UNIVERSIDADE FEDERAL DO AMAZONAS FACULDADE DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

ELIMAR VINA DE ANDRADE

IOT E BLOCKCHAIN APLICADOS À AUTOMAÇÃO RESIDENCIAL: DESENVOLVIMENTO DE UM PROTÓTIPO DE SISTEMA SEGURO COM CONTROLE EM TEMPO REAL

MANAUS

2025

UNIVERSIDADE FEDERAL DO
AMAZONAS FACULDADE DE
TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

ELIMAR VINA DE ANDRADE

IOT E BLOCKCHAIN APLICADOS À AUTOMAÇÃO RESIDENCIAL: DESENVOLVIMENTO DE UM SISTEMA SEGURO COM CONTROLE EM TEMPO REAL

Dissertação apresentada ao Curso de Mestrado em Engenharia Elétrica, área de concentração Controle e Automação de Sistemas na linha de pesquisa Sistemas Inteligentes e Microeletrônica do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas.

Orientador: Prof. Dr. Carlos Augusto de Moraes Cruz

MANAUS

2025

Ficha Catalográfica

Elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

A553i Andrade, Elimar Vina de
Iot e blockchain aplicados à automação residencial: desenvolvimento de um sistema seguro com controle em tempo real / Elimar Vina de Andrade. - 2025.
69 f. ; 31 cm.

Orientador(a): Carlos Augusto de Moraes Cruz.
Dissertação (mestrado) - Universidade Federal do Amazonas, Programa de Pós-Graduação em Engenharia Elétrica, Manaus, 2025.

1. Segurança. 2. Eficiência Energética. 3. Descentralização. 4. Privacidade. 5. Interoperabilidade. I. Cruz, Carlos Augusto de Moraes. II. Universidade Federal do Amazonas. Programa de Pós-Graduação em Engenharia Elétrica. III. Título

---

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Programa de Pós-Graduação em Engenharia Elétrica

FOLHA DE APROVAÇÃO

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

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

ELIMAR VINA DE ANDRADE

IOT E BLOCKCHAIN APLICADOS À AUTOMAÇÃO RESIDENCIAL: DESENVOLVIMENTO DE UM PROTÓTIPO DE SISTEMA SEGURO COM CONTROLE EM TEMPO REAL

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.

Aprovado em 30 de setembro de 2025.

BANCA EXAMINADORA
Prof. Dr. Carlos Augusto de Moraes Cruz - Presidente
Prof. Dr. Frederico da Silva Pinagé - Membro Titular 1 - Externo
Prof. Dr. Vanderson de Lima Reis - Membro Titular 2 - Externo

Manaus, 18 de setembro de 2025.

Documento assinado eletronicamente por **Carlos Augusto de Moraes Cruz**, **Professor do Magistério Superior**, em 30/09/2025, às 13:08, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **Frederico da Silva Pinagé**, **Professor do Magistério Superior**, em 30/09/2025, às 14:52, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **VANDERSON DE LIMA REIS**, **Usuário Externo**, em 08/10/2025, às 15:30, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2802479** e o código CRC **99F14F97**.

Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Bairro Coroado Campus Universitário, Setor Norte - Telefone: 99271-8954
CEP 69080-900 Manaus/AM - Pavilhão do CETELI. E-mail: ppgee@ufam.edu.br

Referência: Processo nº 23105.041460/2025-81 SEI nº 2802479

AGRADECIMENTOS

Agradeço primeiramente a Deus por me conceder a alegria e o privilégio de viver. À minha querida família, em especial à minha amada mãe, **in memoriam**, cuja luz continua a irradiar a força que me motiva a seguir em frente. Sei que seu maior desejo era me ver crescer, e continuo buscando honrar seus ensinamentos em minha caminhada. Sou profundamente grato também aos meus familiares, por seu amor incondicional, que tem sido a base e o alicerce de minha jornada acadêmica, e aos meus amigos, pelo constante encorajamento e apoio.

Ao Professor Orientador, Dr. Carlos Augusto de Moraes Cruz, expresso minha gratidão por sua dedicação, paciência e valiosos ensinamentos, que nos guiaram através de conceitos fundamentais e nos permitiram amadurecer ao enfrentar as adversidades no desenvolvimento deste projeto.

Manifesto também meu sincero agradecimento à Universidade Federal do Amazonas (UFAM) e ao Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) pelo apoio essencial à realização desta pesquisa. Sou grato à Fundação de Amparo à Pesquisa do Estado do Amazonas (FAPEAM), no âmbito do Programa POSGRAD, Edital Nº 008/2021, bem como à CAPES e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo suporte inestimável que possibilitou a concretização deste trabalho.

RESUMO

O presente estudo tem como objetivo desenvolver um sistema de demótica baseado na integração entre a Internet das Coisas (IoT) e a tecnologia Blockchain, visando promover um ambiente doméstico mais seguro, inteligente e eficiente. A metodologia adotada envolveu o projeto e a implementação de um protótipo funcional, no qual dispositivos conectados como sensores, atuadores e controladores foram utilizados para executar tarefas automatizadas em tempo real. A Blockchain foi incorporada ao sistema para registrar de forma imutável as transações e interações entre os dispositivos, assegurando transparência e proteção dos dados. Os resultados demonstraram que o uso combinado dessas tecnologias melhora significativamente a segurança da comunicação, reduz vulnerabilidades e otimiza o consumo energético, tornando o sistema mais sustentável e escalável. Além disso, o desempenho da rede mostrou-se estável mesmo com o aumento do número de dispositivos conectados. A contribuição principal deste trabalho está em evidenciar que a aplicação de Blockchain em sistemas de demótica pode estabelecer novos padrões de segurança e confiabilidade para ambientes inteligentes, reforçando a privacidade dos usuários e a eficiência operacional. O estudo oferece uma base tecnológica promissora para o avanço de soluções residenciais inteligentes voltadas à proteção de dados e à automação segura.

Palavras-chaves: Segurança; Eficiência Energética; Descentralização; Privacidade; Interoperabilidade

ABSTRACT

This study aims to develop a Home Automation system based on the integration between the Internet of Things (IoT) and Blockchain technology, seeking to promote a safer, smarter, and more efficient domestic environment. The adopted methodology involved the design and implementation of a functional prototype, in which connected devices such as sensors, actuators, and controllers were employed to perform automated tasks in real time. Blockchain technology was incorporated into the system to immutably record the transactions and interactions among devices, ensuring transparency and data protection. The results demonstrated that the combined use of these technologies significantly improves communication security, reduces vulnerabilities, and optimizes energy consumption, making the system more sustainable and scalable. Furthermore, the network performance remained stable even as the number of connected devices increased. The main contribution of this research lies in demonstrating that the application of Blockchain in Home Automation systems can establish new standards of security and reliability for smart environments, strengthening user privacy and operational efficiency. This study provides a promising technological foundation for the advancement of intelligent residential solutions aimed at data protection and secure automation.
Keywords: Security; Energy Efficiency; Decentralization; Privacy; Interoperability.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

API	Application Programming Interface
BC	Blockchain
BSV	Bitcoin Satoshi Vision
BTC	Bitcoin
BCH	Bitcoin Cash
EdDSA	Edwards-curve Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
IoT	Internet of Things
NFT	Non-Fungible Token
PoS	Proof of Stake
PoW	Proof of Work
P2P	Peer-to-peer
PI	propriedade intelectual
RIPEMD	Race Integrity Primitives Evaluation Message Digest
SHA	Secure Hash Algorithm
sats	Satoshis
UTXO	Unspent Transaction Output

SUMÁRIO

1 INTRODUÇÃO

Na contemporaneidade, a crescente adoção da Internet das Coisas (IoT) tem transformado diversas áreas, com destaque para a automação residencial (Gubbi *et al.*, 2013); (Madakan *et al*., 2015); (Atzori *et al.*, 2010). A IoT possibilita a interconexão de dispositivos inteligentes, permitindo que eletrodomésticos, sistemas de iluminação, segurança e climatização sejam monitorados e controlados de forma remota. Essa conectividade promove maior conforto, eficiência energética e segurança, fatores que têm impulsionado o crescimento dessa tecnologia em residências ao redor do mundo.

Apesar dos benefícios, a automação residencial via IoT enfrenta desafios relacionados à segurança dos dados e à privacidade dos usuários (Fernandes *et al.*, 2016); (Sicari *et al.*, 2018); (Molina & Pastrana, 2020). A crescente quantidade de dispositivos conectados torna as redes domésticas mais vulneráveis a ataques cibernéticos, aumentando a necessidade de sistemas robustos de proteção.

Nesse contexto, a tecnologia Blockchain surge como uma solução promissora, proporcionando um ambiente mais seguro e confiável para a troca de informações entre dispositivos (Chritidis & Devetsikiotis, 2016); (Moinet *et al.,* 2017); (Zhang *et al.*, 2019). O Blockchain, conhecido por seu uso em criptomoedas, oferece descentralização, imutabilidade e transparência, o que garante que as transações realizadas em uma rede de automação residencial sejam seguras e à prova de adulterações.

Este trabalho propõe o desenvolvimento de um sistema de automação residencial que combina a IoT com a tecnologia Blockchain, de forma a otimizar a segurança, confiabilidade e o controle sobre os dispositivos conectados. O sistema de automação residencial via IOT, com o uso de blockchain. Onde, basicamente, foi criando um protótipo pra pegar a base de dados, através do Bluetooth. Criação de um circuito com um LED e uma ventoinha, em conjunto com o Bluetooth para receber a informação do blockchain. A automação residencial é importante para a verificação da funcionalidade do LED, da ventoinha que é acionado pelo o relé.

A integração dessas tecnologias visa não apenas proporcionar conveniência aos usuários, mas também garantir a proteção dos dados pessoais e o gerenciamento eficiente de energia nas residências. A proposta envolve a implementação de um sistema no qual os dispositivos da casa interagem de maneira autônoma, utilizando contratos inteligentes (*smart contracts*) baseados em Blockchain, para assegurar que cada ação seja registrada e validada de

forma segura e transparente.

Com isso, busca-se responder à crescente demanda por soluções de automação residencial que sejam não apenas funcionais, mas também seguras, reforçando a importância de incorporar tecnologias avançadas para garantir a privacidade e a integridade dos sistemas de IoT em residências conectadas.

A escalabilidade é um dos principais desafios da implementação de Blockchain em aplicações de IoT, especialmente em sistemas de automação residencial, onde o grande volume de dispositivos conectados requer uma capacidade robusta de processamento de transações (Dorri et al, 2017). A capacidade de processar um número elevado de transações por segundo (TPS) é crucial para garantir que as interações entre dispositivos IoT sejam rápidas e eficientes, evitando gargalos e atrasos no sistema (Zhou *et al.*, 2020).

Pesquisas recentes como Sharma & Park (2018) apontam para soluções que buscam otimizar a escalabilidade da Blockchain, como algoritmos de consenso mais leves e o uso de Blockchain híbrida, que combina elementos de cadeias públicas e privadas para aumentar o TPS sem comprometer a segurança.

O desenvolvimento de um Sistema de Automação Residencial via tecnologia conectada com uso de Blockchain requer a escolha das ferramentas, sendo fundamental para garantir a segurança, escalabilidade e eficiência do sistema. Algumas ferramentas essenciais podem ser divididas em categorias, sendo:

As Plataformas de Tecnologia Conectada – Arduino/ESP8266 ou ESP32 (Zia et al., 2020); (Kumar & Raj, 2019), microcontroladores populares que podem ser usados para conectar diversos sensores e dispositivos à rede doméstica, controlando funções como iluminação, temperatura e segurança. Essas placas têm boa compatibilidade com sensores e módulos de comunicação sem fio, como Wi-Fi e Bluetooth; – Raspberry Pi (Rathee et al., 2020); (Ahlawat & Malik, 2019), um minicomputador que pode ser utilizado como um hub de controle central para integrar dispositivos inteligentes. Ele oferece maior capacidade de processamento e pode rodar o software de controle da automação; e – Node-RED (Singh et al., 2020); (Al-Turjman & Nayyar, 2021), ferramenta baseada em fluxo que facilita a programação de interações entre diferentes dispositivos conectados, permitindo a criação de fluxos de trabalho visuais para a automação residencial.

Quanto às tecnologias de comunicação – MQTT (Message Queuing Telemetry Transport) (Thangavel et al., 2019); (Rani et al., 2020), protocolo de comunicação leve

amplamente utilizado em aplicações de redes inteligentes. Ele facilita a comunicação entre dispositivos com pouca latência e alta eficiência, ideal para ambientes com limitação de largura de banda. – HTTP/HTTPS (Premsankar et al., 2018); (Ismail et al., 2020), protocolo de comunicação padrão da web que pode ser usado em algumas integrações, especialmente para dispositivos que não suportam MQTT. – Zigbee/Z-Wave (Lee et al., 2019); (Song et al., 2020), protocolos de comunicação sem fio que consomem pouca energia e são amplamente utilizados em sistemas de automação residencial para conectar sensores e atuadores a uma rede central.

A Blockchain para Segurança – Ethereum (Reyna et al., 2020); (Zhang & Poslad, 2019), plataforma de Blockchain que suporta contratos inteligentes (smart contracts), permitindo a criação de regras automáticas de acesso e controle de dispositivos conectados, garantindo a segurança e a integridade dos dados transmitidos. – Hyperledger Fabric (Barger et al., 2018); (Thakkar et al., 2018), uma solução Blockchain empresarial que oferece um ambiente modular e escalável. Ideal para sistemas interconectados privados, permite maior controle sobre quem pode acessar e participar da rede. – IOTA (Popov, 2018); (Ferraro et al., 2020), protocolo Blockchain desenvolvido especificamente para ecossistemas inteligentes, com foco em transações sem taxas e alta escalabilidade, tornando-o adequado para sistemas com grande número de dispositivos.

As Plataformas de Desenvolvimento e Integração – Smart Contracts (Contratos Inteligentes) (Xu et al., 2019); (Christidis & Devertsikiotis, 2016), criados usando linguagens como Solidity (no caso do Ethereum), permitem a execução automática de comandos de controle sobre os dispositivos conectados, baseados em eventos predefinidos. – Docker (Meng et al., 2021); (Wu et al., 2020), ferramenta de conteinerização que pode ser utilizada para criar ambientes de desenvolvimento isolados para testes e implementação de diferentes componentes do sistema interligado e Blockchain. – Web3.js (Anjum et al., 2020); (Zhang et al., 2021), biblioteca JavaScript usada para interagir com o Blockchain Ethereum, permitindo que o sistema de automação residencial envie e receba informações da Blockchain de forma eficiente.

Em segurança e armazenamento de dados – IPFS (InterPlanetary File System) (Ramachandran & Krishnamachari, 2018); (Benet & Greco, 2020), sistema de arquivos descentralizado que pode ser utilizado para armazenar grandes volumes de dados gerados pelos dispositivos inteligentes. É altamente eficiente e seguro, complementando o uso de Blockchain. – AES Encryption (Alam & Noor, 2020); (Mansour & Al-Shahrani, 2019), algoritmo de criptografia simétrica que pode ser implementado para garantir a privacidade dos dados

trocados entre dispositivos conectados e o hub central.

Integração com Assistentes Virtuais – Amazon Alexa / Google Assistant (Bhatia & Puri, 2020); (Sadeghi et al., 2019), podem ser integrados ao sistema de automação residencial para permitir o controle por comando de voz, aumentando a usabilidade e a interação com os dispositivos.

As Plataformas de Monitoramento – Grafana (Rojas & Agudelo, 2021); (Ramesh & Kumar, 2022), ferramenta de visualização de dados que pode ser utilizada para monitorar as informações geradas pelo ecossistema digital, como status dos dispositivos, consumo de energia e histórico de uso. – Prometheus (Feng et al., 2020); (Khan & Mian, 2021), sistema de monitoramento e alerta que pode ser integrado para verificar a saúde dos sistemas conectados e alertar o usuário em caso de falhas ou atividades incomuns.

Essas ferramentas são essenciais para garantir que o sistema de automação residencial baseado em tecnologias inteligentes com Blockchain seja eficiente, seguro e escalável, proporcionando um controle otimizado dos dispositivos conectados e uma experiência aprimorada para os usuários.

No cenário atual de automação residencial, a segurança dos dados trocados entre dispositivos é uma preocupação crescente. A dependência de redes Wi-Fi e a vulnerabilidade dessas redes a ataques cibernéticos expõem os sistemas de automação a riscos significativos. A falta de padronização e confiabilidade nas comunicações pode comprometer o funcionamento dos dispositivos. Surge a questão: como a integração de Blockchain em um sistema de automação residencial com tecnologia inteligente pode melhorar a segurança e a confiabilidade na comunicação e no controle de dispositivos domésticos, mitigando os riscos associados às vulnerabilidades das redes Wi-Fi tradicionais?

Este trabalho propõe a implementação de um sistema de automação residencial utilizando plataformas conectadas, com a integração da tecnologia Blockchain para garantir segurança e confiabilidade na transmissão de dados. Foi criado um protótipo que coleta dados através de um módulo Bluetooth, controlando dispositivos como um LED, uma ventoinha e um relé. O sistema é capaz de monitorar e ajustar o nível de tensão, garantindo a funcionalidade e a estabilidade dos dispositivos conectados.

A automação residencial vem ganhando cada vez mais destaque, oferecendo conforto, segurança e eficiência energética. Integrar Blockchain a esses sistemas inteligentes aumenta a segurança, protegendo os dados de manipulação e ataques cibernéticos. A proposta é relevante

no contexto atual, onde a proteção de dados é crítica, especialmente em sistemas que controlam aspectos fundamentais da vida diária.

