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

JESSICA MARIELLA DE CARVALHO OLIVEIRA

INTEGRAÇÃO DA TECNOLOGIA BLOCKCHAIN EM REDE DE SENSORES PARA IOT

MANAUS
2024

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

JESSICA MARIELLA DE CARVALHO OLIVEIRA

INTEGRAÇÃO DA TECNOLOGIA BLOCKCHAIN EM REDE DE SENSORES PARA IOT

Dissertação apresentada ao Curso de Mestrado em Engenharia Elétrica, área de concentração em Controle e Automação de Sistemas na linha de pesquisa em 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
2024

Ficha Catalográfica

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

Oliveira, Jéssica Mariella de Carvalho
O48i Integração da tecnologia blockchain em rede de sensores para IoT / Jéssica Mariella de Carvalho Oliveira . 2024
60 f.: il. color; 31 cm.

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

1. Blockchain. 2. Internet das Coisas. 3. Rede de Sensores. 4. Android. 5. Microcontrolador. I. Cruz, Carlos Augusto de Moraes. II. Universidade Federal do Amazonas III. Título

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

JÉSSICA MARIELLA DE CARVALHO OLIVEIRA.

INTEGRAÇÃO DA TECNOLOGIA BLOCKCHAIN EM REDE DE SENSORES PARA IOT

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

Aprovada em 27 de março de 2024.

BANCA EXAMINADORA

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

Prof. Dr. Kenny Vinente dos Santos, Membro
Universidade Federal do Amazonas

Prof. Dr. Frederico da Silva Pinagé, Membro
Universidade Federal do Amazonas

PPGEE
Programa de Pós-Graduação em Engenharia Elétrica - UFAM

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

AGRADECIMENTOS

Expresso minha gratidão primeiramente a Deus por me proporcionar a alegria e o prazer de viver.

À minha amada família, especialmente ao meu esposo Igor Rafael Arruda de Oliveira, cujo apoio inabalável tem sido fundamental para superar os desafios da vida. Agradeço também aos meus pais, Vera Lúcia e João Fernando, pelo amor incondicional que sempre foram minha base e força motriz por trás de minha jornada acadêmica, e a minha irmã Núbia Altina, pelo encorajamento e apoio constante e aos meus irmãos mais novos Fátima Muller e João Miguel pelo amor e paciência.

Ao Professor Orientador Dr. Carlos Augusto de Moraes Cruz, por compartilhar seu tempo, paciência e conhecimento, guiando-nos através dos conceitos essenciais que nos permitiram crescer e amadurecer diante das adversidades no desenvolvimento deste projeto.

Aos estimados colegas de laboratório da UFAM por sua colaboração, em especial a Talita C. Pinheiro, pela cooperação, amizade e apoio mútuo ao longo deste percurso acadêmico, e a Mario R. L. Oliveira, pelo suporte técnico. As discussões e trocas de ideias foram essenciais para o enriquecimento deste trabalho.

Expresso minha sincera gratidão à Universidade Federal do Amazonas (UFAM) e ao Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) pelo apoio inestimável concedido à minha pesquisa que tornou este trabalho possível. Além disso, sou grato à Fundação de Pesquisa do Estado do Amazonas - FAPEAM, no âmbito do programa POSGRAD, Edital Nº 008/2021. Agradecemos profundamente à CAPES e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

RESUMO

A Internet das Coisas (IoT) e a blockchain são duas áreas revolucionárias que estão transformando a maneira como a sociedade está interagindo com o meio digital. Quando combinadas, essas tecnologias podem criar soluções poderosas para diversos problemas.

IoT refere-se a interconexão de dispositivos físicos que podem coletar e trocar dados pela internet o qual tem o potencial de revolucionar uma ampla gama de setores, incluindo a agricultura, saúde, manufatura e cidades inteligentes, através de alguns dispositivos que podem ser sensores, câmeras, medidores, veículos e entre outros.

A tecnologia blockchain é conhecida como um banco de dados por sua capacidade de fornecer um registro imutável e seguro de transações no qual consiste em uma cadeia de blocos interconectados, onde cada bloco contém um registro de transações que é protegido por criptografia. Uma vez registradas em um bloco as informações não podem ser alteradas retroativamente, com isso garantindo a integridade da informação.

Um dos principais desafios da IoT é garantir a segurança e a privacidade da informação, com milhões de dispositivos interconectados na internet coletando e transmitindo informações logo a vulnerabilidade e a manipulação dos dados não autorizados tornam-se uma preocupação crítica, diante deste cenário buscou aplicar a característica da blockchain à IoT.

