protocolo LoRaWAN para IoT, com foco em seu uso em cenários de longo alcance e baixo consumo de energia.

3) Investigar o uso da *Blockchain* Helium para autenticação descentralizada e verificação de integridade dos dados em redes IoT.

4) Desenvolver uma aplicação prática para testar a integração entre *Blockchain* Helium e LoRaWAN em redes IoT.

1.5 JUSTIFICATIVA

A segurança em redes IoT é uma preocupação crescente, especialmente em ambientes sensíveis, como infraestrutura crítica, onde dispositivos conectados pos-

suem recursos limitados para implementar medidas robustas de proteção, tornando-os vulneráveis a ataques cibernéticos (RAMMOUZ et al., 2023). O uso de *blockchain*, particularmente a Helium, oferece uma solução inovadora ao proporcionar autenticação descentralizada e verificação de dados imutáveis, aumentando a resiliência das redes IoT. Além disso, o protocolo LoRaWAN tem demonstrado eficiência ao conectar dispositivos IoT em áreas amplas, embora ainda careça de integrações mais sólidas com soluções de segurança descentralizadas (PANARELLO et al., 2018). Assim, este trabalho justifica-se pela necessidade de uma arquitetura segura e escalável para redes IoT, integrando *Blockchain* e LoRaWAN para resolver desafios de segurança em ambientes críticos.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo abrange uma revisão dos principais conceitos que são indispensáveis para o estudo do tema em questão. Por meio dessa revisão, busca-se proporcionar uma compreensão sólida do contexto e embasamento que fundamentam a integração entre *Blockchain* Helium e o protocolo LoRaWAN (*Long Range Wide Area Network*) no aumento da segurança de redes IoT.

2.1 INTERNET DAS COISAS (IOT)

A Internet das Coisas (IoT) refere-se à interconexão de dispositivos inteligentes, também chamados de “coisas”, que são capazes de coletar dados e tomar decisões inteligentes de forma autônoma. Esses dispositivos conectados geram grandes quantidades de dados que são utilizados para diversas aplicações práticas e beneficiam tanto a academia quanto a indústria. O crescimento exponencial da IoT tem possibilitado o desenvolvimento de novos métodos de negócios e expandido significativamente o mercado de Tecnologia da Informação e Comunicação (ICT) (PANARELLO et al., 2018).

A IoT surge da evolução de tecnologias como sistemas embarcados, microeletrônica, comunicação e sensoriamento, e tem gerado um impacto considerável na sociedade, com aplicações em áreas como cidades inteligentes, saúde e automação de ambientes (SPADINGER, 2024). Com isso, a IoT também trouxe desafios significativos, especialmente no que tange à segurança, privacidade e interoperabilidade entre os dispositivos conectados (PANARELLO et al., 2018).

De forma geral, a IoT está se tornando uma parte integrante do cenário tecnológico global, oferecendo uma ampla gama de oportunidades em diversos setores, desde a automação industrial até o consumo doméstico.

2.1.1 DEFINIÇÃO E EVOLUÇÃO DA IOT

A Internet das Coisas foi originalmente definida por Kevin Ashton em 1999, enquanto trabalhava em um projeto relacionado ao uso da tecnologia RFID (*Radio Frequency Identification*). Desde então, o conceito evoluiu e passou a abarcar diversas outras tecnologias, como sensores, atuadores e redes sem fio, possibilitando a interconexão de objetos físicos com capacidade de comunicação e processamento (PANARELLO et al., 2018).

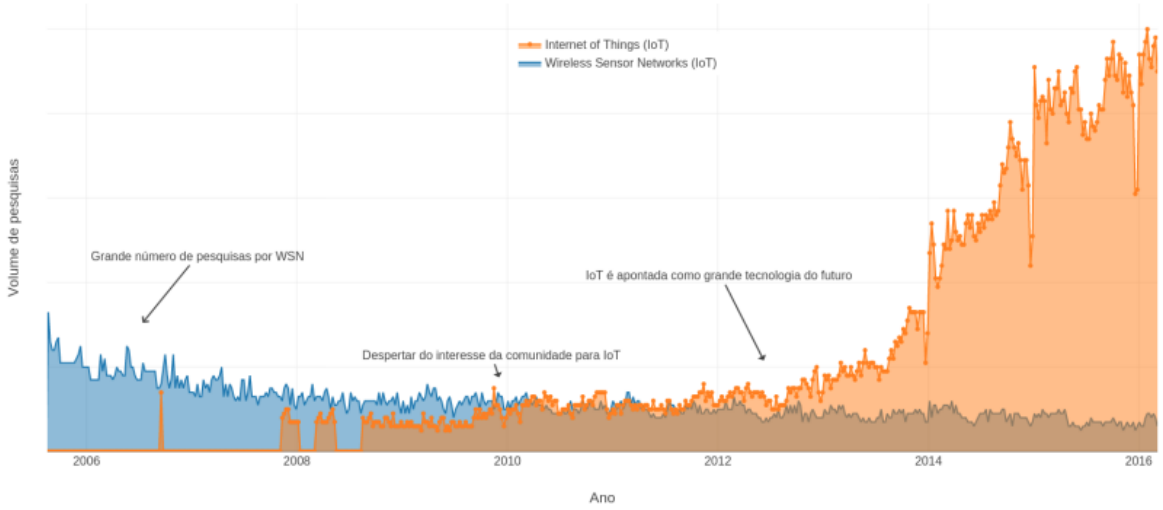

Figura 1 – Volume de pesquisas no Google sobre *Wireless Sensor Networks* e *Internet of Things*.

(SANTOS et al., 2024)

A IoT começou a ganhar popularidade entre 2008 e 2010 como demostrado no gráfico da Figura 1, impulsionada pelo amadurecimento das Redes de Sensores Sem Fio (RSSF) e pelo aumento das expectativas sobre suas aplicações em larga escala. Durante esse período, as pesquisas acadêmicas e industriais relacionadas à IoT começaram a crescer de forma significativa, especialmente após a introdução de novas plataformas e dispositivos voltados para aplicações específicas, como monitoramento ambiental e automação residencial (SANTOS et al., 2024).

Em termos de infraestrutura tecnológica, a IoT depende de avanços em várias frentes, como a redução dos custos de *hardware* e o desenvolvimento de protocolos de comunicação adequados. Nos últimos anos, dispositivos como o Raspberry Pi e o Arduino se tornaram ferramentas fundamentais para a prototipagem e implementação de soluções IoT de baixo custo, facilitando a sua adoção em diversos setores.

Além disso, a padronização das tecnologias subjacentes à IoT tem sido um fator crucial para o seu sucesso. Tecnologias como IPv6, 6LoWPAN, LoRaWAN e outras têm sido utilizadas para resolver os desafios de conectividade e escalabilidade, permitindo que a IoT se expanda e conecte bilhões de dispositivos globalmente (SANTOS et al., 2024). Com isso, a expectativa é que a IoT continue a crescer nos próximos anos, impactando setores como saúde, transporte e agricultura, e criando novas oportunidades para inovação tecnológica (SPADINGER, 2024).

2.1.2 ARQUITETURA DE REDES IOT

A arquitetura da Internet das Coisas (IoT) é composta por 3 camadas que interconectam dispositivos físicos com a rede e seus serviços.

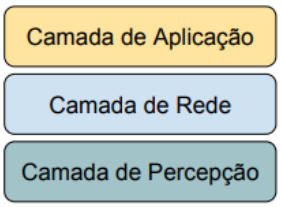

Figura 2 – Arquitetura para IoT.

- **Camada de aplicação:** Onde os dados são processados e transformados em serviços para os usuários.
- **Camada de rede:** Realiza a comunicação entre os dispositivos e a internet;
- **Camada de percepção:** Responsável pelos sensores e atuadores que capturam e transmitem dados do ambiente;

A organização em camadas permite o gerenciamento eficiente da complexidade das redes IoT, garantindo a interoperabilidade entre dispositivos heterogêneos.

A arquitetura de uma rede IoT pode ser composta por sensores, atuadores, *gateways* e servidores na nuvem, cada um desempenhando um papel específico na coleta, transmissão e processamento dos dados (SANTOS et al., 2024).

Na maioria das arquiteturas IoT, os dispositivos conectados (objetos inteligentes) utilizam redes de sensores sem fio (*Wireless Sensor Networks* - WSN) para comunicar dados coletados de ambientes físicos para *gateways*. Os *gateways*, por sua vez, agregam essas informações e as encaminham para servidores em nuvem, onde podem ser armazenadas, processadas e analisadas (REYNEKE; MULLINS; REITH, 2023).

A arquitetura de redes IoT também enfrenta desafios de interoperabilidade, uma vez que diferentes dispositivos e protocolos precisam trabalhar juntos de maneira eficiente e segura. A integração de diferentes padrões e tecnologias continua sendo um campo de pesquisa ativo, com a busca por soluções que facilitem a comunicação fluida entre dispositivos heterogêneos (PANARELLO et al., 2018).

2.1.3 COMUNICAÇÃO EM REDES IOT

A comunicação entre dispositivos IoT é suportada por várias tecnologias, como o M2M (*Machine to Machine*), que permite a comunicação direta entre dispositivos

sem a intervenção humana (SPADINGER, 2024). Além disso, o M2C (*Machine to Cloud*) viabiliza o envio de dados para a nuvem para processamento e armazenamento, enquanto o M2P (*Machine to Person*) apresenta os dados diretamente aos usuários por meio de interfaces específicas.

Diversos protocolos de comunicação específicos para IoT têm sido desenvolvidos para atender a diferentes requisitos, como LoRaWAN, Sigfox, Zigbee, e tecnologias celulares como o *Bluetooth*, NB-IoT e LTE-M:

- **Sigfox**: Protocolo de comunicação de baixa potência e longo alcance, ideal para dispositivos que transmitem pequenas quantidades de dados. É amplamente utilizado em aplicações de rastreamento e monitoramento remoto (SIGFOX, 2024).
- **Zigbee**: Tecnologia de curto alcance e baixo consumo de energia, usada principalmente em automação residencial e industrial. É eficaz em ambientes onde os dispositivos estão próximos uns dos outros (IOT, 2024).
- **NB-IoT (*Narrowband IoT*)**: Protocolo de comunicação celular projetado para dispositivos IoT que exigem baixo consumo de energia e ampla cobertura, ideal para monitoramento de utilidades e sensores em áreas de difícil acesso (GSMA, 2024b).
- **LTE-M (*Long Term Evolution for Machines*)**: Variante do LTE, voltada para IoT, que oferece maior largura de banda e suporte para mobilidade em comparação ao NB-IoT, sendo ideal para rastreamento de veículos e outras aplicações móveis (GSMA, 2024a).
- ***Bluetooth***: Tecnologia de curto alcance, com versões voltadas para baixo consumo de energia (*Bluetooth Low Energy* - BLE), frequentemente usada em dispositivos vestíveis, sensores de proximidade e acessórios para *smartphones* (LABS, 2024).