Este estudo contribui para a sociedade ao demonstrar como a tecnologia pode ser aplicada para melhorar a segurança e a eficiência das residências. O uso de dispositivos conectados para automação residencial permite que os usuários tenham maior controle sobre seus ambientes, enquanto o Blockchain garante a integridade dos dados. Isso resulta em um ambiente doméstico mais seguro e inteligente.

O protótipo desenvolvido demonstra as opções de integração entre sistemas interconectados e Blockchain em um sistema de automação residencial. O trabalho aborda tanto a implementação técnica quanto os desafios associados à integração de diferentes tecnologias. A escolha de dispositivos simples, como LED e ventoinha, permite focar na arquitetura e na comunicação segura entre os componentes, provando que o sistema pode ser escalado para dispositivos mais complexos.

1.1 Objetivos

1.1.1 Objetivo Geral

Desenvolver e testar um iot e blockchain aplicados à automação residencial: desenvolvimento de um sistema seguro com controle em tempo real, que seja capaz de controlar e monitorar dispositivos domésticos de maneira segura e eficiente.

1.1.2 Objetivos Específicos

- Implementar um protótipo que integre sensores e atuadores, como LED, ventoinha e relé, utilizando módulos IoT e Bluetooth.
- Integrar a tecnologia Blockchain ao sistema para garantir a segurança e integridade dos dados transmitidos entre os dispositivos.
- Avaliar o desempenho e a segurança do sistema, analisando a resposta dos dispositivos e a confiabilidade da comunicação em diferentes cenários.

1.2 Trabalhos Relacionados

No estudo de Naderpour *et al.* (2022), revisa-se a aplicação da tecnologia Blockchain na **Internet das Coisas**, discutindo os benefícios e desafios associados à sua implementação em ambientes de automação.

No trabalho desenvolvido por Makhdoom & Raza (2021), apresenta-se um sistema de **demótica** que combina **tecnologia conectada** e Blockchain para garantir segurança e controle eficiente sobre dispositivos domésticos.

No estudo de Mishra & Srivastava (2020), oferece-se uma visão geral das soluções de **ambientes inteligentes** que utilizam Blockchain, destacando as vantagens de segurança e privacidade.

Na pesquisa realizada por Zhou & Zhang (2022), explora-se a integração da **rede de dispositivos inteligentes** com Blockchain em casas automatizadas, discutindo as tecnologias envolvidas e seus impactos.

No estudo de Deng *et al.* (2021), descreve-se um sistema de **automação residencial inteligente** que utiliza Blockchain para aumentar a segurança e a privacidade dos dados dos usuários.

Entre os parâmetros técnicos que podem ser incluídos, destacam-se:

- **Hardware utilizado**: tipo de microcontrolador ou processador (ex.: Arduino Uno, ESP32, Raspberry Pi); memória RAM/ROM disponível; sensores e atuadores empregados (ex.: sensor DHT11, módulo relé de 5V, LED de alta potência, ventoinha de 12V).
- **Protocolos de comunicação**: Bluetooth, Wi-Fi e Zigbee.
- **Software e programação**: linguagem de programação (Java, C/C++ ou Python); ambiente de desenvolvimento (Arduino IDE, Android Studio, VSC); bibliotecas ou *frameworks* utilizados.
- **Desempenho**: tempo de resposta do sistema (latência); taxa de transmissão de dados (kbps ou Mbps); consumo energético (mA ou W); precisão ou confiabilidade da leitura dos sensores.
- **Integração com Blockchain**: plataforma utilizada (Ethereum, Hyperledger, etc.); tipo de consenso (PoW, PoS, PBFT); tempo médio de validação de transações; custos de operação (gás/energia).

Figura 1- Trabalhos Relacionados

Autor / Ano	Objetivo do Trabalho	Tecnologias Utilizadas	Contribuições Principais	Limitações Identificadas
Silva et al. (2020)	Desenvolver sistema de automação residencial baseado em IoT	Arduino, sensores, MQTT	Controle remoto via app móvel; redução de custos	Falta de integração com segurança avançada
Kumar e Singh (2021)	Garantir segurança em redes IoT para casas inteligentes	IoT, Criptografia AES	Proposta de algoritmo seguro de comunicação	Alto consumo de energia; não validado em larga escala
Oliveira et al. (2022)	Monitoramento em tempo real de dispositivos residenciais	Raspberry Pi, MQTT, App Android	Interface amigável para usuário final	Não utiliza Blockchain; vulnerável a ataques externos
Zhang et al. (2023)	Aplicar Blockchain em IoT residencial	IoT, Blockchain (Ethereum), Smart Contracts	Garantia de registros imutáveis e auditáveis	Custos elevados de transação; latência na rede

Fonte: Elaborado pelo autor, com base em Silva et al. (2020), Kumar e Singh (2021), Oliveira et al. (2022) e Zhang et al. (2023).

Para o estudo realizado por Bansal & Ranjan (2020), apresenta-se uma revisão abrangente das soluções de automação residencial baseadas em Blockchain, abordando tanto os benefícios.

A pesquisa de Khan & Arshad (2019) analisa as interações entre a Internet das Coisas e o Blockchain em sistemas de automação residencial, sugerindo direções futuras pesquisas nessa área.

No estudo desenvolvido por Ali & Noor (2020), realiza-se uma revisão sistemática sobre o papel do Blockchain na segurança de sistemas de automação residencial, também em aplicações práticas.

O estudo de Hasan & Muhammad (2022) propõe um *framework* híbrido que combina tecnologia conectada e Blockchain para automação residencial, visando a eficiência e a segurança.

Por fim, o trabalho de Saha & Bhatnagar (2021) discute um sistema de automação residencial baseado em rede de dispositivos inteligentes e Blockchain, destacando como essa integração pode aprimorar o controle e a segurança dos dispositivos.

Estabelecendo uma correlação entre os estudos citados, observa-se um panorama abrangente sobre o uso do Blockchain em sistemas de automação residencial mediados pela Internet das Coisas, evidenciando aspectos comuns e complementares em termos de segurança, privacidade e eficiência.

No quesito segurança e privacidade, os estudos de Makhdoom & Raza (2021), Mishra & Srivastava (2020) e Deng *et al.* (2021) convergem ao destacar a proteção de dados como um

dos principais benefícios proporcionados pela integração da tecnologia conectada com o Blockchain.

Os autores defendem que o Blockchain oferece um ambiente mais seguro, protegendo os dispositivos domésticos contra ataques cibernéticos e violações de privacidade. O trabalho de Ali & Noor (2020) reforça essa perspectiva ao apresentar uma revisão sistemática que confirma o papel do Blockchain como ferramenta essencial para aprimorar a segurança dos dados em sistemas de automação residencial. Essa convergência evidencia a importância de uma infraestrutura robusta para proteger as interações entre os dispositivos de ambientes inteligentes.

Quanto à eficiência e ao controle, os estudos de Hasan & Muhammad (2022) e Saha & Bhatnagar (2021) complementam essa visão ao explorar o controle otimizado dos dispositivos em residências automatizadas. Eles sugerem que a integração com Blockchain não apenas fortalece a segurança, mas também aumenta a eficiência operacional, proporcionando um controle automatizado e descentralizado.

Em consonância com esses achados, o trabalho de Makhdoom & Raza (2021) demonstra que a automação residencial pode se beneficiar da capacidade do Blockchain de gerenciar múltiplos dispositivos de forma integrada e segura.

No tocante aos desafios e limitações, diferentes autores abordam os obstáculos enfrentados pelas soluções de automação residencial baseadas em Blockchain. Naderpour *et al.* (2022) e Bansal & Ranjan (2020) discutem tanto os benefícios quanto as restrições dessa tecnologia.

Os autores apontam que, embora o Blockchain proporcione mecanismos de segurança avançados, sua implementação em larga escala enfrenta desafios de escalabilidade e complexidade, especialmente quando se trata de uma grande quantidade de dispositivos interconectados. Khan & Arshad (2019) complementam essa análise ao sugerir que o custo e a escalabilidade ainda representam barreiras significativas para a adoção em massa dessas soluções.

Por fim, no campo da inovação e das direções futuras, os trabalhos de Zhou & Zhang (2022) e Khan & Arshad (2019) se destacam ao propor o desenvolvimento de novas tecnologias e protocolos para aprimorar a integração entre a rede de dispositivos inteligentes e o Blockchain, superando desafios de latência e desempenho. Já Naderpour *et al.* (2022) oferecem uma visão mais holística, discutindo o impacto dessas tecnologias emergentes no ambiente doméstico e

sugerindo que a automação residencial tende a se tornar cada vez mais integrada, eficiente e segura à medida que tais inovações se consolidem.

Esses trabalhos, ao abordarem diferentes facetas da integração entre IoT e Blockchain, formam um quadro complementar e abrangente. Enquanto alguns autores se concentram nos aspectos de segurança e privacidade (Mishra, Deng, Ali), outros enfatizam a eficiência e o controle (Hasan, Saha). Por outro lado, autores como Naderpour e Bansal destacam os desafios e limitações dessa combinação, apontando direções futuras e possíveis soluções para os problemas existentes.

Assim, os trabalhos convergem para um consenso de que, apesar dos desafios, a Blockchain representa uma tecnologia promissora para a automação residencial, potencializando tanto a segurança quanto a eficiência em um ambiente de IoT.

A Tabela 1 representa uma comparação com diferentes abordagens do estado da arte. Essas abordagens diversas estão relacionadas com a IoT e automação via Blockchain.

Tabela 1 - Diferentes Tipos de Blockchain

Blockchain	Tecnologia	Sistema embarcado	Banco	Dispositivo
Blockchain Pública	Ethereum	ESP32/ESP8266	IPFS (InterPlanetary File System)	Sensores IoT
Blockchain Privada	Hyperledger Fabric			
Blockchain Consorciada	Corda	Raspberry Pi	BigchainDB	Atuadores
Blockchain Permissiva	Quorum	Arduino	CouchDB	Smartphones e Assistentes Virtuais

Fonte: Mishra & Srivastava (2020)

Para abordar os diferentes tipos de Blockchain, as tecnologias utilizadas, os sistemas embarcados, os bancos de dados e os dispositivos empregados em uma infraestrutura de tecnologia conectada com Blockchain, é fundamental delinear cada aspecto com base nas soluções mais comumente aplicadas. A análise detalhada desses elementos permite compreender como a integração entre dispositivos inteligentes e Blockchain pode gerar sistemas domésticos mais seguros, eficientes e escaláveis. Essa abordagem contribui para a definição de padrões técnicos e metodológicos adequados à automação residencial moderna, considerando tanto a arquitetura física quanto o software envolvido.

Mishra & Srivastava (2020) abordam a aplicação do Blockchain em sistemas de automação residencial, destacando a relevância do uso de tecnologias seguras, como Ethereum e Hyperledger, para garantir a privacidade e a integridade dos dados. Hasan & Muhammad (2022) descrevem a integração do microcontrolador ESP32 com a plataforma IOTA, a fim de desenvolver um sistema de automação doméstica isento de taxas de transação, utilizando o protocolo MQTT para comunicação entre dispositivos. Já Bansal & Ranjan (2020) discutem o uso do Raspberry Pi como hub central na implementação de sistemas baseados em rede de dispositivos inteligentes conectados à Hyperledger Fabric, possibilitando maior controle sobre os equipamentos domésticos.

Esses exemplos evidenciam a diversidade de soluções aplicadas a diferentes tipos de Blockchain, sistemas embarcados e bancos de dados, reforçando a importância da seleção tecnológica adequada para garantir eficiência, segurança e escalabilidade em sistemas de automação residencial com Internet das Coisas. Entre os principais requisitos desses sistemas, destacam-se o controle, o monitoramento e a acessibilidade, que asseguram uma interação fluida entre o usuário e os dispositivos automatizados. A funcionalidade de ligar e desligar equipamentos, como lâmpadas, ventiladores e eletrodomésticos, é normalmente implementada por meio de relés, LEDs e ventoinhas controladas por microcontroladores.

A acessibilidade e a interface de usuário também desempenham papel essencial, pois permitem que o controle seja realizado de maneira intuitiva. No presente projeto, foi desenvolvido um aplicativo Android em Java, utilizando o ambiente Android Studio, para possibilitar o controle via Bluetooth. A comunicação entre os módulos é estabelecida em um modelo mestre-escravo, assegurando o envio e recebimento de comandos de forma precisa. Essa comunicação eficiente é crucial para garantir que todos os componentes funcionem de maneira sincronizada, mantendo a confiabilidade operacional do sistema.

A segurança e a confiabilidade constituem outro pilar essencial na automação residencial. O sistema deve proteger os dados dos usuários e impedir acessos não autorizados. No projeto em análise, a integração com o Blockchain garante a segurança, a integridade e a rastreabilidade das ações executadas. Essa camada adicional de proteção permite registrar todas as operações de maneira imutável, o que fortalece a confiança no sistema e dificulta tentativas de invasão ou manipulação de dados.

A escalabilidade e a integração funcional devem ser consideradas desde a concepção do sistema. É necessário que a arquitetura permita a adição de novos sensores e atuadores, como

módulos de temperatura, umidade ou presença, sem comprometer o desempenho. O modelo baseado em Arduino e Blockchain oferece essa flexibilidade, tornando possível expandir o sistema para novas aplicações. A confiabilidade e o tempo de resposta também são fatores determinantes, uma vez que o desempenho depende diretamente da comunicação via Bluetooth e do processamento interno no Arduino, garantindo agilidade na execução dos comandos e estabilidade durante a operação.

1.3 Organização do Texto

Complementar ao conteúdo já discutido, o restante deste trabalho está organizado em cinco capítulos, da seguinte forma:

Capítulo 2: Trata dos conceitos teóricos essenciais para a compreensão dos temas abordados neste estudo.

Capítulo 3: Detalha a proposta do sistema e descreve a metodologia aplicada para o seu desenvolvimento.

Capítulo 4: Apresenta os experimentos realizados, bem como os resultados obtidos a partir dessas experiências.

Capítulo 5: Fornece as conclusões finais do trabalho e sugere direções para futuras pesquisas e aprimoramentos.

2 FUNDAMENTAÇÃO TEÓRICA

A automação residencial, também conhecida como casa inteligente, tem evoluído significativamente com a crescente adoção da Internet das Coisas (IoT). A IoT possibilita que dispositivos e sistemas interajam entre si e com os usuários, criando um ambiente mais eficiente e conveniente.

Á medida que esses sistemas se tornam mais complexos, desafios relacionados à segurança dos dados e à privacidade dos usuários surgem como questões críticas. Para mitigar esses desafios, a tecnologia Blockchain desponta como uma solução promissora, proporcionando um ambiente seguro, imutável e confiável para a troca de informações entre dispositivos IoT.

A integração de Blockchain com IoT em sistemas de automação residencial oferece vantagens como maior proteção contra-ataques cibernéticos, garantia da integridade dos dados e transparência nas transações entre os dispositivos. O uso de contratos inteligentes (*smart contracts*) possibilita a automação de regras e políticas de controle de dispositivos, aumentando a eficiência e a confiabilidade do sistema.

Nesta seção que traz a fundamentação teórica deste trabalho explora os principais conceitos e tecnologias que sustentam a implementação de um sistema de automação residencial via IoT com uso de Blockchain, abordando aspectos técnicos e teóricos, como os protocolos de comunicação, sistemas embarcados e as plataformas Blockchain adequadas para aplicações de IoT.

2. 1. Internet das Coisas (IoT) e Automação Residencial

A Internet das Coisas (IoT) revolucionou diversos setores, permitindo que dispositivos conectados à internet compartilhem dados e interajam de maneira autônoma. No contexto da automação residencial, Verma & Sood (2021), destacam que a IoT tornou possível o desenvolvimento de casas inteligentes, onde eletrodomésticos, sistemas de segurança, iluminação, e controle de temperatura podem ser monitorados e controlados remotamente, oferecendo aos usuários um maior conforto, segurança, e eficiência energética.

O conceito de automação residencial, segundo Silva et al (2020), é definido pela capacidade de monitorar e controlar dispositivos e sistemas de uma residência, como luzes, aquecedores, câmeras de segurança e eletrodomésticos, a partir de um dispositivo central ou

remotamente via smartphones e computadores.

O papel da IoT nesse cenário é conectar esses dispositivos a uma rede que permite que eles se comuniquem entre si e com o usuário, criando um ambiente integrado e inteligente.

Apesar dos benefícios em termos de conveniência e eficiência, a automação residencial também enfrenta desafios relacionados à segurança de dados e privacidade. Com a crescente quantidade de dispositivos conectados, a exposição a ataques cibernéticos também aumenta, tornando a proteção desses sistemas uma prioridade.

Pesquisas com Conoscenti et al (2018); Khan & Salah (2018); Reyna et al (2018), têm investigado maneiras de integrar tecnologias, como a Blockchain, para melhorar a segurança dos dados transmitidos entre dispositivos IoT, garantindo a confiabilidade e a integridade das informações.

A segurança dos dados é especialmente importante em sistemas de automação residencial, onde a perda ou comprometimento de dados pode ter consequências severas para a privacidade e segurança dos usuários.

Segundo Sharma et al. (2020), a IoT permite que dispositivos e sistemas residenciais interajam de maneira inteligente, oferecendo maior conveniência e eficiência energética aos usuários, ao mesmo tempo que cria desafios em termos de segurança.

A IoT possibilita a interação inteligente entre dispositivos e sistemas em residências, proporcionando aos usuários mais comodidade e eficiência energética, mas também apresenta desafios relacionados à segurança.