O sistema utilizará a tecnologia blockchain em uma pequena rede de sensores para aplicações de Internet das Coisas, em automação de ambientes inteligentes que combina os recursos básicos de um microcontrolador arduino uno com um smartphone android integrado com um aplicativo de carteira bitcoin personalizado. Ao integrar esses componentes, o sistema capitaliza os benefícios inerentes do blockchain, permitindo o gerenciamento de dados seguro e transparente dentro da rede de sensores. Essa abordagem inovadora abre novas possibilidades para a integridade de dados aprimorados, controle descentralizado e integração perfeita da rede de sensores com o blockchain. Este trabalho traz uma nova perspectiva como a IoT pode ser aprimorada por meio da tecnologia blockchain, abordando uma solução simples e eficaz utilizando o protocolo bitcoin.

Palavras-chaves: Blockchain; Internet das Coisas; Rede de sensores; Android; Microcontrolador.

ABSTRACT

The Internet of Things (IoT) and Blockchain are two revolutionary areas that are transforming the way society interacts with the digital world. When combined, these technologies can create powerful solutions for various problems. IoT refers to the interconnection of physical devices that can collect and exchange data over the internet, which has the potential to revolutionize a wide range of sectors, including agriculture, healthcare, manufacturing, and smart cities, through devices such as sensors, cameras, meters, vehicles, and more.

Blockchain technology is known for its ability to provide an immutable and secure record of transactions, consisting of a chain of interconnected blocks, where each block contains a record of transactions that is protected by cryptography. Once recorded in a block, the information cannot be retroactively altered, thus ensuring the integrity of the information. One of the main challenges of IoT is ensuring the security and privacy of information, with millions of interconnected devices on the internet collecting and transmitting information, making vulnerability and unauthorized data manipulation a critical concern. In this scenario, the characteristic of Blockchain is applied to IoT.

This work brings a new perspective on how IoT can be enhanced through Blockchain technology, addressing a simple and effective solution using the Bitcoin protocol. The system will use blockchain technology in a small sensor network for Internet of Things (IoT) applications, automation, and smart environments, combining the basic features of an Arduino Uno microcontroller with an Android smartphone integrated with a custom Bitcoin wallet application. By integrating these components, the system capitalizes on the inherent benefits of blockchain, allowing for secure and transparent data management within the sensor network. This innovative approach opens new possibilities for enhanced data integrity, decentralized control, and seamless integration of the sensor network with the blockchain.

Keywords: Blockchain; Internet of Things; Sensor network; Android; Microcontroller.

LISTA DE FIGURAS

Figura 1 – Previsão de dispositivos conectados à Internet das Coisas (IoT) 18
Figura 2 – Arquitetura básica da IoT 19
Figura 3 – Linha do Tempo da Blockchain 20
Figura 4 – Evolução das fases da Blockchain 21
Figura 5 – Estrutura básica da Blockchain 21
Figura 6 – Funcionamento da Blockchain 24
Figura 7 – Arquitetura da Blockchain em 4 camadas 25
Figura 8 – Estrutura interna de um bloco da Blockchain 27
Figura 9 – Interconexão entre dispositivos do sistema 37
Figura 10 – Estados Armazenados na Blockchain 38
Figura 11 – Exemplos de dados do sistema proposto 39
Figura 12 – Arquitetura do Sistema da API 40
Figura 13 – Esquema de entradas e saídas 40
Figura 14 – Módulo DHT22 41
Figura 15 – Módulo bluetooth HC-05 42
Figura 16 – Esquema de ligações para o Arduino 43
Figura 17 – IDE do Arduino 44
Figura 18 – Backend e API 45
Figura 19 – Interface do usuário com carteira embutida 46
Figura 20 – Estado inicial da sincronização 48
Figura 21 – Sincronização de M1 com M2 49
Figura 22 – Estados do LED 001 50
Figura 23 – Dados dos estados do LED 001 gravados na Blockchain 51
Figura 24 – Informações gravados na Blockchain 52
Figura 25 – Resultados do acionamento por temperatura 53

LISTA DE TABELAS

Tabela 1 – Comparação entre PoW e PoS 30
Tabela 2 – Comparação entre as diferentes Blockchains 34
Tabela 3 – Componentes do Sistema 47
Tabela 4 – Atividades de M1 durante a sincronização 47
Tabela 5 – Atividades de M2 durante a sincronização 48