Cada um desses protocolos se adapta a diferentes cenários, oferecendo soluções otimizadas para alcance, consumo de energia e largura de banda (SPADINGER, 2024). Protocolos como o LoRaWAN são especialmente projetados para ambientes de baixa potência e longa distância, enquanto o NB-IoT é ideal para conexões de baixa largura de banda.

A comunicação entre esses dispositivos ocorre principalmente por meio de protocolos como o LoRaWAN, amplamente adotado em sistemas IoT por sua eficiência energética e capacidade de cobrir grandes distâncias. A Figura 3 apresenta uma

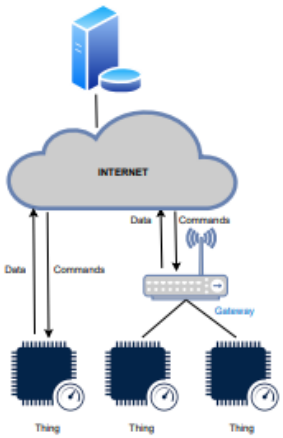

Figura 3 – Representação esquemática de uma arquitetura de rede IoT.
(PENNINO et al., 2022)

representação esquemática dessa arquitetura, destacando o fluxo de comunicação entre dispositivos IoT, *gateways* e a nuvem.

Além de LoRaWAN, outros protocolos como o ZigBee, BLE e o NB-IoT são usados para habilitar diferentes tipos de comunicação em redes IoT, dependendo das exigências de cada aplicação, como alcance, consumo de energia e largura de banda (PANARELLO et al., 2018). O uso desses protocolos sem fio em conjunto com uma infraestrutura de nuvem permite que as redes IoT sejam escaláveis e possam suportar uma vasta gama de aplicações, desde cidades inteligentes até monitoramento industrial e de saúde (SPADINGER, 2024).

A eficiência da comunicação e o design adequado da arquitetura IoT são cruciais para garantir que dispositivos com capacidades limitadas possam operar de forma eficaz em rede, mesmo em ambientes com desafios como baixa energia e alta latência.

2.1.4 SEGURANÇA EM IOT

A cibersegurança refere-se a quaisquer tecnologias, práticas e políticas que atuem na prevenção de ataques cibernéticos ou na mitigação do seu impacto. A cibersegurança tem como objetivo proteger sistemas de computador, aplicações, dispositivos, dados, ativos financeiros e pessoas contra roubos de dados e outras ameaças (IBM, 2024).

A segurança em redes IoT é particularmente crucial em aplicações críticas, como saúde, saneamento e fornecimento de energia, onde a integridade e a autenticidade dos dados são fundamentais para evitar ataques cibernéticos. Por exemplo, no setor de saúde, a conformidade com a LGPD (Lei Geral de Proteção de Dados) exige medidas rigorosas de segurança para proteger a confidencialidade dos dados dos pacientes

(KHOR et al., 2023). Já em setores como energia e infraestrutura, a autenticação de dispositivos é essencial para impedir que criminosos enviem comandos falsos, evitando ações maliciosas que poderiam comprometer sistemas inteiros (PANARELLO et al., 2018).

Apesar das vantagens da IoT, como o monitoramento em tempo real e a automação de processos, os dispositivos IoT enfrentam limitações significativas, incluindo baixa capacidade de processamento, memória e armazenamento de energia. Essas limitações dificultam a implementação de protocolos de segurança robustos. Por exemplo, muitos dispositivos não suportam certificados digitais ou criptografia avançada devido à sua baixa capacidade de memória e processamento (RAMMOUZ et al., 2023).

Mesmo diante desses desafios, a aplicação de mecanismos de segurança em IoT é essencial para proteger e manter a funcionalidade das redes. Algumas funcionalidades que esses mecanismos podem oferecer incluem:

1. **Proteção de dados críticos em aplicações sensíveis:** A IoT permite o monitoramento de ativos e ambientes críticos, como sistemas de saúde e infraestrutura pública, onde a segurança é fundamental para proteger os dados e garantir a continuidade e a operação adequadas do serviço (RAMMOUZ et al., 2023).
2. **Imutabilidade dos dados:** Mecanismos podem ser aplicados em IoT visando assegurar que os dados gerados sejam imutáveis e auditáveis, aumentando a confiança nas informações trocadas entre dispositivos e reduzindo o risco de manipulação (PANARELLO et al., 2018).
3. **Autenticação e autorização:** Podem ser utilizados mecanismos de autenticação de dispositivos, limitando a comunicação apenas a dispositivos autorizados e dessa forma, protegendo a rede contra acessos indevidos (PANARELLO et al., 2018).

Embora as limitações de *hardware* representem um obstáculo para a adoção de soluções avançadas de segurança, tecnologias como *blockchain* e protocolos específicos para IoT, como LoRaWAN, apresentam alternativas viáveis. Esses mecanismos, quando combinados, oferecem proteção robusta contra ataques e garantem maior confiabilidade em redes IoT, especialmente em aplicações que exigem alta disponibilidade e integridade dos dados.

2.2 LORAWAN: PROTOCOLO DE CONECTIVIDADE EM IOT

O LoRaWAN é um protocolo de comunicação sem fio de longa distância que opera no espectro de rádio não licenciado e é amplamente utilizado no contexto da IoT.

Este protocolo é uma das principais tecnologias de comunicação para dispositivos IoT devido à sua baixa potência, longo alcance e capacidade de operar em áreas urbanas e rurais, tornando-o ideal para aplicações que requerem conectividade de sensores distribuídos e com limitações de energia (REYNEKE; MULLINS; REITH, 2023).

No contexto de IoT, o LoRaWAN tem se destacado principalmente por sua habilidade de conectar dispositivos em redes de baixa potência (LPWANs), permitindo que sensores e dispositivos IoT operem por longos períodos usando baterias de pequena capacidade. A comunicação é realizada em grandes distâncias, que podem chegar a 20 km em áreas suburbanas e até 5 km em ambientes urbanos, o que o torna especialmente útil para monitoramento de grandes áreas, como cidades inteligentes e áreas agrícolas (DZHUNEV, 2022).

O protocolo LoRaWAN foi projetado especificamente para atender às necessidades de dispositivos IoT, oferecendo uma solução eficiente em termos de consumo de energia e custos. Ele permite que dispositivos se comuniquem com *gateways* utilizando comunicação de baixa largura de banda, com dados sendo agregados e enviados para a nuvem (RAMMOUZ et al., 2023). Dessa forma, a rede LoRaWAN permite a interoperabilidade entre dispositivos e a escalabilidade para suportar grandes redes de sensores. A Figura 4 ilustra o fluxo de comunicação típico em uma rede LoRaWAN, desde os nós sensores até o servidor de rede LoRaWAN, passando pelos *gateways* e a infraestrutura de *backhaul*.

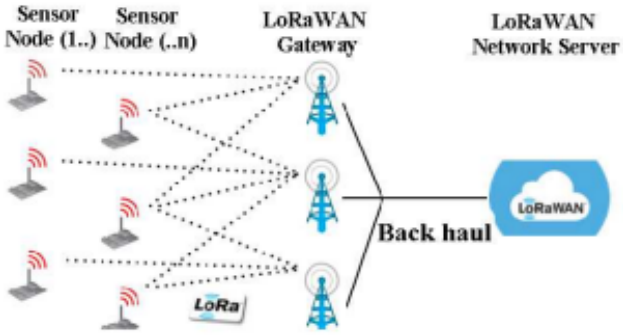

Figura 4 – Arquitetura LoRaWAN
(ALVES et al., 2020)

Características do LoRaWAN no Contexto IoT:

- **Baixa potência:** Dispositivos podem operar por anos utilizando uma única bateria, o que é crucial para sensores IoT em locais de difícil acesso.
- **Grande alcance:** Permite comunicação em áreas amplas, tanto em ambientes urbanos quanto rurais, facilitando a conectividade de redes distribuídas.
- **Custo reduzido:** Utiliza espectro de rádio não licenciado, o que reduz os custos de operação e implantação.
- **Segurança:** O LoRaWAN também possui mecanismos de criptografia de ponta a ponta para garantir a segurança na transmissão de dados, o que é vital para aplicações sensíveis em IoT, como monitoramento ambiental e controle de infraestrutura.

Além disso, o LoRaWAN se integra bem com outras tecnologias emergentes, como a *blockchain*, para melhorar a segurança e a eficiência em redes IoT, especialmente em aplicações que requerem a validação de dados e a rastreabilidade, como em redes de monitoramento de infraestrutura crítica (REYNEKE; MULLINS; REITH, 2023).

2.2.1 COMPARATIVO DE TECNOLOGIAS DE COMUNICAÇÃO EM IOT

No contexto da IoT, diversas tecnologias de comunicação são usadas para atender a diferentes requisitos, como alcance, consumo de energia e largura de banda. O LoRaWAN é uma das mais populares devido ao seu baixo consumo de energia e longo alcance, mas outras tecnologias também são importantes em aplicações específicas.

Quadro 1 – Comparação entre LoRaWAN e Outras Tecnologias IoT.

Tecnologia	**Alcance**	**Consumo de Energia**	**Largura de Banda**	**Aplicações Típicas**
LoRaWAN	5 km em áreas urbanas, até 20 km em áreas rurais	Muito baixo	Baixa	Monitoramento ambiental, agricultura, cidades inteligentes
ZigBee	Até 100 metros	Moderado	Moderada	Automação residencial, controle de iluminação
Wi-Fi	50 a 100 metros	Alto	Alta	Dispositivos de alta taxa de dados, como câmeras
***Bluetooth* LE**	10 a 100 metros	Baixo	Moderada	Dispositivos móveis e *wearables*
NB-IoT	Até 10 km	Muito baixo	Baixa	Monitoramento de utilidades, rastreamento de ativos

Fonte: Elaborado pelo autor.

Principais Diferenciais:

- **LoRaWAN** se destaca por seu longo alcance e eficiência energética, sendo ideal para monitoramento de áreas amplas, como agricultura e cidades inteligentes. Porém, tem largura de banda limitada (RAMMOUZ et al., 2023).
- **ZigBee** é mais adequado para automação residencial e aplicações de curta distância, com eficiência energética moderada, mas limitado em alcance (REYNEKE; MULLINS; REITH, 2023).
- **Wi-Fi** oferece alta largura de banda, porém, seu consumo de energia elevado o torna menos viável para dispositivos IoT de baixo consumo (REYNEKE; MULLINS; REITH, 2023).
- **Bluetooth LE** é eficiente em energia, usado principalmente em dispositivos móveis e *wearables*, mas com alcance reduzido (REYNEKE; MULLINS; REITH, 2023).
- **NB-IoT** é similar ao LoRaWAN em termos de baixo consumo e longo alcance, mas opera em espectro licenciado, o que pode aumentar os custos (PANARELLO et al., 2018).

Cada tecnologia tem suas vantagens dependendo da aplicação IoT, e o LoRaWAN é particularmente eficaz em cenários que exigem baixo custo e ampla cobertura geográfica.