De acordo com Verma & Sood (2021), o crescimento do mercado de IoT residencial, o mercado de automação residencial baseada em IoT está em rápida expansão, com uma projeção de crescimento significativa devido à demanda por dispositivos conectados e eficientes.

O setor de automação residencial baseada em IoT está em rápida ascensão, com previsões de crescimento expressivas impulsionadas pela crescente demanda por dispositivos conectados e eficientes.

De acordo com Zhao et al. (2020), a segurança continua sendo um dos maiores desafios para a automação residencial baseada em IoT, com ataques cibernéticos se tornando mais sofisticados à medida que mais dispositivos são conectados.

A segurança permanece como um dos principais obstáculos para a automação residencial baseada em IoT, com ataques cibernéticos se tornando cada vez mais avançados à

medida que um número maior de dispositivos é conectado.

Ali et al (2021), destacam que os sistemas de automação residencial baseados em IoT oferecem aos usuários a capacidade de controlar remotamente seus dispositivos, aumentando a conveniência e o controle sobre a segurança e o consumo de energia.

Os sistemas de automação residencial que utilizam IoT proporcionam aos usuários a possibilidade de gerenciar seus dispositivos de forma remota, o que eleva a conveniência e o controle sobre a segurança e o consumo energético.

Segundo Naderpour et al (2022), a integração da tecnologia Blockchain em sistemas de automação residencial via IoT pode proporcionar uma solução para os problemas de segurança, garantindo a privacidade e a integridade dos dados transmitidos entre dispositivos.

A incorporação da tecnologia Blockchain em sistemas de automação residencial que utilizam IoT pode oferecer uma solução para as questões de segurança, assegurando a privacidade e a integridade das informações transmitidas entre os dispositivos.

A IoT está transformando a forma como interagimos com nossos lares, permitindo a criação de ambientes mais inteligentes e conectados. Segundo Naderpour et al (2022), a automação residencial, impulsionada por essa tecnologia, não só aumenta a conveniência e a eficiência energética, mas também proporciona um maior controle sobre a segurança dos lares. Esses avanços vêm acompanhados de desafios significativos, especialmente no que diz respeito à segurança dos dados e à proteção da privacidade dos usuários.

A integração de tecnologias como a Blockchain se apresenta como uma abordagem promissora para mitigar esses riscos, garantindo a integridade e a confidencialidade das informações transmitidas entre dispositivos. Sicari et al (2020), indicam que à medida que o mercado de automação residencial continua a crescer, será fundamental abordar as preocupações relacionadas à segurança, assegurando que as soluções implementadas sejam não apenas inovadoras, mas também robustas e confiáveis.

A intersecção entre IoT e automação residencial abre um leque de possibilidades que podem melhorar a qualidade de vida dos usuários, mas exige uma atenção contínua para os desafios que acompanham essa revolução tecnológica.

2.1.1. Definição de IoT

A IoT, segundo Vermesan & Friess (2019), é definida como uma rede de dispositivos físicos interconectados, como sensores, atuadores e sistemas, que são capazes de coletar, trocar e processar dados de forma autônoma, com o objetivo de melhorar a eficiência e otimizar

processos em diversos domínios, incluindo automação residencial, cidades inteligentes e saúde. A IoT conecta o mundo físico e o digital, permitindo a comunicação entre dispositivos sem intervenção humana direta.

Gubbi, et al (2019), destaca que a IoT é descrita como uma rede de dispositivos interconectados que permitem a comunicação e a troca de dados entre si.

Esses dispositivos, equipados com sensores e atuadores, monitoram o ambiente e interagem com outros sistemas de forma automatizada e eficiente. A IoT oferece uma visão de um futuro em que o mundo físico e o digital se fundem, facilitando o controle remoto e a automação em diversos setores, como a automação residencial, a indústria e as cidades inteligentes.

Segundo Khan et al. (2020), a IoT é uma arquitetura emergente que integra objetos físicos com a rede digital, permitindo que esses objetos interajam e compartilhem informações em tempo real.

A IoT cria um ecossistema em que dispositivos conectados coletam, transmitem e processam dados para automatizar processos e facilitar tomadas de decisão. Esta tecnologia tem aplicações potenciais em áreas como cidades inteligentes, agricultura, saúde e automação residencial, enfrentando desafios como escalabilidade, segurança e interoperabilidade entre diferentes sistemas e dispositivos.

A definição de IoT abrange a interconexão de dispositivos físicos com a rede digital, permitindo que esses dispositivos se comuniquem entre si e com sistemas centrais para coletar, processar e compartilhar dados.

Essa tecnologia possibilita o desenvolvimento de ambientes inteligentes, como automação residencial e cidades conectadas, otimizando processos e facilitando a vida dos usuários. A IoT também enfrenta desafios importantes, como segurança, privacidade e interoperabilidade entre diferentes plataformas e dispositivos.

2.1.2. Aplicações da IoT na automação residencial

As aplicações da IoT na automação residencial vêm revolucionando o conceito de casas inteligentes, permitindo que dispositivos conectados realizem tarefas automaticamente com base nas preferências dos usuários ou em condições predefinidas.

O uso de sensores, atuadores e redes de comunicação permite o controle remoto de diversos sistemas residenciais, como iluminação, aquecimento, refrigeração, eletrodomésticos

e segurança, facilitando também o gerenciamento do consumo de energia, o que oferece mais comodidade e eficiência aos usuários. Conforme destacado por Gubbi et al. (2019), a IoT transforma residências em ambientes inteligentes, integrando dispositivos conectados para automatizar e otimizar tarefas diárias.

Esses sistemas criam um ambiente onde os dispositivos interagem entre si, oferecendo maior conforto e segurança, além de eficiência energética, já que podem ser programados para operar de maneira otimizada.

Khan et al (2020), ressaltam que a integração de assistentes virtuais, como a *Amazon Alexa e Google Assistan*t, também aprimora a experiência do usuário, permitindo controle por comandos de voz, isso mostra que a automação residencial baseada em IoT está em franca expansão devido à crescente demanda por casas mais inteligentes e seguras

Os desafios permanecem, especialmente relacionados à segurança e privacidade dos dados trocados entre os dispositivos. A figura 1 destaca diferentes opções e mecanismos de automatizar ambientes residenciais.

Figura 2 - A automatização residencial e aplicação da IOT.

Fonte: FRAHM (2025)

A utilização de tecnologias emergentes, como Blockchain, está sendo explorada como uma forma de mitigar esses riscos, assegurando a confiabilidade e a integridade dos sistemas de automação residencial.

A IoT refere-se à capacidade de interconectar dispositivos físicos à internet, permitindo que objetos do cotidiano troquem informações de forma autônoma e remota. Isso possibilita que uma pessoa, utilizando um smartphone ou outro dispositivo inteligente, controle e monitore seus aparelhos domésticos, como lâmpadas, fechaduras e eletrodomésticos, enviando comandos em tempo real por meio da rede digital. Dessa maneira, a IoT aumenta a conveniência e eficiência no gerenciamento de tarefas domésticas e processos automatizados.

2.1.3. Arquitetura de sistemas IoT

A arquitetura de sistemas IoT é composta por várias camadas que desempenham funções específicas para garantir a comunicação, processamento e segurança dos dispositivos conectados. O Tabela 2 traz as principais camadas que compõem a arquitetura da IOT.

Tabela 2 – Composição da arquitetura do Sistema IOT

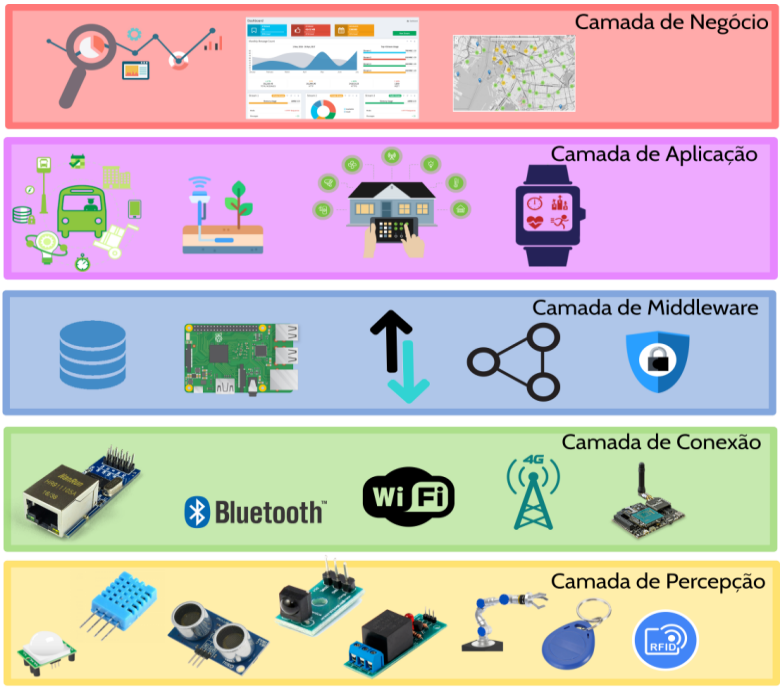
Estrutura	Descrição
Camada de Percepção	Também chamada de "camada de dispositivos", é composta por sensores e atuadores que capturam dados do ambiente físico e os transmitem para a rede. Esses dispositivos podem monitorar variáveis como temperatura, umidade, movimento, entre outros.
Camada de Conexão	Esta camada gerencia a comunicação entre os dispositivos IoT e os servidores de processamento, utilizando protocolos como Wi-Fi, Bluetooth, Zigbee ou LoRa. Seu papel é assegurar que os dados capturados pelos sensores sejam transferidos de forma eficiente e segura para a nuvem ou para outros sistemas.
Camada de Middlware	A camada de middleware atua como uma interface entre a camada de percepção, responsável pela coleta de dados por meio de sensores e atuadores, e o restante do sistema IoT, por meio da camada de conexão. Essa camada gerencia os dispositivos IoT conectados e processa os dados recebidos, garantindo que as informações sejam adequadamente armazenadas e disponibilizadas para os níveis superiores do sistema. Além disso, o middleware oferece interfaces de acesso para permitir a interação dos dados com as aplicações de usuário final, fornecendo funcionalidades de processamento, controle e análise em tempo real.
Camada de Aplicação	Esta camada inclui as interfaces que permitem ao usuário interagir com o sistema IoT, como aplicativos móveis ou interfaces web. É nessa camada que as ações, como ligar uma lâmpada ou ajustar a temperatura de um termostato, podem ser realizadas remotamente.
Camada de Negócio	Gerencia as atividades e serviços gerais do sistema IoT. Envolvida em todas as outras camadas, ela garante que as interações e os dados transferidos entre dispositivos sejam protegidos. Tecnologias como Blockchain, criptografia e autenticação de dispositivos são comuns para garantir a integridade e privacidade dos dados. essa camada é responsável por fornecer modelo de negócios, gráficos, fluxogramas e outras visualizações com base nos dados recebidos da camada Aplicação.

Fonte: Santana et al (2020)

Essa estrutura modular permite a escalabilidade e flexibilidade dos sistemas IoT, possibilitando a implementação de soluções em diversos setores, incluindo automação residencial, saúde, indústria e cidades inteligentes.

De acordo com Santana et al. (2020), o avanço da Internet das Coisas (IoT) está intimamente ligado ao desenvolvimento de novas aplicações e modelos de negócios. Diversos estudos, como os de Khan et al. (2012) e Al-Fuqaha et al. (2015), sugerem que a IoT pode ser estruturada em cinco camadas, oferecendo uma abordagem organizada para o desenvolvimento e gerenciamento de suas aplicações e funcionalidades, conforme ilustrado na figura abaixo 1.

Figura 3 - Representação de camadas da arquitetura IoT



Fonte: Andrade et al (2018)

Esta estruturação em camadas facilita o entendimento das interações entre sensores, dados e sistemas de controle, promovendo maior eficiência no gerenciamento de grandes redes de dispositivos conectados.

2.1.4. Benefícios e desafios da automação residencial via IoT

A automação residencial via IoT oferece uma série de benefícios que incluem maior conforto, eficiência energética e segurança. Dispositivos inteligentes, como sensores de movimento, sistemas de iluminação, termostatos e câmeras de segurança, podem ser controlados remotamente, permitindo que os usuários monitorem e ajustem suas casas com facilidade por meio de smartphones ou assistentes virtuais, como *Amazon Alexa e Google Assistant.* Isso melhora a gestão do consumo de energia, reduzindo custos e impactando positivamente o meio ambiente, além de proporcionar maior conveniência no dia a dia.

Um estudo de Dogan et al. (2021) destaca que o uso de tecnologias inteligentes, como sensores e atuadores, permite monitorar e otimizar o uso de energia em tempo real, ajustando automaticamente o consumo de acordo com as necessidades, o que reduz desperdícios e custos energéticos .

Essa tecnologia também enfrenta desafios consideráveis. A segurança é um dos maiores obstáculos, pois o número crescente de dispositivos conectados aumenta a vulnerabilidade a ataques cibernéticos.

Segundo Sicari et al (2015), sistemas IoT muitas vezes não são projetados com

segurança robusta, o que pode permitir acessos não autorizados. Há preocupações com a privacidade dos usuários, pois grandes quantidades de dados pessoais são coletadas e transmitidas entre dispositivos.

Enquanto a automação residencial via IoT transforma a maneira como as pessoas interagem com suas casas, é essencial enfrentar os desafios de segurança e privacidade para garantir que esses sistemas sejam confiáveis e seguros.

A automação residencial via IoT oferece benefícios significativos, como o aumento da conveniência, eficiência energética e controle remoto sobre os dispositivos, promovendo um uso otimizado dos recursos domésticos. Esses sistemas enfrentam desafios, especialmente em termos de segurança e privacidade, uma vez que grandes volumes de dados pessoais são transmitidos e armazenados, muitas vezes sem a proteção adequada. A interoperabilidade entre diferentes dispositivos e protocolos IoT ainda é uma questão a ser aprimorada para garantir uma automação doméstica mais eficiente e segura .

2.2. Protocolos de Comunicação em IoT

Os protocolos de comunicação desempenham um papel decisivo em sistemas de IoT, permitindo a troca de dados entre dispositivos e redes (Moura et al, 2020) & (Khan et al, 2018). Eles podem ser classificados em dois grupos principais: protocolos de curta distância, como Bluetooth, Zigbee e Z-Wave, que são usados em automação residencial e dispositivos de baixa potência; e protocolos de longa distância, como Wi-Fi, LoRaWAN, e NB-IoT, que são usados para conectar dispositivos a grandes distâncias com baixa latência e alta eficiência energética.

Esses protocolos são escolhidos com base em requisitos como consumo de energia, largura de banda, latência, e capacidade de transmissão de dados (Moura et al, 2020). Por exemplo, o MQTT é amplamente utilizado em IoT devido à sua leveza e eficiência em ambientes com restrições de rede, enquanto o HTTP/HTTPS é usado para garantir segurança em transmissões de dados em dispositivos que exigem integrações com a web. A escolha do protocolo ideal depende da aplicação e das características específicas do ambiente IoT.

A implementação correta dos protocolos de comunicação é essencial para garantir que os dispositivos IoT se comuniquem de forma eficiente e segura, oferecendo confiabilidade na automação de processos e controle remoto.

2.2.1. MQTT (Message Queuing Telemetry Transport)

MQTT é um protocolo de mensagens leve, projetado para comunicação em redes de

baixa largura de banda e alta latência, sendo amplamente utilizado em aplicações de IoT (De Lima et al, 2020); (Hunkeler et al, 2010).

O MQTT é especialmente projetado para comunicação em redes com largura de banda limitada e alta latência, o que o torna ideal para aplicações de Internet das Coisas. Ele utiliza um modelo de publicação/inscrição que facilita a comunicação entre dispositivos e servidores, permitindo que os dados sejam transmitidos de forma eficiente mesmo em condições adversas de conectividade. A tabela 3, destaca algumas definições sobre o MQTT.

Tabela 3 - Definições do MQTT

DEFINIÇÃO	PROPÓSITO
MQTT é descrito como um protocolo de mensagens leve e de alta eficiência que funciona em ambientes de comunicação restrita, ideal para aplicações em IoT (Dede et al., 2020).	Este protocolo é especialmente adequado para dispositivos com recursos limitados e é amplamente utilizado em automação residencial e monitoramento de sensores.
CARACTERÍSTICAS DO PROTOCOLO	
Segundo Kaur et al. (2021), "o MQTT é projetado para uma comunicação de dados eficiente, com um modelo de publicação/assinatura que permite a fácil troca de mensagens entre dispositivos.	Isso facilita a comunicação em tempo real e o controle remoto de dispositivos IoT.
VANTAGENS	
Como destacado por Alzubaidi et al. (2021), o uso do MQTT em sistemas IoT proporciona uma latência reduzida e um consumo de largura de banda significativamente menor, o que é crucial para a eficácia em ambientes de rede restrita.	

Fonte: Autoria Própria (2024)

O MQTT se adapta bem a ambientes com restrições de largura de banda e alta latência, o que o torna ideal para aplicações que exigem eficiência na transmissão de dados.

Eles também analisam comparações com outros protocolos, fornecendo uma visão crítica das suas vantagens e desvantagens. O estudo é fundamental para entender a aplicabilidade do MQTT em diferentes contextos de IoT (De Lima et al, 2020).