2.2.2 LORAWAN E PRÁTICAS DE SEGURANÇA

A segurança é uma preocupação central nas redes IoT, especialmente em protocolos como o LoRaWAN, que conectam dispositivos distribuídos em larga escala. O protocolo LoRaWAN adota diversos mecanismos de segurança para garantir a integridade, a confidencialidade e a autenticidade dos dados transmitidos. Ele utiliza criptografia de ponta a ponta, que protege as mensagens desde o dispositivo até o servidor de rede, garantindo que apenas os dispositivos autorizados possam acessar e modificar os dados (RAMMOUZ et al., 2023) (DZHUNEV, 2022).

O LoRaWAN emprega dois níveis de criptografia:

- **Criptografia de rede:** Esta camada garante a autenticidade dos dispositivos na rede, utilizando uma chave de rede única (*NwkSKey*). Isso impede que dispositivos não autorizados participem da comunicação.
- **Criptografia de aplicação:** Os dados de usuário são criptografados utilizando uma chave de aplicação (*AppSKey*). Essa camada garante que apenas os servidores de aplicação, e não os intermediários, possam acessar os dados transmitidos.

Além disso, o protocolo LoRaWAN usa o método de autenticação de mutual *challenge-response*, o que evita ataques de repetição (*replay attacks*) e garante que a comunicação seja protegida contra interceptação e modificações durante o tráfego de mensagens (DZHUNEV, 2022) Esses mecanismos são projetados para reduzir vulnerabilidades comuns em redes sem fio, como a falsificação de pacotes e a interceptação de dados.

No entanto, mesmo com esses mecanismos de segurança, o LoRaWAN enfrenta alguns desafios, especialmente em ambientes onde há um grande número de dispositivos. A segurança das chaves criptográficas se torna um ponto de atenção crítico, pois um comprometimento dessas chaves pode expor toda a rede a riscos (REYNEKE; MULLINS; REITH, 2023). Além disso, a implementação de medidas de segurança adicionais, como o uso de *blockchain* para autenticação e verificação de dispositivos, tem sido proposta como uma forma de fortalecer a segurança em redes LoRaWAN (DZHUNEV, 2022).

2.3 TECNOLOGIA BLOCKCHAIN

Blockchain é uma tecnologia de registro distribuído que tem ganhado destaque pela sua capacidade de garantir a segurança, integridade e transparência nas transações de dados. Originalmente desenvolvida para sustentar o funcionamento de criptomoedas, como o Bitcoin, a tecnologia *blockchain* transcendeu seu uso inicial e

atualmente é aplicada em diversas áreas, como finanças, gestão de identidade, cadeias de suprimentos e IoT (SIQUETTE, 2020). A principal característica do *blockchain* é sua arquitetura descentralizada, que elimina a necessidade de intermediários, permitindo que transações sejam registradas de forma imutável e auditável em uma rede *peer-to-peer* (ALVES et al., 2020).

A Figura 5 ilustra a diferença na comunicação entre uma rede com arquitetura cliente/servidor, onde o servidor desempenha um papel central, e uma rede *peer-to-peer*, na qual os nós trocam informações diretamente entre si para alcançar um objetivo comum.

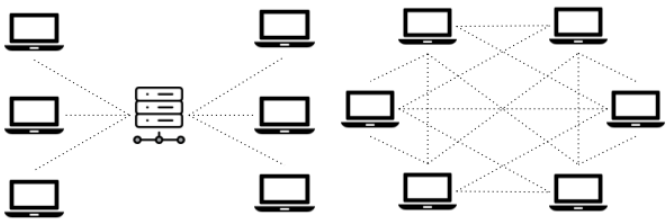

Figura 5 – Arquitetura cliente-servidor e arquitetura *peer-to-peer*.

(ALVES et al., 2020)

O *blockchain* opera através de uma cadeia de blocos, onde cada bloco contém um conjunto de transações, um identificador único (*hash*) e a referência ao bloco anterior, formando uma sequência linear e cronológica de eventos que não pode ser alterada sem o consenso da rede (SANTOS; SOUSA, 2024). Essa estrutura oferece um alto nível de segurança, garantindo que os dados armazenados sejam confiáveis e à prova de manipulações, o que torna a tecnologia atrativa para diversas aplicações além das criptomoedas.

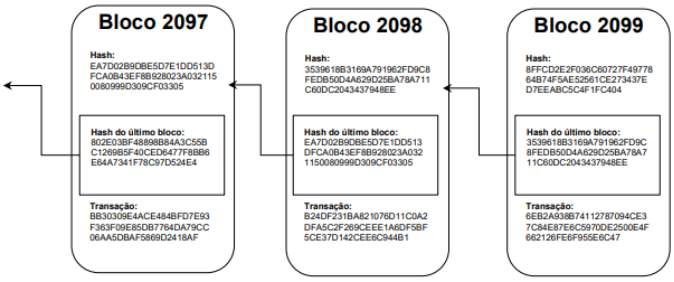

Figura 6 – Cadeia de blocos na rede *Blockchain*.

(ALVES et al., 2020)

A Figura 6 apresenta uma representação de como blocos são encadeados em uma rede *blockchain*, compostos por uma *hash* que o identifica de forma única na rede, a identificação do bloco anterior e o identificador da transação correspondente.

2.3.1 CONCEITO E DESENVOLVIMENTO DA TECNOLOGIA BLOCKCHAIN

Blockchain é uma tecnologia de registro descentralizado que funciona como um livro-razão distribuído e imutável, no qual as transações são organizadas em blocos e vinculadas em sequência. Esse sistema garante que, uma vez registrada, uma transação não possa ser alterada sem a validação de todos os nós participantes da rede, proporcionando um alto nível de integridade e segurança dos dados (ALVES et al., 2020).

A evolução da *blockchain* começou em 2008 com o lançamento do Bitcoin, desenvolvido por um autor anônimo sob o pseudônimo de Satoshi Nakamoto, com o objetivo de criar uma moeda digital descentralizada. O modelo do Bitcoin utilizava um processo de validação chamado prova de trabalho (*Proof of Work*), em que os mineradores competem para validar transações e garantir a segurança da rede (SIQUETTE, 2020).

Desde então, a tecnologia evoluiu para além das criptomoedas, passando a ser utilizada em contratos inteligentes, gestão de identidades digitais e rastreabilidade em cadeias de suprimentos, entre outras aplicações. Cada nova geração de *blockchain* trouxe avanços, como o uso de contratos inteligentes na Ethereum e de mecanismos de consenso mais eficientes, como prova de participação (*Proof of Stake*), que consome menos energia e facilita a adoção da tecnologia em larga escala (KHOR et al., 2023).

Esse avanço demonstra como a *blockchain*, inicialmente focada no setor financeiro, foi adaptada para solucionar problemas em áreas diversas, oferecendo transparência e segurança em setores críticos e reduzindo a dependência de intermediários.

2.3.2 SEGURANÇA EM BLOCKCHAIN

A segurança é um dos principais atrativos da tecnologia *blockchain*, garantida por mecanismos avançados de criptografia e estratégias de prevenção contra ataques cibernéticos. A estrutura descentralizada da *blockchain* dificulta a modificação de dados, uma vez que todas as transações são registradas em blocos que dependem de consenso e são imutáveis. Este nível de segurança é fundamental em redes que envolvem transações sensíveis, como finanças, saúde e IoT (ALVES et al., 2020).

Criptografia em *Blockchain*:

A *blockchain* utiliza criptografia assimétrica para proteger a identidade dos participantes e assegurar a integridade das transações. Cada usuário possui uma chave pública, que funciona como um identificador visível para a rede, e uma chave

privada, usada para assinar transações e garantir que apenas o proprietário pode autorizar movimentações de dados ou recursos (SIQUETTE, 2020). Esse modelo de assinatura digital evita que dados sejam alterados sem a devida autorização, reduzindo riscos de adulteração e fraudes.

Além disso, a estrutura de *hashing*, que cria uma sequência única de caracteres para representar os dados de um bloco, é usada para garantir a interdependência entre os blocos. Qualquer tentativa de alteração nos dados de um bloco resulta na modificação do *hash* correspondente, o que invalida toda a cadeia subsequente e alerta a rede sobre um possível ataque (ALVES et al., 2020).

Prevenção de Ataques:

Mesmo com criptografia e *hashing*, a *blockchain* precisa de estratégias adicionais para prevenir ataques específicos. Dentre os ataques comuns estão:

- **Ataques de 51%:** Esses ataques ocorrem quando um agente mal-intencionado consegue controlar mais de 50% do poder de mineração da rede, permitindo-lhe modificar transações e comprometer a integridade dos dados. Redes descentralizadas com ampla distribuição de participantes reduzem a probabilidade desse ataque.
- **Ataques *Sybil*:** Consiste na criação de várias identidades falsas para manipular o consenso da rede. Redes que utilizam provas de participação ou sistemas de autenticação robustos conseguem mitigar esse tipo de ameaça.
- **Ataques de Repetição (*Replay Attacks*):** Em redes IoT, esse tipo de ataque intercepta dados legítimos e os reproduz repetidamente. A *blockchain* lida com essa ameaça por meio de autenticação e carimbos de tempo, que evitam que transações antigas sejam reutilizadas.

Por meio da criptografia, do *hashing* e de uma abordagem distribuída, a *blockchain* proporciona uma segurança robusta. Esses mecanismos são continuamente aprimorados para lidar com novas ameaças, garantindo que a tecnologia se mantenha resiliente frente a ataques cada vez mais sofisticados (SANTOS; SOUSA, 2024).

2.3.3 BLOCKCHAIN PÚBLICA VS. PRIVADA PARA IOT

A escolha entre *blockchain* pública e privada é fundamental para implementar soluções de IoT, já que cada tipo possui características distintas em termos de segurança, escalabilidade e controle de dados. A *blockchain* pública é uma rede aberta,

onde qualquer usuário pode participar, validar transações e visualizar o histórico de registros (SANTOS; SOUSA, 2024). Esse tipo de *blockchain* oferece alta transparência e segurança, pois depende de mecanismos de consenso descentralizados, como a prova de trabalho (PoW) ou a prova de participação (PoS), o que dificulta ataques e manipulações de dados. No entanto, *blockchains* públicas, como Bitcoin e Ethereum, apresentam desafios para a IoT devido ao elevado consumo de energia e à lentidão das transações.

Por outro lado, a *blockchain* privada restringe o acesso à rede a um grupo seleto de participantes autorizados. Isso permite maior controle sobre os dados e processos e é comumente adotado em aplicações de IoT corporativas, onde a segurança e a eficiência são essenciais. *Blockchains* privadas podem adotar mecanismos de consenso mais leves e menos custosos, como o consenso por prova de autoridade (*Proof of Authority* - PoA), que permite maior escalabilidade e eficiência energética, adaptando-se melhor às necessidades de dispositivos IoT de baixa potência. No entanto, esse modelo sacrifica parte da transparência e descentralização que caracterizam as *blockchains* públicas (ALVES et al., 2020).

Quadro 2 – Comparação entre *Blockchain* Pública e Privada para IoT.

Aspecto	***Blockchain* Pública**	***Blockchain* Privada**
Transparência	Alta	Restrita a participantes autorizados
Segurança	Alta, devido à descentralização	Moderada, com controle centralizado
Consumo de Energia	Alto	Baixo
Escalabilidade	Limitada	Alta
Controle de Acesso	Aberto para todos	Controlado

Fonte: Elaborado pelo autor.