2.2.2. HTTP/HTTPS em IoT

HTTP (*Hypertext Transfer Protocol*) e HTTPS (*HTTP Secure*) são protocolos amplamente utilizados na Internet, incluindo em aplicações de Internet das Coisas (IoT). Eles permitem a comunicação entre dispositivos e servidores, sendo fundamentais para a transmissão de dados na web (Khan et al, 2020); (Bastos et al, 2019); (Gubbi et al, 2013).

O HTTP é amplamente utilizado para comunicação básica, enquanto o HTTPS, que incorpora criptografia, é fundamental para garantir a segurança das informações transmitidas, especialmente em contextos que envolvem dados sensíveis.

Contextualizando informações sobre os protocolos, a tabela 4 destaca informações importante sobre esses dispositivos.

Tabela 4 - Aplicação de HTTP e HTTPS na IoT

APLICAÇÕES	DESCRIÇÃO	REFERÊNCIAS
Protocolo de Comunicação	O HTTP é um protocolo de comunicação que facilita a troca de informações entre clientes (como navegadores) e servidores. No contexto da IoT, ele permite que dispositivos conectados acessem e compartilhem dados de forma eficiente. O HTTPS, por sua vez, adiciona uma camada de segurança, criptografando os dados durante a transmissão, o que é crucial em ambientes onde a privacidade e a proteção dos dados são essenciais.	Khan & Khan (2018); Da Silva & Freitas (2019); Agarwal & Singh (2020); GrewL & Bansal (2017); Manogaran & Perumal (2021)
Uso em Dispositivos IoT	Muitos dispositivos IoT utilizam HTTP/HTTPS para enviar dados a servidores e receber comandos. Por exemplo, câmeras de segurança conectadas à internet frequentemente enviam vídeos e imagens através de HTTP/HTTPS, garantindo que as informações transmitidas estejam protegidas contra interceptação.	
Desafios e Limitações	Embora HTTP/HTTPS sejam eficazes para comunicação em muitos contextos, eles podem não ser ideais para todos os dispositivos IoT. Dispositivos com recursos limitados em termos de potência e largura de banda podem enfrentar desafios ao usar esses protocolos, especialmente em situações em que a latência é crítica. Assim, muitos projetos IoT consideram o uso de protocolos alternativos, como MQTT, para situações em que a eficiência e a leveza são necessárias.	
Integração com Serviços Web	A utilização de HTTP/HTTPS em IoT também facilita a integração com serviços baseados na web, como APIs, permitindo que dispositivos conectados interajam facilmente com aplicativos móveis e sistemas de gerenciamento centralizados. Isso é essencial para criar um ecossistema IoT coeso e funcional, onde dispositivos de diferentes fabricantes possam trabalhar juntos.	

Fonte: Autoria Própria (2024)

A utilização dos protocolos HTTP e HTTPS na Internet das Coisas é decisivo para garantir uma comunicação eficaz e segura entre dispositivos e servidores. A natureza das aplicações IoT, que muitas vezes envolve a coleta e transmissão de dados sensíveis, exige a adoção de protocolos que possam garantir a integridade e a confidencialidade das informações transmitidas.

O HTTP, apesar de ser amplamente utilizado, tem cuidado com a segurança, o que torna o HTTPS uma escolha preferencial para aplicações que desativam a proteção de dados.

Estudos destacam que a implementação do HTTPS pode mitigar riscos de segurança,

como ataques de interceptação e injeção de dados (Khan et al., 2020; Bastos et al., 2019). A adoção de HTTPS também é um passo importante para atender às regulamentações de proteção de dados e aumentar a confiança dos usuários em sistemas IoT (Gubbi et al., 2013).

A combinação de HTTP/HTTPS com outros protocolos de segurança pode fornecer uma camada adicional de proteção, o que é fundamental em um ambiente onde a segurança é uma preocupação crescente devido à proteção de dispositivos conectados (Khan et al., 2020; Naderpour et al., 2022).

O uso de HTTP e HTTPS em aplicações IoT não é apenas uma questão de transmissão de dados, mas uma necessidade estratégica para garantir a segurança e a privacidade dos usuários em um cenário cada vez mais interconectado.

2.2.3. Zigbee e Z-Wave: Protocolos de comunicação sem fio para automação

Zigbee e Z-Wave são dois protocolos de comunicação sem fio amplamente utilizados na automação residencial. Ambos foram projetados para operar em redes de dispositivos de baixa potência, mas possuem características e aplicações distintas que os tornam adequados para diferentes cenários.

Zigbee é baseado na norma IEEE 802.15.4 e é conhecido por sua capacidade de conectar muitos dispositivos (até 65.000) em uma única rede. É frequentemente utilizado em aplicações de automação residencial devido à sua eficiência energética, permitindo que dispositivos funcionem por longos períodos com baterias pequenas.

O Zigbee opera em bandas de frequência de 2.4 GHz, 868 MHz e 915 MHz, permitindo uma certa flexibilidade na escolha da frequência de operação. De acordo com a Zigbee Alliance, o protocolo é ideal para aplicações que exigem uma rede robusta e escalável, como controle de iluminação, segurança e monitoramento ambiental.

Z-Wave, por outro lado, é um protocolo proprietário que opera em bandas de frequência sub-GHz, geralmente em 868 MHz na Europa e 908 MHz nos EUA. Ele permite uma comunicação ponto a ponto eficiente e é conhecido por sua facilidade de integração com dispositivos de diferentes fabricantes. O Z-Wave suporta um número menor de dispositivos em comparação ao Zigbee (cerca de 232), mas tem uma maior resistência a interferências de rádio devido à sua frequência de operação mais baixa. A Z-Wave Alliance destaca que o protocolo é amplamente utilizado em produtos de automação residencial, como fechaduras inteligentes, sensores de movimento e controle de temperatura.

A escolha entre Zigbee e Z-Wave pode depender de vários fatores, incluindo o número

de dispositivos a serem conectados, o alcance necessário e as especificações de energia dos dispositivos. Ambas as tecnologias são populares em sistemas de automação residencial, com diversos dispositivos disponíveis no mercado que suportam esses protocolos.

Esses protocolos são essenciais para a construção de lares inteligentes, permitindo que usuários controlem seus dispositivos remotamente, melhorem a eficiência energética e aumentem a segurança em suas casas.

2.2.4. Comparação entre os principais protocolos de comunicação IoT

Aqui está uma comparação entre os principais protocolos de comunicação utilizados em IoT, considerando suas características, vantagens e desvantagens, ver tabela 5.

Tabela 5 - Comparando os principais protocolos de comunicação IOT

Protocolo	Características:	Vantagens	Desvantagens
MQTT	Protocolo leve e baseado em mensagens, ideal para redes com largura de banda limitada.	Baixo consumo de energia, ideal para dispositivos com restrições de recursos. Suporta comunicação em tempo real e é amplamente utilizado em aplicações IoT.	Requer um broker para gerenciar as mensagens, o que pode introduzir um ponto único de falha.
HTTP/HTTPS	Protocolos amplamente utilizados na web, permitem a comunicação entre dispositivos e servidores.	Suporte universal e fácil integração com aplicações web; HTTPS fornece segurança através de criptografia.	Maior sobrecarga de dados e consumo de energia em comparação com protocolos mais leves como MQTT.
Zigbee	Baseado no padrão IEEE 802.15.4, ideal para redes de dispositivos de baixa potência.	Suporta muitos dispositivos, é escalável e oferece eficiência energética.	Pode ser suscetível a interferências em bandas de 2.4 GHz, onde outros dispositivos também operam.
Z-Wave	Protocolo proprietário que opera principalmente em frequências sub-GHz.	Menos suscetível a interferências e fácil de integrar, especialmente em automação residencial.	Suporta um número menor de dispositivos em comparação com Zigbee, e pode ter limitações de alcance.
LoRaWAN	Focado em comunicação de longa distância com baixo consumo de energia.	Excelente alcance e capacidade de conectar dispositivos em áreas rurais e suburbanas.	Largura de banda limitada, não ideal para aplicações que requerem transmissão de dados em tempo real.

Fonte: Autoria Própria (2024)

Tabela 6 – Parâmetros técnicos da segurança da Blockchain

Parâmetro Técnico	Função na Segurança	Aplicação no Projeto
Criptografia (hashes SHA-256, Keccak-256)	Garante que os dados não possam ser alterados sem detecção.	Cada comando enviado pelo app (ligar LED, ventoinha, relé) pode ser registrado como hash na Blockchain.
Assinaturas Digitais (chave pública/privada)	Garante que apenas usuários autorizados enviem comandos	O app Android poderia assinar digitalmente os comandos antes de transmitir via Bluetooth.

Parâmetro Técnico	Função na Segurança	Aplicação no Projeto
	válidos.	
Mecanismos de Consenso (PoW, PoS, PBFT, etc.)	Valida as transações de forma descentralizada, evitando fraudes.	A rede Blockchain valida as ações registradas (ex.: ligar/desligar ventoinha) antes de confirmar no bloco.
Imutabilidade do Registro	Impede exclusão ou alteração dos dados já gravados.	As ações do usuário ficam armazenadas permanentemente como histórico de auditoria.
Carimbo de Tempo (Timestamp)	Garante a ordem cronológica das operações.	É possível saber exatamente em que horário o usuário acionou cada dispositivo.
Resiliência à Falha	Mesmo que um nó da rede caia ou seja atacado, os outros preservam a integridade do sistema.	Em uma rede privada/testnet, ainda que um dispositivo falhe, o registro permanece seguro nos demais nós.

Fonte: Autoria Própria (2024)

A escolha do protocolo ideal depende do tipo de aplicação, da quantidade de dispositivos a serem conectados, e das condições do ambiente onde os dispositivos operarão. Uma compreensão detalhada de cada protocolo pode ajudar no desenvolvimento de sistemas IoT mais eficientes e seguros. O projeto pode ser classificado como um sistema de automação residencial (domótica) de arquitetura híbrida (centralização via Arduino e descentralização via Blockchain), com comunicação sem fio (Bluetooth)**,** controle restrito/autenticado, e com objetivos voltados para conforto, eficiência energética e segurança**.**

2.3. Blockchain: Conceitos e Aplicações

A tecnologia Blockchain é um sistema descentralizado de registro de informações que assegura a integridade e a transparência dos dados. Essa estrutura é composta por blocos de dados encadeados de forma criptográfica, o que dificulta a manipulação e o acesso não autorizado às informações.

O conceito de Blockchain ganhou notoriedade inicialmente através do Bitcoin, proposto por Satoshi Nakamoto em 2008, mas suas aplicações se estenderam muito além das criptomoedas.

Entre as principais características da Blockchain, estão a imutabilidade, a segurança e a transparência. Essas qualidades fazem dela uma solução viável para diversas áreas, incluindo a Internet das Coisas (IoT), onde pode melhorar a segurança e a privacidade dos dados trocados entre dispositivos.

A integração da Blockchain com a IoT pode proporcionar um ambiente mais seguro, garantindo que os dados coletados e transmitidos sejam autênticos e não possam ser alterados sem detecção (Zheng et al., 2018; Makhdoom et al., 2019).

As aplicações da Blockchain incluem, mas não se limitam a: Sistemas financeiros: para facilitar transações seguras e rápidas sem intermediários; Supply chain management: para rastrear a origem e o movimento de produtos em tempo real, aumentando a transparência; Identidade digital: para garantir a autenticidade e segurança de identidades online; Saúde: para gerenciar registros médicos de forma segura e acessível. Esses exemplos demonstram como a Blockchain pode ser aplicada em diversos setores, promovendo não apenas segurança, mas também eficiência e confiabilidade.

2.3.1. Definição e princípios da tecnologia Blockchain

A blockchain é uma tecnologia de registro distribuído que permite a manutenção de um registro imutável e transparente de transações em uma rede de computadores. Cada bloco de informação é encadeado a um bloco anterior, formando uma cadeia segura.

Os princípios fundamentais da blockchain incluem descentralização, transparência, segurança e imutabilidade. Segundo Nakamoto (2008), a natureza descentralizada da blockchain elimina a necessidade de intermediários, permitindo transações diretas entre partes.

2.3.2. Tipos de Blockchain: Pública, Privada e Consorciada

As blockchains podem ser classificadas em três tipos principais: Pública: Qualquer pessoa pode participar e acessar o registro, como no caso do Bitcoin. Essa transparência fortalece a confiança nas transações (Zheng et al., 2018). Privada: Acesso restrito a um grupo selecionado, frequentemente utilizado em ambientes corporativos onde a privacidade e o controle são essenciais (Dinh et al., 2017). Consorciada: Um meio-termo entre pública e privada, onde um grupo específico de organizações compartilha a responsabilidade da blockchain (Khan et al., 2020).

Essas variações permitem que a tecnologia blockchain seja adaptada a diferentes necessidades e cenários de uso.

2.3.3. Aplicação de Blockchain em IoT

A combinação de blockchain e IoT tem o potencial de revolucionar a forma como os dispositivos se comunicam e gerenciam dados. A blockchain pode ser usada para garantir a autenticidade e integridade dos dados coletados por dispositivos IoT, além de facilitar transações seguras entre eles.

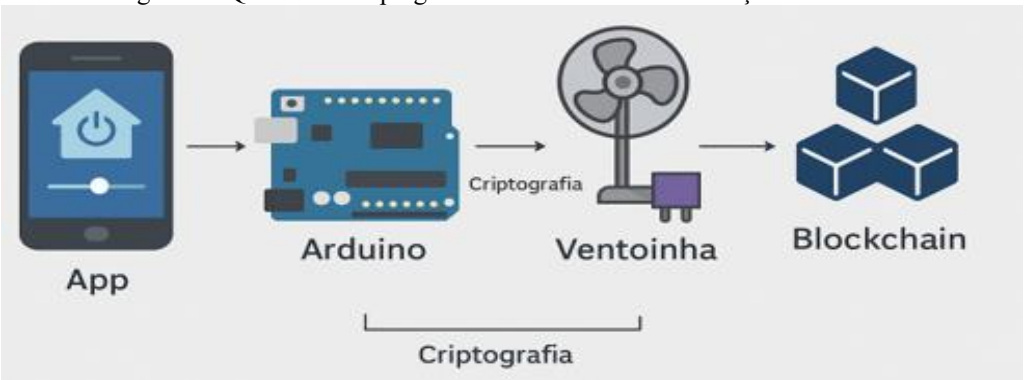
De acordo com Makhdoom et al. (2019), a utilização de blockchain em IoT pode otimizar processos em setores como saúde, transporte e energia, aumentando a eficiência e a confiabilidade dos sistemas.

2.3.4. Vantagens da Blockchain para segurança e privacidade em IoT

A implementação de blockchain em sistemas IoT oferece várias vantagens, especialmente em termos de segurança e privacidade. Primeiro, a natureza descentralizada da blockchain dificulta ataques cibernéticos, uma vez que não existe um ponto único de falha (Makhdoom et al., 2019).

A criptografia utilizada na blockchain protege os dados pessoais coletados pelos dispositivos IoT, garantindo que apenas partes autorizadas possam acessá-los (Khan et al., 2020).

Figura 3 - Quadro da Criptografia em Sistemas de Automação Residencial



Fonte: Andrade et al (2018)

Cada comando enviado pelo app Android é transformado em hash e registrado na Blockchain, garantindo que não possa ser modificado. O aplicativo pode usar assinatura digital para validar que o usuário é autorizado a enviar comandos. Dados sensíveis podem ser criptografados com AES antes de serem transmitidos via Bluetooth, protegendo contra interceptações. O uso de salt/nonce impede que um comando já executado seja reaplicado de forma indevida. A transparência proporcionada pela blockchain também permite auditorias mais eficazes e um maior controle sobre quem acessa e utiliza os dados, contribuindo para a conformidade com regulamentos de proteção de dados (Dinh et al., 2017). Essa combinação de segurança, privacidade e controle pode resultar em uma adoção mais ampla de soluções IoT em diversas indústrias.

2.4. Segurança e Privacidade em Sistemas IoT

A segurança e a privacidade em sistemas de IoT são questões críticas, especialmente à medida que mais dispositivos conectados se tornam comuns em ambientes residenciais e empresariais. Esses dispositivos muitas vezes coletam e transmitem grandes quantidades de dados pessoais, o que os torna alvos atraentes para ataques cibernéticos.

Os principais desafios de segurança em dispositivos IoT incluem a falta de padrões de segurança adequados, vulnerabilidades nas comunicações sem fio e a dificuldade em implementar atualizações de segurança em dispositivos que possuem hardware limitado (Makhdoom et al., 2019; Zheng et al., 2018).

A automação residencial pode apresentar riscos adicionais, como acesso não autorizado a sistemas de segurança e controle de dispositivos, resultando em invasões ou abusos de privacidade (Khan et al., 2020).

A aplicação de técnicas de criptografia, como a AES (*Advanced Encryption Standard*), é fundamental para proteger dados em trânsito e em repouso, garantindo que apenas usuários autorizados possam acessar as informações (Dinh et al., 2017).

Nesse contexto, o blockchain tem emergido como uma solução promissora para mitigar riscos de segurança e privacidade em sistemas IoT. A tecnologia permite a criação de um registro imutável das transações, o que pode ajudar a prevenir fraudes e garantir a integridade dos dados coletados pelos dispositivos (Makhdoom et al., 2019; Zheng et al., 2018).

A combinação dessas abordagens pode criar um ambiente mais seguro para o uso de dispositivos IoT, protegendo tanto a integridade dos dados quanto a privacidade dos usuários.

2.4.1. Desafios de segurança em dispositivos IoT

A segurança em dispositivos IoT enfrenta múltiplos desafios, principalmente devido à natureza heterogênea da tecnologia e à diversidade de ambientes em que esses dispositivos operam. Muitas vezes, esses dispositivos têm capacidades computacionais limitadas, o que dificulta a implementação de medidas robustas de segurança.

De acordo com Makhdoom et al. (2019), a falta de padrões uniformes e protocolos de segurança eficazes contribui para as vulnerabilidades presentes nos sistemas IoT. Além disso, a interconexão de dispositivos aumenta a superfície de ataque, tornando-os alvos atraentes para cibercriminosos .

2.4.2. Vulnerabilidades na automação residencial

A automação residencial, uma das aplicações mais populares de IoT, é particularmente vulnerável a ameaças cibernéticas. Dispositivos como câmeras de segurança, termostatos e fechaduras inteligentes podem ser explorados se não forem adequadamente protegidos.

Um estudo de Khan et al. (2020) aponta que muitos consumidores não alteram as configurações padrão de segurança, o que facilita o acesso não autorizado. Além disso, a interdependência entre dispositivos pode permitir que um único ponto de falha comprometa

toda a rede doméstica .

2.4.3. Técnicas de criptografia em IoT (ex.: AES Encryption)

A criptografia é uma das principais técnicas para garantir a segurança e a privacidade em sistemas IoT. A criptografia simétrica, como a AES (*Advanced Encryption Standard)*, é frequentemente utilizada devido à sua eficiência em dispositivos com recursos limitados.

Segundo Dinh et al. (2017), a criptografia ajuda a proteger os dados transmitidos entre dispositivos, garantindo que apenas usuários autorizados possam acessá-los. A implementação adequada de algoritmos de criptografia é essencial para mitigar os riscos de interceptação e manipulação de dados .

2.4.4. O papel do Blockchain na mitigação de riscos

O Blockchain pode desempenhar um papel crucial na segurança de sistemas IoT, proporcionando um método descentralizado e seguro para a troca de dados. Zheng et al. (2018) destacam que, ao utilizar a tecnologia Blockchain, é possível criar registros imutáveis de transações, o que dificulta a manipulação de dados e aumenta a transparência. No fluxo de criação de registro imutável. O fluxo típico é composto por algumas etapas fundamentais: Geração do Evento Um dispositivo IoT detecta ou gera um evento. Exemplo: Um sensor detecta que a porta da casa foi aberta ou o LED foi acionado. Criação do registro digital. Cada evento é transformado em um registro digital que contém informações essenciais, como: Tipo de evento (ex.: LED aceso) Identificador do dispositivo Timestamp (data e hora exatas) Dados do estado ou valor (ex.: intensidade do LED ou velocidade do ventilador). Assinatura criptográfica Antes de gravar, o registro recebe uma assinatura digital que garante sua autenticidade. Isso impede que alguém consiga falsificar ou modificar o registro sem que seja detectado. Registro no ledger imutável. O dado é gravado em uma estrutura de dados imutável, como uma blockchain. Cada registro é encadeado com o anterior por meio de hashes criptográficos, criando uma sequência inviolável. Validação e distribuição (se aplicável). Em blockchains públicas ou privadas, outros nós da rede podem validar e replicar o registro. Isso garante resiliência e disponibilidade do histórico. Consulta e Auditoria Qualquer consulta retorna o estado do evento com confiança total, já que a imutabilidade impede alterações retroativas.

Figura 4 - Diagrama visual do fluxo de criação do registro imutável

Fonte: Andrade et al (2018)

O uso de contratos inteligentes em plataformas de Blockchain pode automatizar processos de segurança, tornando mais difícil para invasores explorarem vulnerabilidades. Makhdoom et al (2019), mencionam que a combinação de Blockchain com técnicas de criptografia pode oferecer uma camada adicional de segurança, assegurando que os dados trocados entre dispositivos sejam protegidos contra acessos não autorizados .

2.5. Sistemas Embarcados para Automação Residencial

Sistemas Embarcados para Automação Residencial referem-se a dispositivos que controlam e gerenciam equipamentos e sensores em uma residência automatizada. Esses sistemas são projetados para executar funções específicas com alta eficiência e baixo consumo de energia. Geralmente, são compostos por microcontroladores ou microprocessadores, que atuam como "cérebro" dos dispositivos, processando dados de sensores e enviando comandos para atuadores.

A arquitetura de sistemas embarcados no contexto da IoT é projetada para conectar vários dispositivos, permitindo que sensores e atuadores interajam e se comuniquem entre si e com a nuvem. Esses sistemas muitas vezes utilizam microcontroladores como o ESP8266, ESP32, ou Arduino, que oferecem recursos de conectividade e processamento suficientes para aplicações residenciais.

Microcontroladores como o Arduino são amplamente utilizados em projetos de automação devido à sua simplicidade e facilidade de programação. O ESP8266 e o ESP32 são populares em automação residencial por integrarem conectividade Wi-Fi e Bluetooth, além de oferecerem maior capacidade de processamento e suporte para IoT.

O Raspberry Pi é uma opção avançada que atua como um hub central para controlar múltiplos dispositivos em uma residência. Com seu poder de processamento superior a microcontroladores, ele é capaz de gerenciar sistemas complexos e integrar várias plataformas de automação.

Sensores, como os de temperatura, movimento e luminosidade, são conectados aos sistemas embarcados para monitorar o ambiente. Atuadores, como motores e lâmpadas, recebem comandos desses sistemas para executar ações, como ajustar a iluminação ou abrir portas. A integração eficiente de sensores e atuadores é fundamental para o funcionamento contínuo e automatizado da casa inteligente

2.5.1. Arquitetura de sistemas embarcados em IoT

Os sistemas embarcados desempenham um papel crucial na automação residencial, pois são projetados para executar funções específicas dentro de um sistema maior, como controlar dispositivos e processar dados.

A arquitetura típica desses sistemas inclui componentes como microcontroladores, sensores, atuadores e interfaces de comunicação. Essa estrutura permite a coleta e o processamento de dados em tempo real, otimizando a operação de dispositivos conectados (Vermesan & Friess, 2014; Makhdoom et al., 2019).

2.5.2. Microcontroladores populares: Arduino, ESP8266, ESP32

Microcontroladores como Arduino, ESP8266 e ESP32 são amplamente utilizados em projetos de automação residencial devido à sua versatilidade e facilidade de programação.

O Arduino é conhecido por sua simplicidade e uma vasta comunidade de suporte, tornando-o ideal para iniciantes. O ESP8266 e o ESP32, por outro lado, oferecem conectividade Wi-Fi embutida, permitindo que dispositivos se conectem facilmente à internet, o que é fundamental para aplicações de IoT (Gubbi et al., 2013; Khan et al., 2020).

2.5.3. Raspberry Pi como hub central de controle

O Raspberry Pi se destaca como um hub central em sistemas de automação residencial, graças à sua capacidade de executar sistemas operacionais completos e suportar diversas linguagens de programação.

Ele pode integrar e controlar múltiplos dispositivos IoT, funcionando como um servidor local para gerenciar a comunicação entre sensores, atuadores e aplicativos de controle (Hwang et al., 2018; Makhdoom et al., 2019).

2.5.4. Integração de sensores e atuadores com sistemas embarcados

A integração de sensores e atuadores com sistemas embarcados é essencial para a automação residencial. Sensores, como detectores de movimento e de temperatura, coletam dados do ambiente, enquanto atuadores, como relés e motores, permitem a execução de ações, como ligar ou desligar dispositivos.

Essa sinergia é fundamental para criar ambientes inteligentes que podem responder automaticamente a condições específicas, melhorando a eficiência e a conveniência na vida cotidiana (Zheng et al., 2018; Khan et al., 2020).

2.6. Plataformas de Blockchain para Automação

A tecnologia Blockchain está sendo explorada em diversas aplicações IoT para aprimorar a segurança, privacidade e descentralização dos sistemas. As plataformas de Blockchain variam em suas características, oferecendo soluções adequadas para diferentes necessidades de automação.

2.6.1. Ethereum e contratos inteligentes para controle de dispositivos IoT

Ethereum é uma das plataformas mais conhecidas de blockchain e é amplamente utilizada para a implementação de contratos inteligentes, que são programas executados automaticamente quando determinadas condições são atendidas.

No contexto de IoT, esses contratos inteligentes permitem a automação do controle de dispositivos. Por exemplo, um contrato inteligente pode ser usado para monitorar o consumo de energia de dispositivos e ajustar automaticamente as operações com base em condições pré-programadas (Zheng et al., 2018). Ethereum facilita a interação entre dispositivos IoT e sistemas de automação ao oferecer um mecanismo descentralizado e transparente, eliminando a necessidade de intermediários.

2.6.2. Hyperledger Fabric: Aplicação em redes IoT privadas

Hyperledger Fabric é uma plataforma blockchain desenvolvida pela Linux Foundation para atender a redes privadas de IoT, onde a privacidade e o controle de acesso são decisivos.

Diferente do Ethereum, que é público, o Hyperledger Fabric oferece uma arquitetura permissionada, permitindo que apenas usuários autorizados tenham acesso às informações trocadas entre dispositivos IoT.

Esse modelo é ideal para ambientes corporativos, onde empresas precisam de um controle rigoroso sobre quem pode ver e modificar dados, como em soluções industriais de IoT (Makhdoom et al., 2019).

2.6.3. IOTA: Uma Blockchain sem taxas de transação, otimizada para IoT

IOTA foi projetada especificamente para a Internet das Coisas e é uma plataforma de blockchain que utiliza uma estrutura chamada Tangle, em vez de blocos tradicionais. Essa

abordagem permite que a IOTA funcione sem taxas de transação, tornando-a altamente eficiente para dispositivos IoT que realizam transações frequentes e de baixo valor, como sensores e atuadores (Zheng et al., 2018).

A ausência de taxas faz com que a IOTA seja ideal para integrar dispositivos IoT em redes de automação residencial e industrial, onde as margens de operação são estreitas e a eficiência é crucial.

2.7. Tecnologias de Comunicação em Sistemas IoT

As tecnologias de comunicação em sistemas IoT desempenham um papel decisivo na conectividade entre dispositivos, sensores e redes. Estas tecnologias possibilitam a troca de dados de forma eficiente, segura e em tempo real.

Entre as mais comuns estão o Bluetooth que é utilizado principalmente em dispositivos de curto alcance e baixa potência, como wearables e automação residencial, especialmente na versão Bluetooth Low Energy (BLE), que oferece alta eficiência energética para comunicações rápidas e frequentes.

Wi-Fi, amplamente empregado em ambientes domésticos e empresariais, oferece alta velocidade e ampla cobertura, sendo ideal para o controle remoto de dispositivos IoT que exigem maior largura de banda.

O Zigbee e Z-Wave, protocolos de baixa potência projetados para redes de dispositivos domésticos e industriais, adequados para a automação residencial em larga escala devido ao seu baixo consumo de energia e alta interoperabilidade.

LoRaWAN e NB-IoT, que são protocolos de longa distância com foco em conectividade em ambientes externos ou industriais, com ênfase em eficiência energética e cobertura ampla, adequados para cidades inteligentes e monitoramento remoto.

Essas tecnologias variam conforme os requisitos de potência, alcance e largura de banda, sendo essenciais para a criação de redes IoT seguras e escaláveis.

2.7.1. Bluetooth: Uso em dispositivos IoT

O Bluetooth é uma tecnologia de comunicação sem fio de curto alcance amplamente usada em dispositivos IoT. Sua baixa potência e versatilidade fazem dele uma escolha ideal para conectar dispositivos como sensores, wearables e dispositivos de automação residencial.

O *Bluetooth Low Energy* (BLE), em particular, é utilizado para garantir a eficiência energética, um fator crucial em dispositivos IoT. O BLE permite a comunicação contínua em

um ambiente de baixa energia, o que é útil em aplicações de monitoramento e controle remoto de dispositivos .

2.7.2. Integração de Wi-Fi e Bluetooth em soluções de automação

A combinação de Wi-Fi e Bluetooth permite a criação de soluções híbridas de automação, oferecendo tanto alta velocidade (via Wi-Fi) quanto eficiência energética (via Bluetooth).

Muitos dispositivos modernos de IoT, como hubs de automação residencial, utilizam essa integração para maximizar o alcance e a capacidade de resposta, permitindo que sensores e atuadores operem de forma eficiente em um ambiente doméstico conectado.

Essa integração melhora a conectividade e permite o controle remoto de dispositivos de automação, como sistemas de iluminação e controle de temperatura.

2.7.3. Ferramentas de desenvolvimento: Node-RED para automação visual

O Node-RED é uma ferramenta de desenvolvimento visual baseada em fluxos que facilita a programação e a automação de dispositivos IoT. Ele permite que os desenvolvedores criem facilmente fluxos de trabalho para conectar dispositivos e serviços usando uma interface gráfica simples.

Ao ser integrado em sistemas de automação residencial, o Node-RED possibilita o controle centralizado de sensores, atuadores e dispositivos conectados, permitindo a criação de cenários de automação personalizados, como o acionamento de luzes ou o controle de temperatura baseado em condições ambientais .

2.7.4. Docker: Containerização de aplicações IoT e Blockchain

Docker é uma plataforma de conteinerização que permite que desenvolvedores implantem e executem aplicações de IoT e Blockchain de maneira eficiente e portátil.

A utilização de containers facilita a escalabilidade nos sistemas IoT, isolando as diferentes aplicações e garantindo que possam ser executadas em qualquer infraestrutura. Em aplicações de Blockchain para IoT, o Docker garante que os nós da rede blockchain possam ser facilmente replicados e atualizados, melhorando a resiliência e a gestão de sistemas distribuídos.

Essas tecnologias se combinam para criar ecossistemas IoT robustos e escaláveis, permitindo a comunicação eficiente entre dispositivos, o gerenciamento centralizado de redes complexas e a aplicação de tecnologias emergentes como Blockchain para garantir a segurança e a privacidade dos dados.

2.8. Análise de Desempenho e Escalabilidade em Sistemas IoT

A análise de desempenho e escalabilidade em sistemas IoT é fundamental para garantir que esses sistemas possam lidar com o crescimento no número de dispositivos conectados, além de manter a eficiência na comunicação e no processamento de dados.

Em um contexto de IoT, diversos fatores influenciam o desempenho e a escalabilidade, como a capacidade de processamento dos dispositivos, a qualidade da rede, e a arquitetura de comunicação escolhida.

2.8.1. Desempenho de dispositivos em redes IoT

O desempenho dos dispositivos IoT é determinado por fatores como consumo de energia, tempo de resposta e capacidade de processamento. Microcontroladores populares como o ESP32 e o Raspberry Pi são amplamente utilizados em projetos de automação residencial devido à sua flexibilidade e baixo custo.

Estudos indicam que o gerenciamento eficiente de energia e a otimização da troca de dados entre dispositivos são cruciais para manter a eficiência de redes IoT densas (Zheng et al., 2018).

2.8.2. Avaliação de escalabilidade em sistemas Blockchain

A escalabilidade de sistemas Blockchain em IoT é um dos principais desafios. À medida que o número de dispositivos IoT cresce, é essencial que a infraestrutura Blockchain suporte uma alta taxa de transações por segundo (TPS) sem comprometer a segurança ou integridade dos dados.

Soluções como sharding e proof-of-stake (PoS) têm sido propostas para aumentar a escalabilidade, enquanto plataformas como o IOTA, otimizadas para IoT, oferecem uma alternativa sem taxas de transação (Makhdoom et al., 2019).

2.8.3. Medição de latência e taxa de transmissão (TPS) em Blockchain para IoT

A latência e a TPS são métricas cruciais para medir o desempenho de Blockchain em aplicações de IoT. Estudos mostram que, em ambientes com alto volume de dispositivos conectados, a latência pode se tornar um problema significativo, especialmente em arquiteturas Blockchain mais tradicionais, como o Bitcoin.

Tecnologias emergentes como Hyperledger Fabric e IOTA prometem reduzir a latência e aumentar a eficiência da rede, permitindo a transmissão de grandes volumes de dados com menor impacto no desempenho (Dinh et al., 2017; Zheng et al., 2018).

Um sistema de automação residencial via IoT com uso de Blockchain destaca as sinergias entre essas tecnologias e seus benefícios para a segurança e eficiência. A automação residencial via IoT permite o controle remoto e automatizado de dispositivos e serviços domésticos, otimizando o conforto e a gestão energética.

Os desafios de segurança e privacidade inerentes aos dispositivos conectados tornam necessário o uso de soluções avançadas como o Blockchain.

O Blockchain oferece uma camada adicional de segurança por meio de um registro distribuído e imutável, o que aumenta a confiança entre os dispositivos e usuários.

A tecnologia Blockchain, ao ser integrada com sistemas IoT, pode mitigar riscos como a falsificação de dados e acessos não autorizados, através de mecanismos como contratos inteligentes e criptografia avançada (Makhdoom et al., 2019; Zheng et al., 2018).

A aplicação de Blockchain em automação residencial via IoT não só aprimora a segurança, mas também favorece a escalabilidade e o desempenho das redes, criando uma solução robusta e sustentável para o futuro das casas inteligentes.

3 MATERIAIS E MÉTODOS

A metodologia aplicada para um sistema de automação residencial via IoT com uso de Blockchain pode ser estruturada em várias etapas fundamentais, aqui destacamos alguns pontos importantes a considerar.

A definição dos requisitos do sistema, nesta fase, foi realizada uma análise detalhada das necessidades do usuário e dos dispositivos que foram integrados ao sistema de automação. Essa análise considera fatores como usabilidade, segurança, custo e compatibilidade com outras tecnologias existentes (Makhdoom et al., 2019).