A aplicação de *blockchains* públicas em IoT é mais adequada para casos que requerem transparência e confiança pública, como sistemas de monitoramento ambiental em cidades inteligentes. Já a *blockchain* privada é mais indicada para operações internas em empresas, onde o controle e a eficiência são prioritários. Ambas as abordagens têm sido exploradas para aumentar a segurança e a integridade dos dados em redes IoT, mas a escolha depende dos requisitos específicos de cada aplicação (KHOR et al., 2023).

2.4 REDE HELIUM

A Rede Helium é uma infraestrutura descentralizada projetada para conectar dispositivos de IoT com segurança e baixo consumo de energia, utilizando o protocolo

LoRaWAN e uma *blockchain* própria. Com foco em aplicações como cidades inteligentes e monitoramento ambiental, a Helium oferece uma rede pública e econômica para suportar IoT em grande escala (DZHUNEV, 2022).

Um de seus principais diferenciais é o protocolo *Proof-of-Coverage* (PoC), que recompensa os participantes com *tokens* HNT ao fornecerem cobertura de rede através de *hotspots*. Esse modelo incentiva a expansão contínua da rede, promovendo uma infraestrutura robusta e distribuída sem a necessidade de provedores tradicionais (KHOR et al., 2023).

A *blockchain* da Helium registra transações de dados, garantindo segurança e transparência, e representa uma alternativa viável para suportar o crescimento de dispositivos IoT globalmente (DZHUNEV, 2022).

2.4.1 ESTRUTURA E FUNCIONAMENTO DA REDE HELIUM

A Rede Helium é uma rede de longo alcance projetada para conectar dispositivos de IoT usando o protocolo LoRaWAN. Seu conceito principal é oferecer conectividade de baixo custo e alta eficiência energética, viabilizando a comunicação entre dispositivos IoT distribuídos em grande escala (DZHUNEV, 2022). A rede é suportada por uma infraestrutura descentralizada, onde os participantes, ao instalarem *hotspots*, ampliam a cobertura de rede e recebem incentivos em *tokens* HNT por meio do protocolo de consenso PoC.

Figura 7 – Representação esquemática da arquitetura da Rede Helium.
(HELIUM, 2024)

A arquitetura da Helium é composta por três principais elementos:

1. **Ponto de Acesso (*SenseCap hotspot*):** São dispositivos que conectam os sensores IoT à rede, operando como pontos de acesso para transmitir dados por meio de LoRaWAN. Cada *hotspot* valida sua localização e cobertura para ser recompensado pelo protocolo PoC, incentivando a expansão da rede.

2. ***Blockchain* Helium:** Registra transações de dados e valida a cobertura de rede, garantindo segurança e transparência na comunicação. A *blockchain* Helium utiliza uma abordagem pública e distribuída, permitindo que qualquer participante valide a cobertura sem a necessidade de uma autoridade central.

3. ***Tokens* HNT:** A moeda nativa da Helium *Network*, usada como incentivo para os participantes que oferecem conectividade. Os *tokens* HNT são recompensados com base na contribuição de cobertura dos *hotspots*, promovendo a ampliação contínua da rede.

Essa arquitetura permite à Helium criar uma rede IoT que alia baixo custo e segurança com o incentivo financeiro, uma solução que se adapta a diversas aplicações em cidades inteligentes, monitoramento ambiental e rastreamento de ativos, com um modelo sustentável e descentralizado (DZHUNEV, 2022).

2.4.2 FUNCIONAMENTO DO PROTOCOLO PROOF-OF-COVERAGE NA REDE HELIUM

O *Proof-of-Coverage* (PoC) é o protocolo de consenso usado pela Rede Helium para validar a cobertura de rede de forma descentralizada e segura. O PoC opera com base na localização geográfica dos *hotspots* e na comunicação entre eles, garantindo que a cobertura oferecida por cada participante seja genuína e efetiva. Este protocolo permite que a Helium mantenha uma rede distribuída e confiável, incentivando os *hotspots* a expandirem e consolidarem a conectividade de IoT (DZHUNEV, 2022).

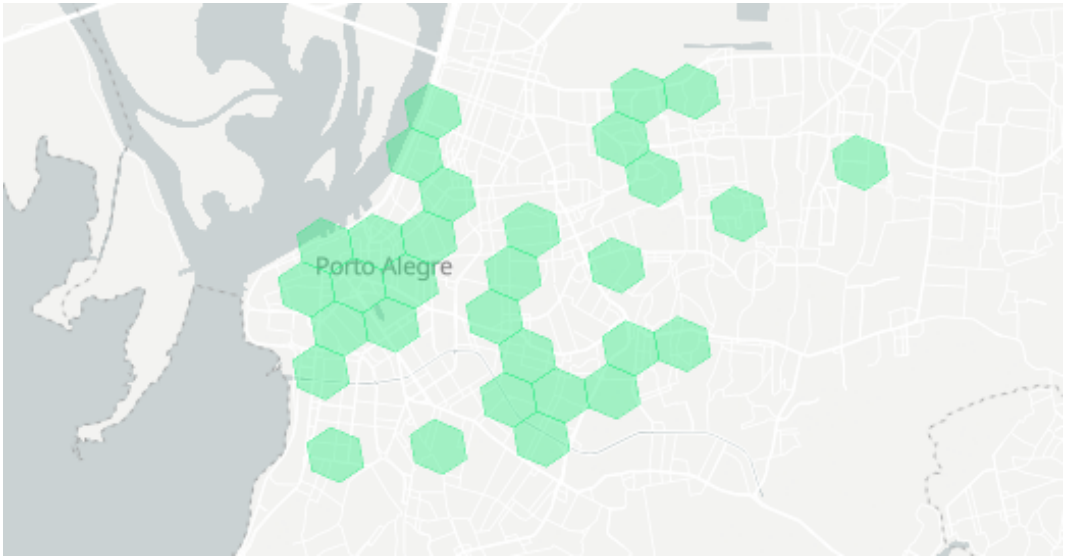

Figura 8 – Cobertura da Rede Helium em Porto Alegre.
(EXPLORER, 2024)

Como Funciona o *Proof-of-Coverage*

1. **Desafios de Cobertura (*Beacons*):** Cada *hotspot* emite sinais periódicos (*beacons*) que são detectados por outros *hotspots* próximos. Esses *beacons* servem como "desafios"para validar a localização e a cobertura do *hotspot* emissor. Os *hotspots* que capturam esses sinais confirmam que o *hotspot* emissor está em uma localização real e ativa na rede.

2. **Testemunhas (*Witnesses*):** Quando um *hotspot* emite um *beacon*, outros *hotspots* próximos atuam como "testemunhas", confirmando a recepção do sinal. Quanto maior a quantidade e a qualidade das testemunhas, mais válida é a prova de cobertura do *hotspot* emissor. Esse processo é feito de forma distribuída, permitindo que qualquer *hotspot* possa participar sem a necessidade de uma autoridade central.

3. **Recompensas em *Tokens* HNT:** Os *hotspots* que participam do PoC, seja como emissores de *beacons* ou como testemunhas, são recompensados com *tokens* HNT. A recompensa é proporcional à contribuição de cada *hotspot* na cobertura da rede, incentivando os participantes a manterem uma cobertura confiável e estável.

O PoC diferencia a Rede Helium de outras *blockchains* e redes IoT, pois permite uma validação descentralizada da cobertura geográfica em tempo real, promovendo a expansão contínua da infraestrutura de rede sem a necessidade de operadoras convencionais (DZHUNEV, 2022).

2.4.3 CASOS DE USO DA REDE HELIUM EM IOT

A Rede Helium possibilita aplicações práticas de IoT, oferecendo conectividade de longo alcance e baixo consumo de energia. Utilizando *hotspots* de fácil instalação e o protocolo LoRaWAN, a rede é voltada para soluções que exigem monitoramento e comunicação de dados (HELIUM, 2024). Abaixo estão alguns casos de uso de destaque para a Helium no contexto de IoT:

1. Monitoramento Ambiental: A Helium permite a conexão de sensores ambientais, como medidores de qualidade do ar, umidade e temperatura, possibilitando monitoramento contínuo. Essa conectividade de baixo custo e consumo é útil para órgãos governamentais e empresas interessadas na vigilância de condições ambientais em áreas urbanas e rurais (DZHUNEV, 2022).

2. Cidades Inteligentes: A infraestrutura da Helium é usada em cidades inteligentes para conectar dispositivos, como semáforos e iluminação pública inteligente,

transmitindo dados em tempo real. Isso possibilita o controle e ajuste de iluminação conforme a presença de pedestres ou veículos, otimizando o uso de energia e melhorando a segurança urbana (RAMMOUZ et al., 2023).

3. Rastreamento de Ativos e Logística: Empresas de logística podem usar a rede para monitorar a localização e o estado de contêineres e mercadorias. Sensores conectados permitem o rastreamento em tempo real, ajudando a manter o controle sobre cargas sensíveis durante o transporte (REYNEKE; MULLINS; REITH, 2023).

4. Agricultura de Precisão: A Helium é aplicada no monitoramento de fatores críticos da agricultura, como umidade do solo e temperatura, facilitando o uso eficiente de recursos naturais, como água e fertilizantes, por meio de dados coletados de sensores em áreas remotas (KHOR et al., 2023).

5. Infraestruturas Críticas: A rede também é usada para monitorar infraestruturas essenciais, como pontes e instalações industriais. Sensores de vibração e temperatura conectados à rede Helium enviam alertas sobre potenciais falhas, permitindo manutenções preventivas e garantindo a segurança (DZHUNEV, 2022).

Esses exemplos ilustram como a Helium contribui para uma infraestrutura IoT descentralizada, oferecendo soluções que combinam baixo custo e segurança, adaptando-se a diversas demandas de conectividade de longa distância e baixo consumo de energia.

2.4.4 SEGURANÇA E PRIVACIDADE NA REDE HELIUM

A Rede Helium adota práticas específicas para segurança e privacidade, fundamentais em redes de IoT descentralizadas. Utilizando o protocolo PoC, a Helium valida a localização e cobertura dos *hotspots*, mitigando ataques e garantindo a integridade dos dados transmitidos (RAMMOUZ et al., 2023)

Medidas de Segurança:

1. **Autenticação Descentralizada:** A validação de dispositivos é feita de forma descentralizada, reduzindo riscos de interceptação e aumentando a privacidade.
2. **Encriptação de Dados:** A rede utiliza criptografia ponta a ponta para proteger os dados entre dispositivos IoT e pontos de acesso, evitando acessos não autorizados.
3. **Prevenção de Ataques *Sybil*:** O PoC exige que *hotspots* provem sua localização, limitando a criação de *hotspots* falsos para manipulação de recompensas.

Privacidade dos Usuários:

A Helium mantém a privacidade ao registrar transações de forma anônima na *blockchain*. Sem armazenar informações pessoais, os participantes permanecem protegidos e anônimos na rede (RAMMOUZ et al., 2023). Essas medidas reforçam a Rede Helium como uma alternativa segura para IoT, priorizando a integridade dos dados e a proteção dos usuários.