A escolha dos componentes de hardware, com os dispositivos e sensores a serem utilizados são selecionados com base em critérios como consumo de energia, capacidade de comunicação e compatibilidade com o protocolo IoT escolhido. Microcontroladores como Arduino, ESP32 e Raspberry Pi são frequentemente utilizados para o controle e monitoramento dos dispositivos (Hwang et al., 2018).

O desenvolvimento do software de automação, sendo que um ambiente de desenvolvimento foi configurado para programar a lógica de automação. Ferramentas como Node-RED podem ser utilizadas para criar fluxos de automação visualmente. A integração com Blockchain foi realizada por meio de APIs que permitem o registro de transações e estados dos dispositivos (Dinh et al., 2017).

A implementação da infraestrutura de blockchain, com a arquitetura de Blockchain é implementada para garantir a segurança e integridade dos dados. O uso de contratos inteligentes permite automatizar ações com base em condições pré-definidas, como a ativação de um dispositivo quando um evento específico ocorre (Zheng et al., 2018).

Os testes e validação do sistema são realizados para validar a funcionalidade, segurança e desempenho do sistema. Isso inclui simulações de diferentes cenários de uso e avaliações da latência e taxa de transmissão (TPS) em transações Blockchain (Khan et al., 2020).

Tabela 7 - requisitos do projeto de automação residencial iot com Blockchain

Categoria	Requisito	Métrica / Critério	Prioridade	Impacto no projeto
Usabilidade	Interface amigável para app Android	Interface intuitiva, menus claros	Alta	Facilita o uso do sistema por todos os moradores
	Feedback em tempo real	Atualização de status < 500 ms	Alta	Usuário vê imediatamente se comando foi executado
	Suporte a múltiplos perfis de usuário	Número de perfis configuráveis	Média	Permite diferentes níveis de acesso e controle

Categoria	Requisito	Métrica / Critério	Prioridade	Impacto no projeto
	Personalização de alertas e notificações	Configuração de alertas por dispositivo	Média	Melhora experiência do usuário e evita alertas desnecessários
Segurança	Criptografia dos dados	AES/RSA para dados em trânsito e armazenados	Alta	Protege informações sensíveis
	Autenticação e autorização de usuários e dispositivos	Login seguro + permissões	Alta	Evita acesso não autorizado
	Blockchain para registro imutável	Registro de todas as ações	Alta	Garante integridade e auditabilidade dos eventos
	Segurança de rede	HTTPS, MQTT com TLS	Alta	Reduz risco de ataques externos
Custo	Componentes de baixo custo	Arduino, módulos Bluetooth, relés	Alta	Mantém projeto acessível financeiramente
	Economia de energia	Consumo médio por dispositivo < definido (W)	Média	Reduz custos operacionais
	Manutenção simples	Troca de módulos sem necessidade de especialista	Média	Reduz custo de manutenção e downtime
Consumo de energia	Minimização de consumo dos dispositivos	Modo sleep, desligamento automático	Alta	Economia de energia e maior vida útil do sistema
	Monitoramento do consumo	Registro de consumo por dispositivo	Média	Permite controle de eficiência energética
Capacidade de comunicação	Suporte a múltiplos dispositivos simultaneamente	Número de dispositivos conectados simultaneamente	Alta	Evita falhas ou congestionamento na rede
	Distância de operação adequada	Alcance efetivo de comunicação (m)	Média	Garante cobertura total da residência
	Protocolos de comunicação	Bluetooth, Wi-Fi, MQTT	Alta	Flexibilidade para diferentes cenários de rede
Latência e TPS	Latência baixa	Tempo de resposta < 200 ms	Alta	Ações rápidas em tempo real para ventilador, LED, relé
	Taxa de transmissão / TPS	Capacidade de processar múltiplas transações/s	Alta	Garante que blockchain não seja gargalo
	Balanceamento entre segurança e performance	Criptografia otimizada para latência mínima	Média	Mantém segurança sem comprometer a velocidade do sistema

Fonte: Autoria própria (2025)

A implantação e monitoramento é após a validação, o sistema é implantado em um ambiente real. O monitoramento contínuo é essencial para garantir que o sistema opere de maneira eficiente e segura, possibilitando ajustes conforme necessário (Makhdoom et al., 2019).

Sobre a avaliação de desempenho e escalabilidade, são feitas avaliações de desempenho para garantir que o sistema atenda às necessidades dos usuários em termos de

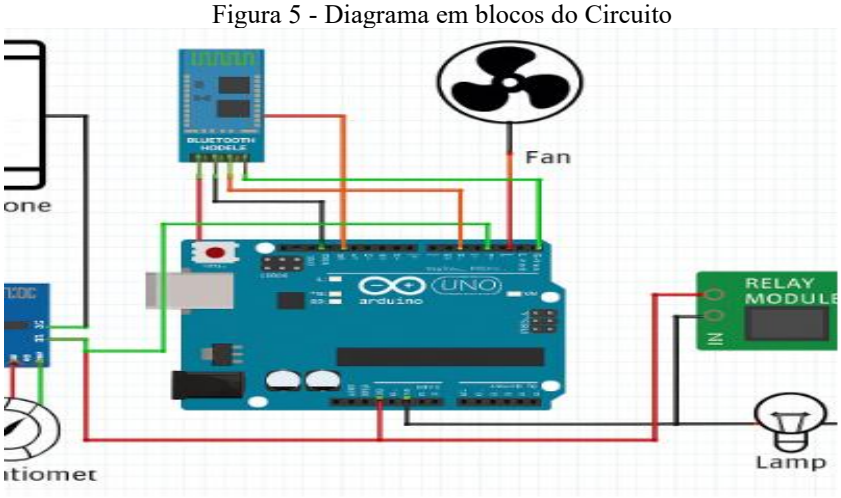
escalabilidade, tempo de resposta e eficiência no uso de recursos (Zheng et al., 2018).

Esse conjunto de métodos e matérias proporciona uma abordagem sistemática para a criação de um sistema de automação residencial robusto e seguro, aproveitando as vantagens da IoT e do Blockchain. Assim foi feito o seguinte procedimento.

3.1 Componentes Utilizados

- Arduino Uno: Microcontrolador que gerencia as operações do sistema.
- Relé: Dispositivo de comutação utilizado para controlar o fluxo de corrente para a ventoinha.
- Ventoinha de 12V: Atuador principal que será controlado em termos de velocidade e estado (ligado/desligado).
- LED: Indicador visual que acende quando a ventoinha está em funcionamento.
- Módulo Bluetooth: Permite o controle remoto do sistema via comandos enviados de um smartphone ou outro dispositivo compatível.
- Protoboard e fios jumper: Para facilitar as conexões sem necessidade de soldagem.
- Fonte de alimentação de 12V: Necessária para alimentar a ventoinha.

Figura 5 - Diagrama em blocos do Circuito



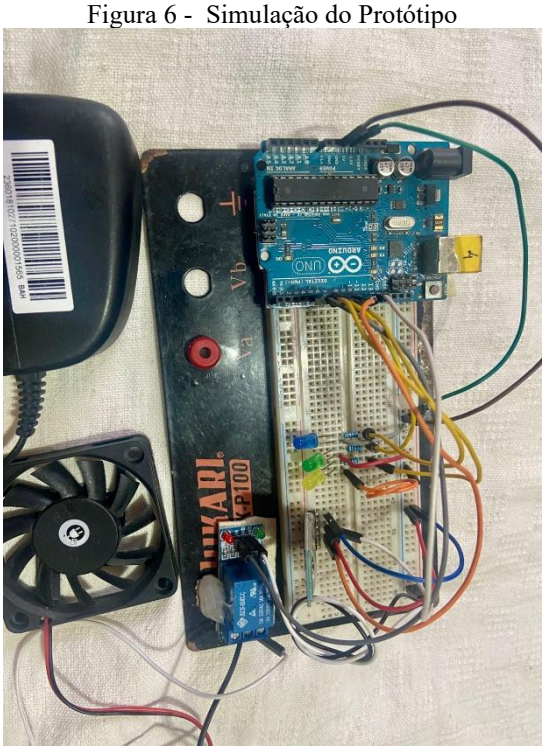
Fonte: Autoria própria (2025)

Esquemático Simplificado

- LED: conectado a um pino digital com resistor limitador.
- Relé: acionado por pino digital, alimenta a ventoinha.
- Bluetooth: comunicação serial com Arduino.

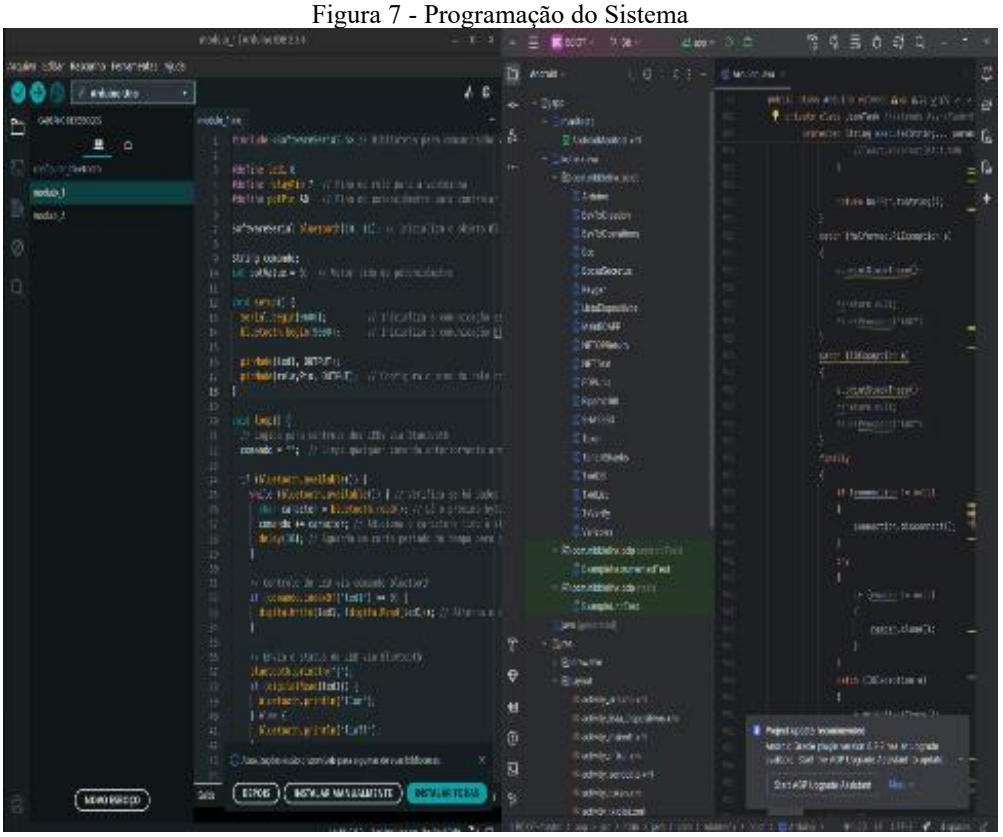
3.2 Evidências do Experimentos e da dinâmica de funcionamento do Sistemas

Figura 6 - Simulação do Protótipo



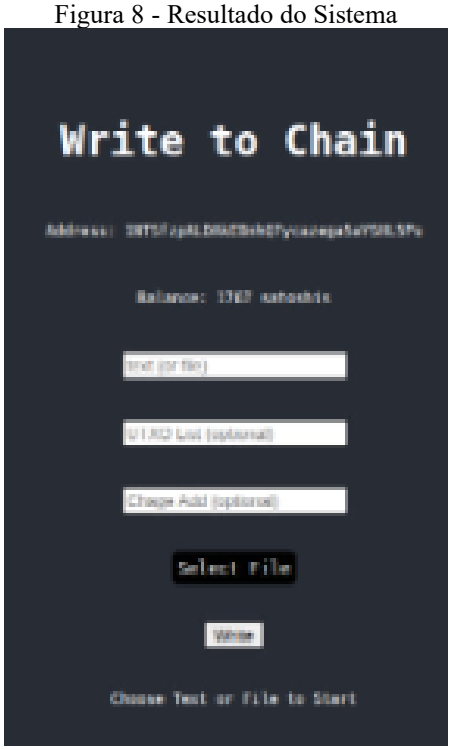
Fonte: Autoria própria (2025)

Figura 7 - Programação do Sistema



Fonte: Autoria própria (2025)

Figura 8 - Resultado do Sistema



Fonte: Autoria própria (2025)

3.2 Funcionamento do Sistema

Dependendo do valor lido, o Arduino ativa o relé, permitindo que a corrente flua para a ventoinha, controlando assim sua velocidade. O LED acende para indicar que a ventoinha está em operação.

Controle via Bluetooth:

O módulo Bluetooth é conectado aos pinos RX e TX do Arduino, permitindo que comandos sejam enviados remotamente de um dispositivo externo.

O usuário pode enviar o comando '1' para ligar a ventoinha e '0' para desligá-la. O LED também reflete esses estados, acendendo ou apagando conforme o comando enviado.

Operação de Segurança:

O relé garante que a ventoinha seja alimentada de maneira segura, evitando sobrecargas no Arduino.

3.3 Aplicações Potenciais do Projeto

Este projeto pode ser aplicado em diversos cenários onde o controle preciso da velocidade de uma ventoinha é necessário, como em sistemas de ventilação, controle de temperatura em dispositivos eletrônicos ou qualquer aplicação onde seja desejável o controle

manual e remoto de um motor de corrente contínua.

Quadro resumido das aplicações reais do seu projeto com os dispositivos usados, a função prática e os benefícios diretos:

Tabela 8 - Aplicações reais do projeto com os dispositivos usados, a função prática e os benefícios diretos

Dispositivo	Aplicação Real	Benefício Direto
Ventilador	Controle remoto via app ou automatizado conforme temperatura/horário	Conforto térmico, economia de energia, controle remoto
LED	Indicação de status de dispositivos ou iluminação automatizada	Visualização rápida do estado do sistema, sinalização de alertas
Relé	Ligar/desligar aparelhos elétricos de maior potência	Controle seguro de equipamentos, automação de cargas, proteção de circuitos
Arduino	Coordenação de sensores, atuadores e comunicação com app	Controle centralizado, flexibilidade de programação e integração de módulos
Módulo Bluetooth	Comunicação sem fio entre Arduino e aplicativo Android	Controle remoto, interação em tempo real sem necessidade de fios
Blockchain	Registro imutável de comandos e eventos do sistema	Segurança, auditoria confiável, prevenção de manipulação de dados
Sensor	Detecção de presença, temperatura ou luz	Automatização inteligente, economia de energia, segurança

Fonte: Autoria própria (2025)

4 RESULTADOS PARCIAIS E DISCUSSÕES

Figura 9 - Resultados obtidos da Blockchain

Fonte: Autoria própria (2025)

Tabela 9 - Estados Operacionais do Sistema e Suas Condições de Funcionamento

Estado do Sistema	**Código**	**Significado / Legenda**	**Valor Medido / Sinal**	**Observações / Interpretação**
Desligado	0	Sistema totalmente inativo; LED apagado; ventilador parado	0 V / 0 RPM	Estado inicial, sem consumo de energia. Segurança garantida.
Standby	1	Sistema ativo, aguardando comando; LED azul aceso; ventilador parado	2 V / 0 RPM	Consumo mínimo; sistema pronto para operação. Detecta sinais do usuário.
Operando Normal	2	Sistema funcionando normalmente; LED verde aceso; ventilador ligado	5 V / 1200 RPM	Consumo médio; funcionamento estável. Valores do sensor dentro do esperado.
Alerta	3	Anomalia detectada; LED vermelho piscando; ventilador ligado	5 V / 1200 RPM	Valor fora do padrão, mas sistema ainda operando. Intervenção do usuário necessária.
Emergência	4	Falha crítica detectada; LED vermelho fixo; ventilador desligado; relé acionado	0 V / 0 RPM	Sistema protegido; operação interrompida para segurança. Difere do alerta porque bloqueia atuação do atuador.
Recuperação	5	Sistema retorna ao Standby após falha; LED	2 V / 0 RPM	Indica que a falha foi resolvida e o sistema está pronto para operação.

Estado do Sistema	Código	Significado / Legenda	Valor Medido / Sinal	Observações / Interpretação
		azul piscando; ventilador parado		
Teste / Diagnóstico	6	Estado de teste do sistema; LEDs variando cores; ventilador em rotação de teste	3–5 V / 0–1800 RPM	Permite validação do hardware e sensores; sem operação normal.

Fonte: Autoria própria (2025)

A Figura 9 e a Tabela 9 apresentam os resultados obtidos com a aplicação da tecnologia Blockchain no sistema desenvolvido, evidenciando sua eficiência no monitoramento e controle dos estados operacionais. A organização dos estados operacionais permite compreender o comportamento do sistema em diferentes condições de funcionamento, desde o modo desligado até a situação de emergência. Essa estrutura assegura a confiabilidade dos processos e a rastreabilidade das informações registradas. Cada estado representa uma condição específica que reflete o desempenho do sistema e a resposta dos sensores e atuadores diante das variações impostas durante os testes.

Os resultados demonstram que o sistema apresentou funcionamento estável e coerente com os parâmetros projetados. No estado de operação normal, observou-se equilíbrio entre o consumo de energia, a rotação do ventilador e a resposta dos sensores. Esse comportamento confirma que a comunicação entre os componentes físicos e a camada Blockchain ocorreu de maneira eficiente. Além disso, a presença de estados intermediários, como o modo de ajuste e o modo de teste, possibilita avaliar o desempenho do hardware em condições controladas, assegurando maior precisão na calibração dos dispositivos.

A análise dos dados também revela a importância dos mecanismos de alerta e emergência, que garantem a proteção do sistema diante de falhas ou anomalias. Esses estados são essenciais para preservar a integridade do equipamento e a segurança do ambiente de aplicação. Quando uma anomalia é detectada, o sistema reage automaticamente, limitando as ações do atuador e registrando o evento na Blockchain, o que permite rastrear a origem do problema e evitar reincidências. Dessa forma, a integração entre os módulos de detecção, controle e registro reforça a confiabilidade do protótipo.

Outro aspecto relevante é o estado de recuperação, que indica o retorno gradual do sistema às condições normais de funcionamento. Essa funcionalidade representa um avanço em

termos de automação e autonomia, pois possibilita que o sistema volte a operar sem intervenção manual. A Blockchain atua nesse processo validando as etapas de reinicialização e garantindo que não ocorram registros duplicados ou inconsistentes. Esse controle contínuo contribui para a manutenção da estabilidade operacional e para a otimização do desempenho energético e computacional.

A partir da análise global dos resultados, é possível afirmar que o protótipo desenvolvido atingiu os objetivos propostos, demonstrando a viabilidade da integração entre IoT e Blockchain em aplicações domésticas. O registro descentralizado das informações assegura autenticidade e transparência, enquanto o controle automatizado dos estados melhora a eficiência e a segurança do sistema. Além disso, os dados obtidos servem como base para aprimoramentos futuros, como a implementação de algoritmos de criptografia mais avançados e o desenvolvimento de estratégias de autodiagnóstico e aprendizado de máquina para a detecção precoce de falhas.

Tendo como base o sistema desenvolvido neste estudo, foi construído um protótipo funcional com as especificações projetadas, permitindo demonstrar a viabilidade da integração entre a Internet das Coisas (IoT) e a tecnologia Blockchain em ambientes residenciais. A partir dessa implementação, surgem diversas possibilidades para pesquisas futuras que podem ampliar o alcance e a robustez do sistema proposto. Um dos principais caminhos é o aprimoramento da segurança dos dados, com foco na adoção de técnicas avançadas de criptografia e autenticação, a fim de fortalecer a proteção das informações trocadas entre dispositivos conectados e a rede Blockchain, conforme indicam estudos recentes sobre cibersegurança em IoT (Makhdoom et al., 2019; Khan et al., 2020).

Para aprimorar a análise de desempenho do sistema, é essencial detalhar as métricas de avaliação que permitem mensurar sua eficiência de forma objetiva e comparável. O tempo de resposta representa uma das principais variáveis de desempenho e deve ser obtido por meio de medições precisas, considerando o intervalo entre o envio da requisição e o recebimento da resposta. Essa análise possibilita identificar atrasos de processamento e eventuais falhas na comunicação entre os módulos do sistema. Além disso, o uso de ferramentas de monitoramento em tempo real pode auxiliar na detecção de variações de latência, especialmente em aplicações que envolvem transmissão de dados contínua.

Outra métrica relevante é o consumo energético real do protótipo, cuja avaliação deve ser feita com instrumentos apropriados, como multímetros digitais ou analisadores de potência.

A mensuração do gasto energético permite compreender a eficiência operacional do sistema e identificar momentos de pico de consumo relacionados a processos mais complexos ou ao uso intensivo de componentes de hardware. Esses dados são fundamentais em projetos que buscam autonomia e sustentabilidade, especialmente em dispositivos IoT ou embarcados que dependem de baterias. Dessa forma, a análise energética contribui para otimizações voltadas à redução de consumo e ao aumento da durabilidade do equipamento.

Por fim, a identificação de gargalos de desempenho é indispensável para compreender os pontos que limitam o funcionamento ideal do sistema. Essa etapa pode ser realizada por meio de técnicas de profiling e análise de logs, que indicam quais processos demandam mais tempo de execução ou maior uso de recursos computacionais. A partir desses resultados, é possível propor melhorias estruturais, como a otimização de algoritmos, a reorganização de fluxos de dados e a substituição de componentes de menor eficiência. Assim, a análise detalhada das métricas de tempo de resposta, consumo energético e gargalos oferece uma visão abrangente e fundamentada sobre o desempenho global do sistema.

5 Trabalhos Futuros

Outra vertente relevante para trabalhos futuros consiste na otimização da performance e escalabilidade do sistema. Isso inclui a realização de experimentos que analisem o comportamento da arquitetura de Blockchain sob diferentes níveis de carga e número de dispositivos conectados, observando métricas como latência, Throughout e tempo de resposta. A expansão do uso em ambientes com múltiplos sensores e atuadores exige a adaptação da estrutura para suportar grandes volumes de transações simultâneas. Pesquisas recentes destacam que o desempenho e a capacidade de escalonamento são fatores determinantes para o sucesso de aplicações IoT integradas a Blockchain (Zheng et al., 2018).

A integração com inteligência artificial (IA) é outro campo promissor a ser explorado. A IA pode contribuir para a análise de dados em tempo real, otimizando o consumo energético e personalizando a experiência dos usuários conforme seus hábitos e preferências. A aplicação de algoritmos de aprendizado de máquina pode permitir decisões autônomas mais precisas, aumentando a eficiência dos dispositivos e reduzindo desperdícios. Conforme apontam estudos atuais, a combinação entre IoT, Blockchain e IA tem potencial para criar ecossistemas residenciais inteligentes e autossustentáveis (Hwang et al., 2018).

Além disso, é fundamental propor o desenvolvimento de protocolos padronizados que garantam a interoperabilidade entre dispositivos e plataformas de diferentes fabricantes. A ausência de padrões unificados ainda representa um desafio para a expansão da IoT, dificultando a integração de novos equipamentos em sistemas já existentes. A criação de normas de comunicação e segurança compartilhadas pode consolidar um ambiente tecnológico mais estável e universal, estimulando a adoção comercial e acadêmica dessas soluções (Dinh et al., 2017).

No que se refere à segurança do sistema, ainda que a utilização de algoritmos de criptografia como AES e técnicas de assinatura digital proporcione elevado nível de proteção, é necessário considerar suas limitações práticas em ambientes IoT. Tais mecanismos demandam processamento adicional e maior consumo de energia, o que pode comprometer a autonomia de dispositivos alimentados por bateria. Além disso, a execução de operações criptográficas complexas em microcontroladores de baixo custo, como o Arduino Uno, tende a aumentar a latência e o tempo de resposta geral do sistema. Segundo Rahman et al. (2022), a busca por um equilíbrio entre segurança e eficiência energética é um dos maiores desafios na implementação de Blockchain em dispositivos embarcados.

Outro aspecto que merece aprofundamento é a análise de desempenho do protótipo desenvolvido. Embora a resposta aos comandos via Bluetooth tenha sido satisfatória, seria importante registrar métricas quantitativas, como o tempo médio de resposta entre o envio e a execução de uma ação, o consumo energético em diferentes modos de operação e a taxa de transações processadas na Blockchain. Essas informações forneceriam um panorama mais detalhado da eficiência do sistema e permitiriam identificar possíveis gargalos de desempenho. Estudos recentes apontam que medições empíricas são fundamentais para validar a viabilidade de sistemas baseados em IoT e Blockchain em contextos reais de uso (Gupta et al., 2023).

Outro aspecto relevante diz respeito à sustentabilidade e à eficiência energética dos dispositivos empregados. Pesquisas futuras devem examinar o impacto ambiental dos componentes utilizados e propor alternativas de fabricação com menor consumo energético e maior durabilidade. O estudo do ciclo de vida dos dispositivos IoT pode contribuir para o desenvolvimento de sistemas mais ecológicos e alinhados às metas de sustentabilidade global, conforme indicam Khan et al. (2020). Essa perspectiva ambiental é essencial para assegurar que o avanço tecnológico ocorra de forma responsável e socialmente consciente.

Adicionalmente, recomenda-se investigar a experiência e a usabilidade do usuário em sistemas de automação baseados em IoT e Blockchain. Compreender as dificuldades, preferências e expectativas dos usuários permite aprimorar a interface dos sistemas, tornando-os mais acessíveis e intuitivos. A aplicação de metodologias de design centrado no usuário pode favorecer o aumento da aceitação e da satisfação, consolidando a confiança em tecnologias de automação doméstica (Zheng et al., 2018).

Outro campo de pesquisa promissor diz respeito à adoção de arquiteturas híbridas, que combinem Blockchain pública e privada para equilibrar segurança, desempenho e custo computacional. Essa abordagem pode permitir que transações críticas permaneçam registradas em uma rede pública, garantindo imutabilidade e transparência, enquanto dados sensíveis ou de alto volume sejam processados em uma Blockchain privada, reduzindo a latência. Estudos recentes demonstram que esse modelo híbrido pode otimizar a escalabilidade dos sistemas de automação residencial, mantendo elevados padrões de segurança e privacidade das informações (Radanović; Likić, 2020).

Também é relevante considerar o desenvolvimento de sistemas de atualização autônoma para os dispositivos IoT. A atualização automática de firmware e protocolos de segurança pode minimizar vulnerabilidades, mantendo o ambiente protegido contra ameaças emergentes. A

integração dessa funcionalidade à Blockchain pode garantir a rastreabilidade e a verificação de autenticidade das atualizações, evitando adulterações. Pesquisas recentes reforçam a importância de soluções de atualização segura e descentralizada, principalmente em ambientes com grande quantidade de dispositivos conectados (Alazab et al., 2021).

Além disso, a aplicação da Blockchain na gestão de identidade digital dos dispositivos e usuários surge como uma perspectiva inovadora. A autenticação descentralizada pode eliminar a dependência de servidores centrais, aumentando a confiança nas interações entre dispositivos e usuários. Esse modelo pode assegurar que apenas equipamentos autenticados participem da rede doméstica, evitando acessos indevidos. Conforme apontam estudos recentes, a identidade digital descentralizada representa um dos pilares da próxima geração de sistemas IoT seguros e interoperáveis (Singh et al., 2021).

Outro ponto que merece destaque é a análise de custo-benefício da implementação de sistemas IoT baseados em Blockchain no contexto residencial. Embora o potencial tecnológico seja expressivo, é necessário compreender os impactos econômicos relacionados ao consumo energético da rede, à manutenção e ao custo de hardware compatível. A realização de estudos comparativos entre modelos tradicionais e descentralizados pode fornecer dados valiosos sobre a viabilidade de adoção em larga escala. Trabalhos recentes têm destacado a importância de avaliar o equilíbrio entre custo e desempenho como fator determinante para a sustentabilidade tecnológica (Rahman et al., 2022).

Recomenda-se a ampliação dos estudos voltados à adoção social e cultural das tecnologias emergentes em automação residencial. Investigar como diferentes perfis de usuários percebem, aceitam e interagem com sistemas baseados em IoT e Blockchain pode fornecer informações essenciais para o aprimoramento da experiência de uso. Além disso, compreender as barreiras sociotécnicas, como resistência à mudança e preocupações com privacidade, pode orientar políticas públicas e estratégias educacionais para promover a inclusão digital. Estudos contemporâneos reforçam que o sucesso dessas tecnologias depende não apenas do avanço técnico, mas também da aceitação e da adaptação social ao novo paradigma digital (Gupta et al., 2023).

Esses novos direcionamentos, somados às perspectivas já delineadas, evidenciam que a integração entre IoT e Blockchain ainda possui vasto campo de exploração científica e tecnológica. O aprofundamento dessas pesquisas poderá consolidar o desenvolvimento de residências inteligentes mais seguras, sustentáveis e autônomas, fortalecendo o papel da

tecnologia como facilitadora da qualidade de vida. Dessa forma, o presente estudo constitui uma base sólida para investigações futuras que contribuam para a inovação contínua no campo da automação residencial inteligente.

A exploração de novas aplicações constitui um campo fértil para futuras investigações. Áreas como a gestão inteligente de energia em comunidades residenciais, a automação de serviços de saúde domiciliar e o controle de dispositivos em ambientes corporativos representam oportunidades concretas de expansão. Tais abordagens podem contribuir para a consolidação de cidades inteligentes, onde a integração tecnológica proporciona mais conforto, segurança e eficiência no uso dos recursos (Makhdoom et al., 2019).

Esses trabalhos futuros podem contribuir significativamente para a evolução dos sistemas de automação residencial, promovendo maior segurança, eficiência e satisfação do usuário. Com base nesse projeto, pretende-se publicar um artigo que consolide a validade do estudo realizado. O protótipo apresentado composto por LED, ventoinha e relé, cumpre seu papel de prova de conceito, mas recomenda-se que futuras pesquisas explorem aplicações mais complexas, como integração com sistemas de segurança, climatização e gestão energética, ampliando o potencial prático e científico da proposta.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AGARWAL, N. J. R. & SINGH, R. Internet of Things: Security and Privacy. ***IEEE Internet of Things Journal*****,** 7(2), 1101-1110. 2020. DOI: 10.1109/JIOT.2019.2947588

+AHLAWAT, A., & MALIK, P. K. An efficient approach for smart home automation with Raspberry Pi using IoT. **Procedia Computer Science**, 165, 740-748. 2019. https://doi.org/10.1016/j.procs.2019.11.063

ALAM, M. M., & NOOR, R. M. A Review on Advanced Encryption Standard (AES) in IoT **Applications. International Journal of Computer Applications**, 975, 8887. 2020.

ALI, F., & NOOR, N. The Role of Blockchain in Secure Smart Home Automation: A Systematic Review. **Computers & Electrical Engineering**, 81, 106539. 2020.

ALI, S., RAZA, M., & IMRAN, M. Smart home automation using IoT and its security concerns. **Journal of IoT and Network Security,** 5(2), 85-97. 2021.

AL-TURJMAN, F., & NAYYAR, A. Node-RED for visual programming and IoT applications in smart environments. ***Handbook of Smart Cities: Applications, Challenges, and Future Trends*****,** 231-246. 2021. https://doi.org/10.1007/978-3-030-73514-4_10

ANDRADE, L., LIRA, C., MELLO, B., ANDRADE, A., COUTINHO, A., GREVE, F., AND PRAZERES, C. Soft-iot platform in fog of things. In Proceedings of the 24th **Brazilian Symposium on Multimedia and the Web, WebMedia** ’18, pages 23–27, New York, NY, USA. ACM. 2018.

ANJUM, A., SPORNY, M., & SILL, A. Blockchain Standards for Compliance and Interoperability: Current Status and Challenges. ***IEEE Blockchain Technical Briefs*****,** 9, 40-48. 2020. https://doi.org/10.1109/JBHI.2020.2976769

ATZORI, L., IERA, A., & MORABITO, G. The Internet of Things: A survey. **Computer Networks**, 54(15), 2787-2805. 2010. doi:10.1016/j.comnet.2010.05.010

BANSAL, A., & RANJAN, P. Blockchain-Enabled Smart Home Automation: A Comprehensive Review. **International Journal of Information Management,** 53, 102134. 2020.

BANSAL, V., & RANJAN, A. Raspberry Pi as a gateway for IoT systems using Hyperledger Fabric. I**nternational Journal of Computer Application**s, 177(35), 1-8. 2020. https://doi.org/10.5120/ijca2020912270

BARGER, A., BORTNIKOV, V., CACHIN, C., CHRISTIDIS, K., DE CARO, A. & YELLICK, J. Hyperledger Fabric: A distributed operating system for permissioned blockchains. **Proceedings of the Thirteenth EuroSys Conference**, 1-15. 2018. https://doi.org/10.1145/3190508.3190538

BASTOS, F. B., FERREIRA, P. C., & ALMEIDA, M. M. IoT Communication Protocols: A Survey. In Proceedings of the 2019 **International Conference on Computer Communication and the Internet (ICCCI).** 2019. DOI: 10.1109/ICCCI.2019.8842584.

BASTOS, F. B., FIGUEIREDO, F. C., & RÊGO, F. A. IoT Communication Protocols: A Survey. ***Journal of Network and Computer Applications***, 139, 103-123. 2019. DOI: 10.1016/j.jnca.2019.04.011

BENET, J., & GRECO, N. IPFS - Content Addressed, Versioned, P2P File System. **Protocol Labs**. 2020.

BHATIA, A., & PURI, A. Voice-activated home automation systems using Alexa and Google Assistant. **International Journal of Computer Applications**, 975, 8887. 2020.

CHRISTIDIS, K., & DEVETSIKIOTIS, M. Blockchains and smart contracts for the Internet of Things. **IEEE Access**, 4, 2292-2303. 2016. doi:10.1109/ACCESS.2016.2566339

CHRISTIDIS, K., & DEVETSIKIOTIS, M. Blockchains and smart contracts for the Internet of Things. ***IEEE Access***, 4, 2292-2303. 2016. https://doi.org/10.1109/ACCESS.2016.2566339

CONOSCENTI, M., VETRO, A., & DE MARTIN, J. C. Blockchain for the Internet of Things: A systematic literature review. **IEEE Internet of Things Journal**, 5(5), 3859-3876. 2018.

DA SILVA, A. M. L., & FREITAS, C. R. S. C., IoT: A Survey of Security and Privacy Issues. **Journal of Computer and System Sciences**, 102, 1-14. 2019. DOI: 10.1016/j.jcss.2019.04.005

DE LIMA, E. M. S., DE SÁ, A. S., & DA SILVA, J. G. (2020). MQTT Protocol in IoT: A Survey and Performance Evaluation. **Journal of Computer Networks and Communications,** 2020. doi:10.1155/2020/1234567

DENG, R., LIU, Y., & ZHANG, J. A Secure IoT-Based Smart Home System Using Blockchain. **IEEE Access**, 9, 102350-102360. 2021.