2.5 INTEGRAÇÃO DE BLOCKCHAIN E IOT

A combinação de *blockchain* com IoT oferece uma abordagem inovadora para enfrentar desafios de segurança, privacidade e interoperabilidade em redes IoT. Com o crescimento do número de dispositivos conectados, torna-se essencial uma infraestrutura que permita o compartilhamento seguro de dados de maneira confiável e escalável. Nesse cenário, a *blockchain* introduz uma arquitetura descentralizada que protege os dados, elimina a necessidade de intermediários e proporciona transparência nas interações entre dispositivos (RAMMOUZ et al., 2023).

A integração de *blockchain* e IoT não só reforça a segurança dos dados transmitidos, mas também facilita a automação de processos com o uso de contratos inteligentes. Isso possibilita que dispositivos tomem decisões autônomas de forma segura, criando oportunidades para aplicações como monitoramento remoto, rastreamento de ativos e gestão de cidades inteligentes. No entanto, essa integração também traz desafios técnicos, como o consumo de energia e a escalabilidade, que devem ser superados para que a tecnologia atinja seu potencial completo (KHOR et al., 2023).

2.5.1 BLOCKCHAIN COM IOT: BENEFÍCIOS E DESAFIOS

A integração de *blockchain* com IoT traz benefícios significativos, especialmente em segurança e automação de processos. No entanto, essa combinação também apresenta desafios que precisam ser resolvidos para garantir seu sucesso e adoção em larga escala. Abaixo, são detalhados os principais benefícios e desafios da integração de *blockchain* com IoT:

Benefícios:

1. **Segurança e Imutabilidade dos Dados:** A *blockchain* proporciona uma camada adicional de segurança para dados de IoT, tornando-os imutáveis e verificáveis. A natureza distribuída da *blockchain* protege os dados de adulterações, oferecendo maior segurança em redes IoT sensíveis, como cidades inteligentes e infraestrutura crítica (KHOR et al., 2023).

2. **Descentralização e Redução de Intermediários:** A *blockchain* elimina a necessidade de intermediários centralizados, permitindo que dispositivos IoT compartilhem informações diretamente. Isso reduz os custos de operação e minimiza o risco de falhas em pontos únicos, tornando a rede mais resiliente e distribuída (DZHUNEV, 2022).

3. **Automação com Contratos Inteligentes:** A *blockchain* facilita a automação de processos por meio de contratos inteligentes, que executam ações automaticamente com base em condições pré-definidas. No contexto de IoT, isso possibilita que dispositivos atuem de forma autônoma, como no controle de acesso, rastreamento de ativos e monitoramento ambiental, sem a necessidade de intervenção humana (KHOR et al., 2023).

Desafios:

1. **Escalabilidade e Latência:** A quantidade de transações e dispositivos conectados em uma rede IoT é considerável, o que pode sobrecarregar a *blockchain* e aumentar a latência. Soluções como *sharding* e *off-chain* transactions estão sendo exploradas para tornar a *blockchain* mais escalável e adaptável a grandes redes de IoT (DZHUNEV, 2022).

2. **Consumo de Energia:** Protocolos de consenso, como *Proof-of-Work*, são intensivos em energia, o que é incompatível com muitos dispositivos IoT de baixo consumo. Alternativas, como *Proof-of-Stake* e *Proof-of-Coverage*, têm sido desenvolvidas para reduzir o impacto energético e tornar essa integração viável em dispositivos de baixa potência (KHOR et al., 2023).

3. **Interoperabilidade entre Dispositivos e Redes:** A diversidade de dispositivos e padrões de comunicação em IoT dificulta a integração universal com a *blockchain*. A padronização de protocolos e o desenvolvimento de sistemas interoperáveis são necessários para facilitar a comunicação entre dispositivos IoT e redes *blockchain*, permitindo que eles operem de forma eficiente e segura (REYNEKE; MULLINS; REITH, 2023).

A integração entre *blockchain* e IoT oferece vantagens notáveis para segurança e automação, mas o sucesso dessa combinação depende de avanços em escalabilidade, eficiência energética e interoperabilidade para atender às exigências de redes IoT complexas e de larga escala.

2.5.2 PROTOCOLOS DE VERIFICAÇÃO DE DADOS

Na integração entre *blockchain* e IoT, os protocolos de verificação de dados são essenciais para assegurar a integridade e autenticidade das informações. Esses protocolos garantem que as transações sejam válidas e que os dados em redes IoT distribuídas sejam confiáveis e precisos.

Principais Protocolos:

1. ***Proof-of-Work* (PoW):** Utilizado em redes como o Bitcoin, o PoW demanda alta capacidade computacional, o que o torna seguro, mas pouco viável para dispositivos IoT de baixa potência devido ao elevado consumo energético (DZHUNEV, 2022).
2. ***Proof-of-Coverage* (PoC):** Utilizado pela Rede Helium, o PoC valida a conectividade e cobertura de dispositivos IoT, especialmente em cenários que exigem grande alcance e baixo consumo de energia (REYNEKE; MULLINS; REITH, 2023).
3. ***Public Data Integrity Verification*:** Projetado para redes IoT de baixa potência, esse protocolo verifica a integridade dos dados de forma pública, sendo eficiente e adequado para IoT, onde a verificação rápida e confiável é necessária (DZHUNEV, 2022).

A escolha do protocolo depende das necessidades de segurança, eficiência energética e escalabilidade de cada aplicação IoT, garantindo robustez e proteção contra ameaças cibernéticas.

2.6 SEGURANÇA EM REDES IOT E BLOCKCHAIN

A segurança é um aspecto essencial nas redes IoT e *blockchain*, pois ambas envolvem o gerenciamento de dados sensíveis e operam em ambientes amplamente distribuídos e potencialmente vulneráveis. Em redes IoT, os dispositivos conectados coletam, processam e compartilham informações continuamente, o que pode expô-los a ataques de interceptação, manipulação de dados e acessos não autorizados. Já a *blockchain*, com sua estrutura descentralizada e imutável, oferece mecanismos para mitigar alguns desses riscos, ao mesmo tempo que enfrenta desafios específicos de segurança, como ataques de 51% e a manipulação de consenso (DZHUNEV, 2022).

A integração dessas duas tecnologias amplia as possibilidades de segurança, mas também cria novos desafios que exigem estratégias inovadoras. Enquanto a *blockchain* fornece autenticação e integridade dos dados por meio de registros distribuídos,

as redes IoT precisam lidar com restrições de recursos dos dispositivos, como processamento e armazenamento limitados. Assim, soluções de segurança em redes IoT e *blockchain* devem abordar a proteção dos dados desde a coleta até o armazenamento, buscando assegurar a privacidade e a resiliência das operações (KHOR et al., 2023).

2.6.1 PRINCIPAIS AMEAÇAS CIBERNÉTICAS EM IOT

As redes de IoT, com sua conectividade ampla e variada, estão sujeitas a uma série de ameaças cibernéticas, que são amplificadas pela falta de padronização de segurança, limitações de hardware dos dispositivos e complexidade da rede. Abaixo estão descritas algumas das principais ameaças enfrentadas por essas redes (TARIQ et al., 2023):

1. **Ataques DDoS (*Distributed Denial of Service*):** Dispositivos IoT comprometidos podem ser usados em botnets para sobrecarregar redes e servidores, interrompendo serviços essenciais. Um exemplo significativo é o ataque Mirai, que usou dispositivos IoT para gerar tráfego massivo, causando paralisação em partes da internet. Esses ataques aumentam os custos operacionais, exigindo estratégias robustas de mitigação (KUZLU; FAIR; GULER, 2021).

2. **Ataques de Interceptação de Dados (MitM):** Em ataques de *Man-in-the-Middle* (MitM), invasores interceptam e possivelmente alteram dados entre dispositivos IoT e servidores. Isso compromete a privacidade e a integridade, especialmente em setores críticos como saúde. A criptografia e autenticação são fundamentais para proteger contra esses ataques (TARIQ et al., 2023).

3. **Ataques de Repetição (Replay Attacks):** Em ataques de repetição, dados interceptados são retransmitidos, fazendo sistemas executarem comandos antigos como novos. Esse ataque pode causar falhas operacionais, especialmente em automação industrial e sistemas de segurança. Soluções incluem criptografia baseada em temporização e verificação de integridade dos dados (GIANNOUTAKIS et al., 2020).

4. **Exploração de Vulnerabilidades de *Firmware*:** Dispositivos com *firmware* desatualizado são vulneráveis a invasores, que podem explorar falhas conhecidas para obter controle total do dispositivo. A incapacidade de suportar atualizações automáticas em muitos dispositivos torna esses ataques persistentes. Atualizações seguras de *firmware* são essenciais para a proteção (KUZLU; FAIR; GULER, 2021).

5. **Ataques à Privacidade:** Com a coleta massiva de dados pessoais, ataques à privacidade em IoT são uma grande ameaça. Invasores podem acessar infor-

mações sensíveis de usuários, violando regulamentações como a LGPD. Em residências inteligentes e hospitais, isso pode comprometer a segurança e a confiança pública. A criptografia e autenticação são essenciais para proteção da privacidade (WYLDE et al., 2022).

6. **Limitações de Segurança em Dispositivos IoT:** A capacidade limitada de processamento e armazenamento dos dispositivos IoT dificulta o uso de criptografia avançada, tornando-os vulneráveis a ataques. Para esses dispositivos, é necessário desenvolver alternativas leves de segurança, como algoritmos de criptografia simplificados (TARIQ et al., 2023).

Essas ameaças reforçam a necessidade de práticas avançadas de segurança em redes IoT, como autenticação robusta, criptografia otimizada e atualizações regulares de *firmware*. A integração com tecnologias como *Blockchain* pode também adicionar uma camada de segurança, assegurando a integridade e rastreabilidade dos dados (GIANNOUTAKIS et al., 2020) (KUZLU; FAIR; GULER, 2021).

2.6.2 INTEGRIDADE DE DADOS EM BLOCKCHAIN PÚBLICA PARA IOT

A integridade de dados é essencial na integração de *blockchain* pública com IoT, dado que os dados gerados por dispositivos IoT são críticos e sensíveis. Em uma *blockchain* pública, a estrutura de blocos encadeados e protocolos de consenso, como *Proof-of-Work* e *Proof-of-Stake*, garantem que as transações de dispositivos IoT sejam autênticas e imutáveis, protegendo-as contra adulterações (DZHUNEV, 2022).

Benefícios para IoT:

1. **Transparência:** Todos os participantes podem visualizar e verificar dados armazenados, essencial para a rastreabilidade em setores como logística e saúde.

2. **Segurança e Resiliência a Ataques:** A estrutura descentralizada impede manipulações, aumentando a resistência contra ataques ao exigir consenso da rede para qualquer alteração (TARIQ et al., 2023).

3. **Autenticidade dos Dispositivos:** A *blockchain* pública permite verificar a autenticidade dos dispositivos IoT, garantindo que apenas dispositivos verificados registrem dados, essencial para operações automatizadas (GIANNOUTAKIS et al., 2020).