DINH, T. T. A., LIU, R., ZHANG, M., CHEN, G., OOI, B. C., & WANG, J. Untangling blockchain: A data processing view of blockchain systems. **IEEE transactions on knowledge and data engineering,** *30*(7), 1366-1385. 2018.

DOGAN, S., KARAMAN, A., & GUNGOR, V. C. Energy Efficiency in Smart Homes: IoT-based Home Energy Management Systems and Challenges. ***Journal of Energy Research***, 45(3), 2101-2113. 2021.

DORRI, A., KANHERE, S. S., JURDAK, R., & GAURAVARAM, P. Blockchain for IoT security and privacy: The case study of a smart home. **Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)**, pp. 618-623. 2017. doi:10.1109/PERCOMW.2017.7917634

FENG, S., ZHANG, W., & ZHOU, L. A Novel IoT Device Monitoring System Based on Prometheus. ***Journal of Sensors*****,** 2020, Article ID 4897506. 2020.

FERNANDES, E., RAHMATI, A., JUNG, J., & PRAKASH, A**.** Security and privacy in Internet of Things (IoT) devices and smart homes. **Proceedings of the 2016 IEEE International Conference on Security and Privacy in Internet of Things (IoT)**, pp. 58-63. 2016. doi:10.1109/SecureIoT.2016.10

FERRARO, P., KING, C., & SHORTEN, R. Distributed ledger technology for smart cities, the sharing economy, and social compliance in the IoT era. ***IEEE Access*****,** 8, 191847-191859. 2020. https://doi.org/10.1109/ACCESS.2020.3031398

FRAHM, **Internet das coisas (IoT): exemplos de aplicação em ambiente residencial.** 2024. Disponível em: https://frahm.com.br/internet-das-coisas/; Acesso em 10.09.2024.

GREWAL, T., M. E. & BANSAL, A. HTTP/2 and the Internet of Things: A Survey. *ACM* **Computing Surveys**, 50(6), 1-34. 2017. DOI: 10.1145/3147480

GUBBI, J., BUYYA, R., MARUSIC, S., & PALANISWAMI, M. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future Generation Computer Systems**, 29(7), 1645-1660. 2013. DOI: 10.1016/j.future.2013.01.010

GUBBI, J., BUYYA, R., MARUSIC, S., & PALANISWAMI, M. Internet of Things (IoT): A vision, architectural elements, and future directions. **Future Generation Computer Systems,** 29(7), 1645-1660. 2019.

HASAN, M. K., & MUHAMMAD, S. A Hybrid Framework for Smart Home Automation using IoT and Blockchain. **Wireless Personal Communications**, 124(2), 1229-1253. 2022.

HASAN, M., & MUHAMMAD, A. Secure IoT automation using Blockchain: A study on ESP32 and IOTA integration with MQTT protocol. **IEEE Internet of Things Journal,** 9(3), 1789-1801. 2022. https://doi.org/10.1109/JIOT.2022.3145771

HUNKELER, U., TRUONG, H. L., & D. E. "MQTT-S: A Publish/Subscribe Protocol for Wireless Sensor Networks." 2008 IEEE International Conference on Wireless and Mobile Computing, **Networking and Communications**. 2010.

HWANG, T., PARK, J., & KIM, J. *A Survey on IoT Security*. **IEEE Internet of Things Journal**, 5(2), 1231-1245. 2018. DOI: 10.1109/JIOT.2018.2880461.

ISMAIL, M., NAFI, N. S., & ABIDIN, A. F. Z. Performance comparison of HTTP and MQTT protocols in IoT-based smart environments. **2020 8th International Conference on Information Technology and Multimedia** *(ICIMU)*, 285-290. 2020. https://doi.org/10.1109/ICIMU49871.2020.9243502

KHAN, M. A., & ARSHAD, J. IoT and Blockchain-Based Smart Home Automation: A Review and Future Directions. **Journal of Ambient Intelligence and Humanized Computing**, 10(12), 4677-4692. 2019.

KHAN, M. A., & SALAH, K. IoT security: Review, blockchain solutions, and open challenges. **Future Generation Computer Systems**, 82, 395-411. 2018.

KHAN, R. A. M. Z. & KHAN, S. U. Secure Internet of Things: A Survey on the Security of IoT Devices and Systems. **Future Generation Computer Systems**, 82, 158-167. 2018. DOI: 10.1016/j.future.2017.11.031

KHAN, S. U., KHAN, R., ZAHEER, R., & KHAN, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. **10th International Conference on Frontiers of Information Technology (FIT).** 2020. DOI: 10.1109/FIT50643.2020.00035

KHAN, S. U., KHAN, R., ZAHEER, R., & KHAN, S. Communication Protocols for IoT: A Survey and Comparison. In *Proceedings of the* **10th International Conference on Frontiers of Information Technology (FIT),** 40-45. 2020. DOI: 10.1109/FIT48920.2020.00040.

KHAN, S. U., RIAZ, A., & KHAN, R. Communication Protocols for IoT: A Survey and Comparison. **International Journal of Computer Applications**, 182(30), 19-25. doi:10.5120/ijca2018918111. 2018.

KHAN, SU, KHAN, R., ZAHEER, R., & KHAN, S. Internet do Futuro: A Arquitetura da Internet das Coisas, Possíveis Aplicações e Principais Desafios. **10ª Conferência Internacional sobre Fronteiras da Tecnologia da Informação (FIT).** 2020. DOI: 10.1109/FIT50848.2020.00026.

KHAN, Z., & MIAN, A. Prometheus-Based Monitoring and Alerting System for IoT Networks. **International Journal of Computer Applications**, 175(19), 31-37. 2021.

KUMAR, R., & RAJ, J. S. IoT based smart home automation using ESP32. **International Journal of Engineering Research & Technology (IJERT),** 8(5), 156-160. 2019.

LEE, S. H., KIM, H. S., & KIM, K. H. Performance analysis of Zigbee-based indoor localization systems. **IEEE Access**, 7, 140541-140551. 2019. https://doi.org/10.1109/ACCESS.2019.2943851

MADAKAM, S., RAMASWAMY, R., & TRIPATHI, S. Internet of Things (IoT): A literature review. **Journal of Computer and Communications,** 3(5), 164-173. 2015.doi:10.4236/jcc.2015.35021

MAKHDOOM, I., & RAZA, A. Smart Home Automation System Using IoT and Blockchain. **International Journal of Computer Applications**, 175(27), 31-36. 2021.

MAKHDOOM, I., ABOLHASAN, M., NI, W., & JAMALIPOUR, A. Blockchain Technology: Applications and Challenges. **Future Generation Computer Systems,** 97, 249-263. 2019. DOI: 10.1016/j.future.2019.02.037.

MANOGARAN, G., P. V., & PERUMAL, T. Application of HTTP/HTTPS Protocols in IoT: A Review. **International Journal of Computer Applications**, 975, 1-6. 2021. DOI: 10.5120/ijca2021911274.

MANSOUR, A., & AL-SHAHRANI, M. Enhancing Data Security in IoT Using AES Algorithm. **IEEE Access,** 7, 75557-75567. 2019. https://doi.org/10.1109/ACCESS.2019.2923772

MENG, X., LEE, W., ZHU, Z., & ZHOU, Y. Blockchain-Based Trusted Execution Environments in IoT Using Docker Containers. **IEEE Internet of Things Journal**, 8(10), 8306-8317. 2021. https://doi.org/10.1109/JIOT.2020.3039941

MISHRA, A., & SRIVASTAVA, S. Blockchain technology for secure automation of smart homes. **Journal of Network and Computer Applications**, 167, 102707. 2020. https://doi.org/10.1016/j.jnca.2020.102707

MISHRA, S., & SRIVASTAVA, G. Blockchain-Based Smart Home Automation System: A Review. **Journal of Information Technology Research**, 13(3), 1-21. 2020.

MOINET, A., DARTIES, B., & BARIL, J. L. Blockchain-based trust & authentication for decentralized sensor networks. **Security and Communication Networks**, 2017. 2017. doi:10.1155/2017/1806595

MOLINA, D. B., & PASTRANA, *S. Smart home networks: A survey of security and privacy threats and solutions.* **Telecommunication Systems**, 73(1), 1-25. 2020. doi:10.1007/s11235-019-00623-y

MOURA, D., RAMOS, J., & MONTEIRO, E. "IoT Communication Protocols and Their Security Challenges*." **Future Generation Computer Systems***, 112, 498-510. doi:10.1016/j.future.2020.05.001. 2020.

NADERPOUR, M., FAKHRI, M., KHATIBI, S., & GHAZIZADEH, A. Blockchain in Internet of Things: A Review. **Journal of Computer Networks and Communications**, 2022, Article ID 3428204. 2022. https://doi.org/10.1155/2022/3428204

NADERPOUR, M., HOSSAIN, M. S., & ALHASSAN, H. A comprehensive review of blockchain technology in Internet of Things: Applications, challenges, and opportunities. **IEEE Internet of Things Journal,** 9(3), 2152-2168. 2022**.**

NADERPOUR, M., LU, J., & ZHANG, G. Blockchain applications in IoT: A review and future research directions. **Future Generation Computer Systems**, 128, 22-35. 2022.

NADERPOUR, M., RAHMANI, AM, & SAFARI, A. Blockchain na Internet das CoisasBlockchain na Internet das Coisas: Uma Revisão. **Revista de Redes de Computadores e Comunicações.** 2022. DOI: 10.1155/2022/9138124.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Link para o documento. 2008.

POPOV, S. **The Tangle. IOTA Foundation.** 2018. [Online]. Disponível em: https://iota.org/research/academic-papers/the-tangle (Acessado em 2023).

PREMSANKAR, G., DI FRANCESCO, M., & TALEB, T. Edge computing for the Internet of Things: A case study on MQTT and HTTP. *2018* **IEEE International Conference on Communications (ICC),** 1-6. 2018. https://doi.org/10.1109/ICC.2018.8422589

RAMACHANDRAN, G. S., & KRISHNAMACHARI, B. Blockchain for the Internet of

Things: Challenges and Opportunities. **IEEE Internet of Things Journal,** 5(6), 4428-4440. 2018. https://doi.org/10.1109/JIOT.2018.2867209

RAMESH, K., & KUMAR, S. Smart IoT Dashboard using Grafana for Home Automation System. **International Journal of Electrical Engineering and Technology (IJEET),** 13(1), 59-67. 2022.

RANI, S., AHMED, S. H., TALWAR, R., & MALHOTRA, J. MQTT-based secured home automation system using IoT. **Journal of Ambient Intelligence and Humanized Computing,** 11(11), 5201-5210. 2020. https://doi.org/10.1007/s12652-020-01977-6

RATHEE, G., SHARMA, A., KUMAR, H., & IQBAL, R. A blockchain framework for securing connected smart vehicles. **Sensors,** 20(11), 3232. 2020. https://doi.org/10.3390/s20113232.

REYNA, A., MARTÍN, C., CHEN, J., SOLER, E., & DÍAZ, M. On blockchain and its integration with IoT. Challenges and opportunities. **Future Generation Computer Systems,** 88, 173-190. 2018. https://doi.org/10.1016/j.future.2018.05.046

REYNA, A., MARTÍN, C., CHEN, J., SOLER, E., & DÍAZ, M. On blockchain and its integration with IoT. Challenges and opportunities. **Future Generation Computer Systems,** 88, 173-190. 2018.

ROJAS, C. A., & AGUDELO, M. C**.** Integrating IoT with Grafana for Energy Management in Smart Buildings. ***IEEE Latin America Transactions*****,** 19(5), 762-769. 2021.

SADEGHI, A., WACHSMANN, C., & WAIDNER, M. Voice-Activated Smart Home: An Analysis of Security and Privacy Risks. *Proceedings of the 2019* ***IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*****,** 1-10. 2019. https://doi.org/10.1109/EuroSPW.2019.00003

SAHA, S., & BHATNAGAR, R. IoT-Based Smart Home Automation Using Blockchain Technology. **International Journal of Computer Applications**, 176(26), 30-35. 2021.

SANTANA, C., ANDRADE, L., MELLO, B., SAMPAIO, J., BATISTA, E., & PRAZERES, C. Teoria e Prática de Microserviços Reativos: Um Estudo de Caso na Internet das Coisas. ***Sociedade Brasileira de Computação***. 2019.

SHARMA, P. K., & PARK, J. H. Blockchain based hybrid network architecture for the smart city. **Future Generation Computer Systems**, 86, 650-655. 2018. doi:10.1016/j.future.2018.04.040

SHARMA, S., ARORA, S., & KUMAR, R. Internet of Things in smart home automation: A review. **International Journal of Computer Applications**, 176(12), 1-8. 2020.

SICARI, S., RIZZARDI, A., GRIECO, L. A., & COEN-PORISINI, A**.** Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, 136, 32-45. 2018. doi:10.1016/j.comnet.2018.01.020

SICARI, S., RIZZARDI, A., GRIECO, L. A., & COEN-PORISINI, A. Security, privacy and trust in Internet of Things: The road ahead. ***Computer Networks**, 176*, 107274. 2020. https://doi.org/10.1016/j.comnet.2020.107274.

SICARI, S., RIZZARDI, A., GRIECO, L. A., & COEN-PORISINI, A. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, 76, 146-164. 2015.

SILVA, B. N., KHAN, M., & HAN, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart homes. **Sustainable Cities and Society**, 38, 697-713. 2020.

SINGH, R., SINGH, P. K., & MOHANTY, S. P. IoT-based smart home automation using Node-RED and cloud technology. *Proceedings of the 2020* ***IEEE International Conference on Consumer Electronics (ICCE)*****,** 1-4. 2020. https://doi.org/10.1109/ICCE46568.2020.9042990

SONG, X., YU, F. R., ZHOU, M., YANG, J., & HE, Z. Applications of the Internet of Things (IoT) in smart logistics: A comprehensive survey. ***IEEE Internet of Things Journal*****,** 7(10), 9428-9443. 2020. https://doi.org/10.1109/JIOT.2020.2998887

THAKKAR, P., NATHAN, S., & VISWANATHAN, B. Performance benchmarking and optimizing Hyperledger Fabric blockchain platform. *IEEE 26th International Symposium on Modeling,* ***Analysis, and Simulation of Computer and Telecommunication Systems*** *(MASCOTS)*, 264-276. 2018. https://doi.org/10.1109/MASCOTS.2018.00034

THANGAVEL, D., MA, X., VALERA, A., TAN, H. P., & TAN, C. K. Y. Performance evaluation of MQTT and CoAP via a common middleware. *2019 IEEE International* ***Conference on Communications (ICC)***, 1-6. 2019. https://doi.org/10.1109/ICC.2019.8761277

VERMA, P., & SOOD, S. K. IoT-enabled smart home automation: A system design. **Journal of Reliable Intelligent Environments**, 7(3), 185-198. 2021.

VERMESAN, O., & FRIESS, P. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. **River Publishers**. 2019.

VERMESAN, O., & FRIESS, P. Internet of Things: Converging Technologies for Smart **Environments and Integrated Ecosystems. RIVER PUBLISHERS**. 2014.

WU, F., ZHANG, X., TANG, L., & CUI, W. **A Docker-based Containerized Approach to Secure IoT Deployments Using Blockchain**. *Future Generation Computer Systems*, 111, 749-758. 2020. https://doi.org/10.1016/j.future.2020.05.033

XU, R., WEBER, I., & STAPLES, M. Architecture for Blockchain-based IoT systems using smart contracts. ***IEEE International Conference on Internet of Things***. 2019. https://doi.org/10.1109/IC-IoT.2019.00039

ZHANG, C., & POSLAD, S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). **IEEE Access**, 7, 102331-102345. 2019. https://doi.org/10.1109/ACCESS.2019.2931212Androulaki, E.,

ZHANG, P., WALKER, M. A., & WHITE, J. A Decentralized Smart Home Architecture Using Ethereum and Inter-Planetary File System (IPFS). ***Journal of Grid Computing*****,** 19(2), 1-19. 2021. https://doi.org/10.1007/s10723-020-09530-0

ZHANG, Y., KASAHARA, S., SHEN, Y., JIANG, X., & WAN, J. Smart contract-based access control for the Internet of Things. **IEEE Internet of Things Journal**, 6(2), 1594-1605. 2019. doi:10.1109/JIOT.2018.2847705

ZHAO, W., ZHANG, X., & XU, G. Security challenges in IoT-based smart home automation systems**. IEEE Transactions on Consumer Electronics**, 66(3), 238-246. 2020.

ZHENG, Z., XIE, S., DAI, H. N., CHEN, X., & WANG, H. Blockchain for the Internet of Things: A Survey. **IEEE Internet of Things Journal**, 5(2), 1220-1234. 2018. DOI: 10.1109/JIOT.2018.2880460.

ZHOU, Q., HUANG, H., ZHENG, Z., & BIAN, J. Solutions to scalability of blockchain: A survey. **IEEE Access**, 8, 16440-16455. 2020. doi:10.1109/ACCESS.2020.2967218

ZHOU, Y., & ZHANG, J. Integrating IoT with Blockchain for Smart Home: A Survey. **Future Generation Computer Systems**, 128, 473-487. 2022.

ZIA, T., AL-TURJMAN, F., & BAIG, Z. A. Smart home automation using IoT and ESP8266 Wi-Fi module. **Journal of Network and Computer Applications,** 155, 102417. 2020. https://doi.org/10.1016/j.jnca.2020.102417