4. **Proteção da Privacidade com Criptografia:** Criptografia avançada na *blockchain* ajuda a proteger dados sensíveis, importante para setores que lidam com dados pessoais (WYLDE et al., 2022).

Desafios para a IoT na Blockchain Pública:

Apesar dos benefícios, a integração enfrenta alguns desafios:

1. **Consumo de Energia:** Protocolos como *Proof-of-Work* são intensivos em energia, limitando sua aplicabilidade em IoT de baixo consumo. Alternativas como *Proof-of-Stake* ajudam a mitigar esse problema (KUZLU; FAIR; GULER, 2021).
2. **Escalabilidade:** A *blockchain* pública enfrenta desafios para escalar o volume de transações em redes IoT, exigindo técnicas como *sidechains* e *sharding* (GIANNOUTAKIS et al., 2020).
3. **Custos de Armazenamento:** O armazenamento completo de dados IoT na *blockchain* é caro e consome muito espaço, tornando mais viável a utilização de *hashes* de dados para manter integridade com menor custo (GIANNOUTAKIS et al., 2020).

Esses pontos destacam os benefícios e os desafios técnicos da *blockchain* pública para IoT, evidenciando a necessidade de pesquisas em tecnologias de consenso e escalabilidade para uma integração eficiente em redes de IoT.

2.6.3 MECANISMOS DE DEFESA NA BLOCKCHAIN HELIUM

A *Blockchain* Helium emprega uma série de mecanismos de defesa para garantir a segurança e a confiabilidade dos dados transmitidos por dispositivos IoT conectados à rede. Esses mecanismos são fundamentais para proteger a rede de ataques e manipulações, especialmente devido à natureza distribuída e de longo alcance da infraestrutura Helium, que conecta dispositivos IoT usando o protocolo LoRaWAN.

Principais Mecanismos de Defesa:

1. ***Proof-of-Coverage* (PoC):** O protocolo PoC valida a conectividade dos *hotspots*, verificando sua localização e legitimidade por meio da comunicação entre dispositivos, evitando fraudes de "*hotspots* falsos".
2. **Criptografia de Dados:** A Helium protege os dados com criptografia, garantindo que apenas dispositivos autorizados possam acessar informações sensíveis, reduzindo o risco de interceptação.

3. **Descentralização e Redundância:** A estrutura descentralizada distribui as responsabilidades de validação por toda a rede, eliminando pontos únicos de falha e aumentando a resiliência contra invasões.
4. **Autenticação de Dispositivos:** Dispositivos passam por autenticação antes de transmitir dados, permitindo que apenas dispositivos verificados participem da rede.

Esses mecanismos de defesa ajudam a *Blockchain* Helium a oferecer uma infraestrutura IoT segura e confiável, com foco em criptografia, descentralização e autenticação robusta (KHOR et al., 2023) (DZHUNEV, 2022).

2.7 ESCALABILIDADE E DESEMPENHO

A escalabilidade e o desempenho são aspectos críticos para a implementação de *blockchain* em redes IoT. Com o aumento do número de dispositivos conectados, redes IoT exigem sistemas que suportem grandes volumes de dados e transações sem comprometer a eficiência. Em *blockchain* pública, onde cada transação é registrada em blocos, a escalabilidade é frequentemente um desafio, especialmente quando há necessidade de validação rápida e consumo mínimo de energia.

2.7.1 DESAFIOS DE ESCALABILIDADE EM REDES IOT

Em redes IoT, o volume de transações pode sobrecarregar a *blockchain*, causando problemas de latência e atrasos nas validações. Protocolos como PoW, usados em *blockchains* tradicionais, são lentos e consomem muita energia, tornando-os impraticáveis para a maioria das aplicações IoT, que dependem de dispositivos de baixo consumo e de rápida conectividade. (DZHUNEV, 2022).

Soluções para Melhorar a Escalabilidade:

1. ***Proof-of-Stake* (PoS) e *Proof-of-Coverage* (PoC):** Protocolos de consenso alternativos, como PoS e PoC, oferecem soluções de baixo consumo de energia e são mais rápidos, adaptando-se melhor às necessidades de redes IoT de larga escala. O PoC, utilizado na Rede Helium, permite validações rápidas de cobertura com baixo custo energético.
2. **Soluções *Off-Chain*:** Processos de verificação e validação *off-chain* permitem que algumas transações sejam executadas fora da *blockchain* principal, aliviando a sobrecarga de dados e aumentando a capacidade de resposta da rede. Essa abordagem permite que as redes IoT gerenciem um volume maior de transações sem impactar negativamente o desempenho geral.

3. ***Sharding* e Fragmentação de Dados:** A fragmentação, ou "*sharding*,"divide a *blockchain* em partes menores, cada uma gerenciada por diferentes grupos de nós. Essa técnica reduz a quantidade de dados processados por cada nó, permitindo uma operação mais eficiente e escalável para redes IoT distribuídas.

Essas soluções visam adaptar a *blockchain* às necessidades de redes IoT, onde a escalabilidade e o desempenho são cruciais para garantir conectividade eficiente e baixa latência em aplicações de larga escala, como cidades inteligentes e monitoramento ambiental (KHOR et al., 2023).

2.8 ASPECTOS LEGAIS E REGULATÓRIOS

A expansão de tecnologias como IoT e *blockchain* traz desafios legais e regulatórios complexos, especialmente à medida que esses sistemas operam em setores críticos e lidam com dados sensíveis. Questões relacionadas à privacidade, proteção de dados e conformidade regulatória são centrais para a implementação dessas tecnologias, pois envolvem tanto a segurança dos dados quanto a responsabilidade dos atores envolvidos.

2.8.1 PRIVACIDADE E PROTEÇÃO DE DADOS EM IOT E BLOCKCHAIN

A privacidade e a proteção de dados são elementos essenciais em redes IoT e *blockchain*, devido à grande quantidade de informações pessoais e sensíveis transmitidas. Em redes IoT, dispositivos conectados coletam dados contínuos sobre o ambiente e os usuários, expondo-os a riscos de invasão de privacidade e *exfiltração* de dados (REYNEKE; MULLINS; REITH, 2023). A *blockchain*, embora seja segura e imutável, enfrenta desafios relacionados à privacidade dos dados registrados, uma vez que as informações são armazenadas de forma transparente e distribuída.

Para lidar com essas preocupações, algumas soluções incluem:

- **Anonimização e Pseudonimização de Dados:** Técnicas que protegem a identidade dos usuários, permitindo o processamento e a transmissão de dados sem expor informações pessoais diretamente.
- **Compliance com Regulamentos de Privacidade:** Conformidade com leis como o Lei Geral de Proteção de Dados Pessoais (LGPD), que impõe normas rigorosas sobre o tratamento de dados pessoais e a proteção dos direitos dos titulares dos dados em redes IoT e *blockchain*.

Essas práticas buscam equilibrar a transparência oferecida pela *blockchain* com a necessidade de proteger a privacidade em redes IoT, promovendo uma abordagem de segurança que respeita os direitos dos indivíduos e garante a integridade dos dados (KHOR et al., 2023).

2.8.2 REGULAÇÕES DE BLOCKCHAIN E IOT EM AMBIENTES CRÍTICOS

Ambientes críticos, como infraestrutura de energia, saúde e transportes, requerem normas regulatórias rígidas para o uso de tecnologias como IoT e *blockchain*, pois qualquer falha nesses sistemas pode ter consequências graves para a segurança pública. A regulamentação nesses setores se concentra em garantir que os sistemas operem de forma segura e estejam protegidos contra ataques, ao mesmo tempo em que cumprem exigências de auditoria e transparência (RAMMOUZ et al., 2023).

Alguns aspectos regulatórios incluem:

- **Conformidade com Normas de Segurança Cibernética:** Em ambientes críticos, dispositivos IoT e redes *blockchain* devem atender a padrões de segurança cibernética, como a ISO/IEC 27001, que estabelece requisitos de gerenciamento de segurança da informação.
- **Monitoramento e Auditoria Contínuos:** As regulamentações exigem que sistemas IoT e *blockchain* sejam auditados regularmente para garantir a conformidade e mitigar riscos de segurança, protegendo infraestruturas críticas contra possíveis ataques e falhas.

Essas regulamentações buscam criar uma infraestrutura segura e confiável para o uso de *blockchain* e IoT, especialmente em setores onde a segurança e a conformidade são essenciais para a proteção pública e a eficiência operacional.

3 METODOLOGIA

A metodologia para este trabalho envolve o desenvolvimento e a implementação de um sensor IoT na Rede Helium, visando testar a conectividade, segurança e eficiência da rede em um ambiente controlado. Abaixo, cada etapa é detalhada para orientar o processo desde o planejamento até a avaliação dos resultados.

3.1 DEFINIÇÃO DOS REQUISITOS DO PROJETO

Nesta etapa inicial, serão definidos os requisitos técnicos e operacionais do sensor IoT e da Rede Helium para garantir que o projeto atenda aos objetivos esperados. Utilizando o sensor DHT11 para medir temperatura e umidade, o módulo RA-02 da Ai-Thinker para comunicação LoRaWAN, e o microcontrolador ESP32 com conectividade Wi-Fi, os seguintes requisitos foram estabelecidos:

- **Seleção do tipo de sensor**: O sensor DHT11 foi escolhido para este projeto devido à sua capacidade de medir temperatura e umidade com eficiência em aplicações de baixo custo. Esse sensor possui um tempo de resposta rápido e é amplamente utilizado em projetos IoT por sua precisão básica e pelo baixo consumo de energia. A decisão de monitorar temperatura e umidade baseia-se na relevância desses dados em diversos cenários, como monitoramento ambiental e controle de condições internas em edifícios.
- **Especificação do *hardware* e *software***: Para o desenvolvimento do sensor IoT integrado à Rede Helium, foram escolhidos componentes que oferecem eficiência, compatibilidade e capacidade de integração com o protocolo LoRaWAN e a *blockchain* da Helium. A seguir, as especificações de cada elemento selecionado são detalhadas.
  - **ESP32**: O microcontrolador ESP32 é um componente central no projeto, escolhido por sua versatilidade e capacidade de conectividade. Ele possui um processador dual-core de 32 bits com frequência de até 240 MHz, 520 KB de SRAM (*Static Random-Access Memory*) e conectividade Wi-Fi e Bluetooth integradas. Essas características tornam o ESP32 adequado para tarefas de processamento moderado e para a comunicação com o módulo RA-02 via SPI (*Serial Peripheral Interface*). A escolha do ESP32 permite o controle simultâneo do sensor DHT11 e do módulo LoRa, garantindo uma integração eficiente.

Figura 9 – ESP32: Microcontrolador utilizado para comunicação em redes IoT.

– **DHT11**: O sensor DHT11 foi selecionado para medir temperatura e umidade, parâmetros úteis em várias aplicações de monitoramento. Ele possui uma faixa de medição de 0 a 50 °C para temperatura e 20 a 90% para umidade, com precisão de ±2 °C e ±5% UR, respectivamente. O DHT11 comunica-se através de uma interface digital única, facilitando a integração com o ESP32. Embora seja um sensor básico, o DHT11 é suficiente para aplicações que não exigem alta precisão e possui um consumo de energia muito baixo, o que se alinha com os requisitos de IoT de longo prazo.

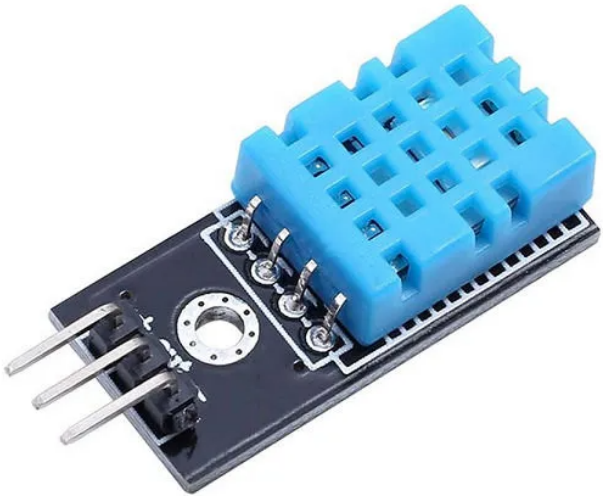

Figura 10 – DHT11: Sensor de temperatura e umidade utilizado para coleta de dados ambientais em aplicações IoT.

  - **Módulo RA-02 (LoRa da Ai-Thinker)**: Este módulo LoRa é utilizado para permitir a comunicação de longo alcance, característica essencial para a integração com a Rede Helium. O RA-02 opera na faixa de frequência de 433 MHz a 915 MHz, com alcance de até 10 km em ambientes ideais e potência de transmissão ajustável até 20 dBm. Ele usa a tecnologia de modulação LoRa, que permite uma comunicação confiável mesmo em condições de sinal fraco e consome pouca energia, fator crítico para dispositivos IoT. O RA-02 se comunica com o ESP32 por meio do protocolo SPI, garantindo uma integração eficiente. O módulo será configurado para operar em modo de baixa potência durante a transmissão e em modo de espera em períodos ociosos.

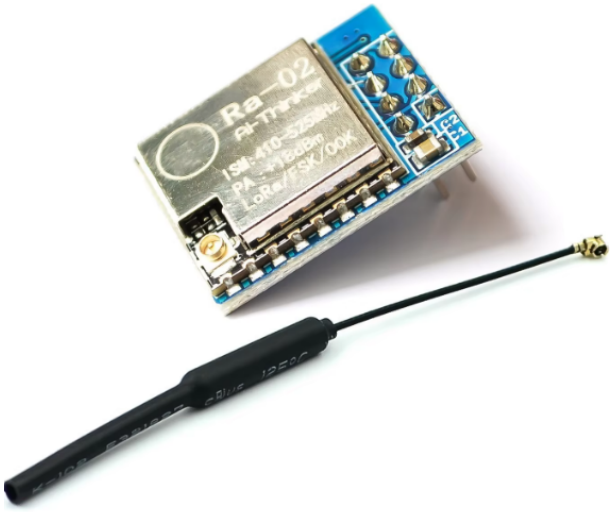

Figura 11 – RA-02: Módulo LoRa utilizado para comunicação de dados IoT em longas distâncias.

- **Desenvolvimento de *software***: O software será desenvolvido para gerenciar a coleta, o processamento e a transmissão dos dados do sensor DHT11 para a Rede Helium por meio do módulo RA-02. As etapas de desenvolvimento do *software* incluem:

  - **Programação do ESP32 em C++**: A linguagem C++ será usada para programar o ESP32, devido à sua compatibilidade com a biblioteca Arduino e ao suporte a bibliotecas específicas para o DHT11 e o RA-02. O código incluirá funções para ler dados de temperatura e umidade, gerenciar a comunicação SPI com o módulo RA-02, e controlar o modo de operação do ESP32 para economizar energia.

  - **Integração com o Protocolo LoRaWAN**: Para garantir que o dispositivo possa se comunicar eficientemente com a Rede Helium, será implementado o protocolo LoRaWAN no módulo RA-02. Isso envolve o uso de bibliotecas específicas de LoRa para Arduino/ESP32, que auxiliam no estabelecimento de comunicação com *gateways* Helium. A configuração dos parâmetros do protocolo, como *spread factor*, potência de transmissão e controle de *Duty Cycle*, será ajustada para equilibrar alcance, consumo de energia e qualidade de sinal.
  - **Gerenciamento de Consumo de Energia**: A eficiência energética é um ponto crítico para dispositivos IoT, especialmente em ambientes remotos. O software incluirá rotinas de gerenciamento de energia, alternando o ESP32 para o modo *Deep Sleep* sempre que o sensor DHT11 não estiver coletando dados ou o módulo LoRa não estiver transmitindo. O ESP32 será programado para acordar em intervalos definidos, coletar e enviar os dados, e retornar ao modo de economia de energia.
  - **Processamento de Dados e Verificação de Integridade**: Antes de enviar os dados coletados para a Rede Helium, o *software* realizará uma verificação básica de integridade para garantir que os dados de temperatura e umidade estejam dentro dos parâmetros esperados, minimizando a transmissão de dados incorretos. Além disso, serão aplicados algoritmos de hashing para assegurar que os dados enviados para a *blockchain* da Helium não possam ser alterados ou manipulados, aumentando a confiabilidade dos dados transmitidos.

- **Configuração do módulo LoRa RA-02**: O módulo RA-02 opera na frequência LoRaWAN adequada para a Rede Helium, o que exige uma configuração inicial para definir parâmetros como potência de transmissão, tempo de resposta, e intervalo de envio de dados. A configuração será ajustada para equilibrar o alcance de cobertura com o consumo de energia. A configuração de Duty Cycle será implementada para regular os períodos de inatividade e transmissão do módulo, permitindo a economia de energia em longos períodos de operação.

- **Requisitos de conectividade e cobertura**: Para avaliar o alcance e a qualidade de conectividade, o dispositivo será testado em diferentes cenários, incluindo ambientes internos e externos, com obstáculos variados. A distância de comunicação do RA-02 será medida para estabelecer a cobertura máxima viável dentro dos parâmetros da Rede Helium. Durante os testes, métricas como taxa de perda de pacotes, consumo de energia e estabilidade do sinal serão monitoradas. Esses testes visam fornecer uma análise abrangente da performance do sistema, incluindo a eficácia do protocolo LoRaWAN em cenários de longo alcance.

- **Critérios de segurança e integridade dos dados**: Considerando a importância da segurança em redes IoT, o projeto integrará medidas básicas de segurança, como autenticação de dispositivos e verificações de integridade, para garantir que os dados enviados não sejam interceptados ou alterados durante a transmissão. A autenticação no nível do dispositivo e a verificação de integridade de dados são passos fundamentais para proteger as comunicações com a Rede Helium. O uso de hash para cada pacote de dados será explorado para validar a origem e autenticidade das informações.
- **Gestão de Consumo Energético**: O sistema será otimizado para consumo de energia, um fator crucial em projetos IoT. Configurações de economia de energia do ESP32, como modo *Deep Sleep*, serão integradas para reduzir o uso de energia durante períodos ociosos. O sensor DHT11 e o módulo RA-02 também serão ativados apenas em intervalos programados.

3.2 ESTUDO DA REDE HELIUM E LORAWAN

A segunda etapa compreende uma revisão teórica e técnica aprofundada da infraestrutura da Rede Helium e do protocolo LoRaWAN, com foco nos aspectos necessários para uma implementação prática e eficiente. O estudo envolve a análise de documentação técnica, avaliação de mecanismos de segurança e configuração da rede, como detalhado abaixo:

- **Análise da documentação técnica**: Será realizada uma revisão detalhada da documentação oficial da Helium e do protocolo LoRaWAN, incluindo guias técnicos, tutoriais e especificações de configuração. O objetivo é compreender as funcionalidades oferecidas pela Rede Helium, como o modelo de incentivo com *Proof-of-Coverage* e a integração com *gateways*. Além disso, será explorada a arquitetura do LoRaWAN, que inclui a camada de aplicação, o *Network Server* e os *gateways*, para garantir que o dispositivo IoT possa ser configurado corretamente para a transmissão de dados.
- **Estrutura de segurança e autenticação**: Será conduzido um estudo dos mecanismos de segurança da Helium, com foco no protocolo de consenso *Proof-of-Coverage* (PoC). Este protocolo valida a cobertura e conectividade dos *hotspots*, recompensando-os com *tokens* HNT (*Helium Network Token*), e garante que a rede opere de forma descentralizada. Serão investigados os métodos de autenticação de dispositivos oferecidos pela Helium, incluindo a forma como dispositivos são registrados e autenticados na rede, bem como os mecanismos de criptografia usados para proteger os dados transmitidos.

- **Configuração da rede**: A configuração da Rede Helium e do protocolo LoRaWAN será estudada para garantir uma integração eficaz com o sensor IoT. Isso incluirá:
  - **Registro de dispositivos**: Revisão do processo para registrar o sensor DHT11 na Helium, utilizando o módulo RA-02 para estabelecer comunicação. Serão explorados os procedimentos para configurar as chaves de autenticação e associar o dispositivo a um *gateway* Helium.
  - **Definição de parâmetros de transmissão**: Estudo das configurações de transmissão do LoRaWAN, incluindo fatores como *spread factor*, potência de transmissão e *Duty Cycle*. Esses parâmetros serão ajustados para otimizar a eficiência energética e maximizar a cobertura do dispositivo.
  - **Integração com *gateways***: Será avaliado como os dados coletados pelo sensor IoT serão roteados para os *gateways* da Helium e, posteriormente, armazenados na *blockchain*. Essa etapa também envolve a configuração da taxa de envio de pacotes e a análise de possíveis interferências no ambiente de teste.
- **Exploração prática de casos de uso**: Além do estudo teórico, serão explorados casos práticos de uso da Helium e do LoRaWAN, como monitoramento ambiental e redes de sensores em áreas urbanas. Esses exemplos ajudarão a identificar os desafios e as oportunidades da integração, fornecendo uma base para a avaliação prática do desempenho da rede.
- **Testes iniciais em ambiente controlado**: Após a conclusão do estudo teórico, será conduzido um experimento inicial em ambiente controlado para validar a conectividade e funcionalidade da configuração. Isso inclui a medição da taxa de perda de pacotes, estabilidade de conexão e latência nos dados transmitidos pelo sensor IoT.

3.3 CONFIGURAÇÃO E DESENVOLVIMENTO DO SENSOR IOT

Nesta etapa, o sensor será preparado e configurado para operar dentro da infraestrutura da Rede Helium:

- **Programação do *firmware***: Desenvolvimento de um *firmware* customizado para o sensor, incluindo rotinas para coleta de dados, comunicação com o módulo LoRaWAN e envio de informações.
- **Configuração de comunicação LoRaWAN**: Ajuste do protocolo LoRaWAN para otimizar o uso de energia e garantir a comunicação de longa distância, com parâmetros específicos para frequências e taxas de transmissão.

- **Integração com a Helium**: Registro do sensor na Rede Helium e configuração inicial para que os dados sejam corretamente recebidos e armazenados nos servidores da rede.

3.4 IMPLEMENTAÇÃO E TESTES DA REDE

Com o sensor configurado, esta etapa inclui a realização de testes de conectividade e qualidade de transmissão na Rede Helium:

- **Teste de alcance**: Realização de testes em diferentes cenários (áreas internas e externas) para avaliar a distância máxima de transmissão com manutenção de dados consistentes.
- **Avaliação da estabilidade**: Monitoramento contínuo da qualidade de conexão, analisando taxas de perda de dados e frequência de reconexões.
- **Testes de eficiência**: Comparação do desempenho do sensor em termos de latência, consumo de energia e confiabilidade dos dados transmitidos.

3.5 ANÁLISE DOS DADOS COLETADOS

A análise dos dados coletados visa avaliar o desempenho do sensor e da Rede Helium em termos de qualidade e confiabilidade:

- **Avaliação de integridade dos dados**: Verificação da consistência dos dados coletados, analisando possíveis variações e perdas.
- **Análise de latência**: Medição do tempo de resposta entre a coleta de dados pelo sensor e a chegada dos dados aos servidores da Helium.
- **Estudo do consumo de energia**: Avaliação do consumo de energia do sensor durante os testes, para verificar se o protocolo LoRaWAN oferece a economia de energia esperada.

3.6 DOCUMENTAÇÃO DOS RESULTADOS

Nesta etapa final, os resultados do projeto serão compilados e organizados para possibilitar uma análise crítica do desempenho e da viabilidade da Rede Helium para redes IoT:

- **Análise de desempenho**: Documentação da eficácia da Rede Helium em fornecer conectividade confiável e segura para o sensor.

- **Discussão dos desafios e limitações**: Relato das dificuldades encontradas durante o desenvolvimento e dos desafios enfrentados, incluindo limitações de alcance e latência.
- **Sugestões para trabalhos futuros**: Recomendações para aprimoramentos na aplicação prática da Helium e LoRaWAN para IoT.

3.7 CRONOGRAMA

Quadro 3 – Cronograma de Desenvolvimento do Projeto

Etapas do Projeto	**Março**	**Abril**	**Maio**	**Junho**
Definição dos Requisitos	X			
Estudo da Rede Helium e LoRaWAN	X			
Configuração do Sensor IoT		X		
Implementação e Testes da Rede		X	X	
Análise dos Dados Coletados				X
Documentação dos Resultados				X

Fonte: Elaborado pelo autor.

4 CONSIDERAÇÕES FINAIS

Neste trabalho, investigou-se o potencial da Rede Helium integrada ao protocolo LoRaWAN para aumentar a segurança e eficiência de redes IoT. Através do estudo teórico e da preparação prática para a implementação de um sensor IoT, buscou-se explorar como a estrutura descentralizada da Helium e seu protocolo de consenso *Proof-of-Coverage* (PoC) podem oferecer uma solução escalável e econômica para a transmissão de dados em IoT.

As etapas planejadas para o TCC1 (Trabalho de Conclusão de Curso 1) permitiram uma análise aprofundada das tecnologias envolvidas, abordando tanto os requisitos de segurança quanto os desafios de interoperabilidade e eficiência energética que surgem em redes IoT. O levantamento bibliográfico forneceu uma base sólida para o entendimento das vantagens e limitações da Helium e do LoRaWAN, revelando a importância de protocolos de baixo consumo e de longo alcance para aplicações em grande escala.

Com a configuração prática do sensor IoT prevista para o TCC2 (Trabalho de Conclusão de Curso 2), espera-se validar os conceitos estudados e avaliar a aplicabilidade da Rede Helium para IoT em cenários reais. Assim, o trabalho desenvolvido até o momento oferece uma base teórica consistente, que norteará a fase experimental e contribuirá para a análise prática dos benefícios e limitações da integração entre IoT e *blockchain* para ambientes críticos.

REFERÊNCIAS

ALVES, P. H. et al. Desmistificando blockchain: Conceitos e aplicações. In: MACIEL, C.; VITERBO, J. (Ed.). *Computação e Sociedade*. Rio de Janeiro, RJ, Brasil: Sociedade Brasileira de Computação, 2020. Versão dos autores para distribuição. Referência para citação da versão definitiva. Disponível em: <https://doi.org/10.47820/computacaoesociedade.v5.2020>. Citado 5 vezes nas páginas 21, 24, 25, 26 e 27.

DZHUNEV, P. Helium network - integration of blockchain technologies in the field of telecommunications. In: *2022 13th National Conference with International Participation (ELECTRONICA)*. [S.l.: s.n.], 2022. p. 1–4. Citado 11 vezes nas páginas 11, 20, 23, 28, 29, 30, 31, 33, 34, 36 e 38.

EXPLORER, H. *Helium Explorer - Network Map*. 2024. Acesso em: 6 out. 2024. Disponível em: <https://explorer.helium.com/>. Citado na página 29.

GIANNOUTAKIS, K. M. et al. A blockchain solution for enhancing cybersecurity defence of iot. In: IEEE. *2020 IEEE International Conference on Blockchain (Blockchain)*. 2020. p. 490–495. Disponível em: <https://doi.org/10.1109/Blockchain50366.2020.00071>. Citado 3 vezes nas páginas 35, 36 e 37.

GSMA. *Long Term Evolution for Machine-Type Communication (LTE-M)*. 2024. Acessado em: 11 out. 2024. Disponível em: <https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/>. Citado na página 17.

GSMA. *Narrow Band Internet of Things (NB-IoT)*. 2024. Acessado em: 11 out. 2024. Disponível em: <https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/>. Citado na página 17.

HELIUM. *Helium Ecosystem*. 2024. Acesso em: 6 out. 2024. Disponível em: <https://www.helium.com/stories>. Citado 2 vezes nas páginas 28 e 30.

IBM. *Cybersecurity - IBM*. 2024. Acesso em: 21 nov. 2024. Disponível em: <https://www.ibm.com/br-pt/topics/cybersecurity>. Citado na página 18.

IOT, C. *Zigbee*. 2024. Acessado em: 11 out. 2024. Disponível em: <https://csa-iot.org/pt/todas-as-solu%C3%A7%C3%B5es/zigbee/>. Citado na página 17.

KHOR, J. H. et al. Public blockchain-based data integrity verification for low-power iot devices. *IEEE Internet of Things Journal*, IEEE, v. 10, n. 14, p. 13056–13063, 2023. Citado 11 vezes nas páginas 19, 25, 27, 28, 31, 32, 33, 35, 38, 39 e 40.

KUZLU, M.; FAIR, C.; GULER, O. Role of artificial intelligence in the internet of things (iot) cybersecurity. *Discover Internet of Things*, Springer, v. 1, p. 7, 2021. Disponível em: <https://doi.org/10.1007/s43926-020-00001-4>. Citado 3 vezes nas páginas 35, 36 e 37.

LABS, S. *Simplicity Connect Mobile App*. 2024. Acessado em: 11 out. 2024. Disponível em: <https://www.silabs.com/developers/simplicity-connect-mobile-app?source=Media&detail=Google-PPC&cid=med-gos-blu-061824&s_kwcid=AL!16736!3!549500376656!b!!g!!nordic%20bluetooth&gad_source=1&gclid=CjwKCAjwmaO4BhAhEiwA5p4YL1N_sZRROOXJL_P2CQyEBMLj91C7zpJnn5gnock69vS-Wp0Iw8Xi7xoCsGAQAvD_BwE>. Citado na página 17.

PANARELLO, A. et al. Blockchain and iot integration: A systematic survey. *Sensors*, v. 18, n. 8, p. 2575, 2018. Disponível em: <https://doi.org/10.3390/s18082575>. Citado 6 vezes nas páginas 13, 14, 16, 18, 19 e 22.

PENNINO, D. et al. Blockchain as iot economy enabler: A review of architectural aspects. *Journal of Sensor and Actuator Networks*, MDPI, v. 11, n. 2, p. 20, 2022. This article belongs to the Special Issue Journal of Sensor and Actuator Networks: 10th Year Anniversary. Disponível em: <https://doi.org/10.3390/jsan11020020>. Citado na página 18.

RAMMOUZ, V. et al. Helium-based iot devices: Threat analysis and internet-scale exploitations. In: *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. [S.l.: s.n.], 2023. p. 206–211. Citado 8 vezes nas páginas 13, 19, 20, 22, 23, 31, 32 e 40.

REYNEKE, M. A.; MULLINS, B. E.; REITH, M. G. Lorawan & the helium blockchain: A study on military iot deployment. In: *Proceedings of the 18th International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2023. p. 341–350. Disponível em: <https://doi.org/10.34190/iccws.18.1.944>. Citado 10 vezes nas páginas 11, 16, 20, 21, 22, 23, 31, 33, 34 e 39.

SANTOS, B. P. et al. Internet das coisas: da teoria à prática. In: *Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil*. Belo Horizonte, MG, Brasil: Universidade Federal de Minas Gerais (UFMG), 2024. cap. 1. {bruno.ps, lams, claysonceles, joaoborges, bperes, mmvieira, lfvieira, olga, loureiro}@dcc.ufmg.br. Citado 2 vezes nas páginas 15 e 16.

SANTOS, H. C. de L.; SOUSA, R. R. de. Além das criptomoedas: Um estudo exploratória sobre o uso do blockchain. *RECIMA21 - Revista Científica Multidisciplinar*, RECIMA21 - Ciências Exatas e da Terra, Sociais, da Saúde, Humanas e Engenharia/Tecnologia, v. 5, n. 7, 2024. ISSN 2675-6218. Disponível em: <https://doi.org/10.47820/recima21.v5i7.5461>. Citado 4 vezes nas páginas 11, 24, 26 e 27.

SIGFOX. *Supply Chain & Logistics Use Cases*. 2024. Acessado em: 11 out. 2024. Disponível em: <https://www.sigfox.com/use-cases/supply-chain-logistics/>. Citado na página 17.

SIQUETTE Ághata L. O. *Segurança da Informação com Blockchain*. Monografia de Graduação — Faculdade de Tecnologia de Americana, Americana, SP, 2020. Orientador(a): Juliane Borsato Beckedorff Pinto. Citado 3 vezes nas páginas 24, 25 e 26.

SPADINGER, R. Internet das coisas (iot), transformação digital e indústria 4.0. In: KUBOTA, L. C. (Ed.). *Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil*. 1. ed. Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada (Ipea), 2024. v. 1, cap. 6. ISBN 97885656350660. Disponível em: <http://dx.doi.org/10.38116/97885656350660cap6>. Citado 4 vezes nas páginas 14, 15, 17 e 18.

TARIQ, U. et al. A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, MDPI, v. 23, p. 4117, 2023. Disponível em: <https://doi.org/10.3390/s23084117>. Citado 2 vezes nas páginas 35 e 36.

WYLDE, V. et al. Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, Springer, v. 3, p. 127, 2022. Disponível em: <https://doi.org/10.1007/s42979-022-01020-4>. Citado 2 vezes nas páginas 36 e 37.