LISTA DE SIGLAS

AES-CBC	*Advanced Encryption Standard - Cipher Block Chaining*
API	*Application Programming Interface*
BCH	*Bitcoin Cash*
BFT	*Bizantine Fault Tolerance*
BSV	*Bitcoin Satoshi Vision*
BTC	*Bitcoin*
BVM	*Bitcoin Virtual Machine*
BaaS	*Blockchain as a Service*
DAG	*Directed Acyclic Graph*
DER	*Distinguished Encoding Rules*
DPoS	*Delegate Proof of Stake*
DSA	*Digital Signature Algorithm*
EdDSA	*Edwards-curve Digital Signature Algorithm*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EVM	*Ethereum Virtual Machine*
GPToken	*General Purpose Token*
HMAC	*Hash-based Message Authentication Code*
IA	*Artificial Intelligence*
IBM	*International Business Machines Corporation*
IEEE	*Institute of Electrical and Electronics Engineers*
IoT	*Internet of Things*
IV	*Initialization Vector*
NFT	*Non-Fungible Token*
PoS	*Proof of Stake*
PoW	*Proof of Work*
P2P	*Peer-to-peer*
RSA	*Rivest-Shamir-Adleman*
SHA	*Secure Hash Algorithm*

SAT	*Satoshis*
TXID	*Transaction Identication*
TPS	*Transaction per second*
UTXO	*Unspent Transaction Output*

SUMÁRIO

1 INTRODUÇÃO 13

1.1 Objetivo Geral 14

1.2 Objetivos Específicos 14

1.3 Organização do Trabalho 15

1.4 Revisão da Literatura 15

1.5 Trabalhos Relacionados sobre a Integração de IoT e Blockchain 16

2 REFERENCIAL TEÓRICO 18

2.1 A Internet das Coisas 18

2.2 Arquitetura IoT 19

2.3 História da Tecnologia Blockchain 19

2.3.1 Fase 1 - Blockchain 1.0: Transações 21

2.3.2 Fase 2 - Blockchain 2.0: Contratos inteligentes 22

2.3.3 Fase 3 - Blockchain 3.0: Aplicações 23

2.4 Como funciona a blockchain 23

2.5 Tipos de Blockchain 28

2.5.1 Bitcoin (BTC) 30

2.5.2 Bitcoin Satoshi Vision (BSV) 31

2.5.3 Etherum (ETH) 32

3 MATERIAIS E MÉTODOS 35

3.1 Metodologia 35

3.2 Composição inicial e básica do sistema 37

3.3 Placa Arduino Uno 40

3.4 Módulo de Temperatura DHT 22 para o arduino 41

3.5 Módulo de Comunicação Bluetooth 42

3.6 Seleção do Ambiente do Arduino Uno 43

3.7 Seleção do ambiente da API para o dispositivo Android 45
3.8 Dados armazenados na Blockchain BSV 45
4 RESULTADOS E DISCUSSÕES 46
4.1 Apresentação 46
4.2 Resultados da Sincronização 47
4.3 Resultados do Acionamento por Temperatura 50
5 CONCLUSÃO E TRABALHOS FUTUROS 54
6 REFERÊNCIAS BIBLIOGRÁFICAS 56

1 INTRODUÇÃO

Esta dissertação trata da integração da tecnologia blockchain em rede de sensores para Internet das Coisas (IoT). A pesquisa foi realizada com o objetivo de explorar como a tecnologia Blockchain pode ser utilizada para aumentar a segurança, a privacidade e a eficiência das redes de sensores em aplicações IoT. Resultados preliminares deste trabalho foram apresentados no XVI Simpósio Brasileiro de Automação Inteligente (SBAI 2023) e o X Simpósio Brasileiro de Sistemas Elétricos (SBSE 2023), realizado nos dias 15 e 18 de outubro de 2023 em Manaus, Amazonas, onde foram discutidos e avaliados por especialistas da área [1].

As características e atributos de segurança da tecnologia blockchain têm recebido atenção significativa devido à sua desejabilidade para uma infinidade de aplicações em contratos inteligentes, incluindo IoT e muitas outras formas de automação [2-4].

Em 2008, o surgimento da blockchain da aplicação bitcoin trouxe um conceito inovador que inicialmente escapou de uma compreensão completa [5] mas, em 2017, demonstrou finalmente o potencial para construir contratos inteligentes e aplicações inovadoras [6]. No entanto a tecnologia blockchain despontou como uma solução para uma diversidade de desafios. Seu emprego abrange áreas como armazenamento e execução de trechos de código [7], serviços de DNS (Domain Name System) [8], controle de transações [9], votação eletrônica [10] e gestão de direitos autorais [11]. Essas aplicações diversas tiram proveito das características de resiliência, provenientes da natureza descentralizada da rede assegurada por meio de assinaturas digitais nas transações, e da imutabilidade. Assim, a blockchain confere confiabilidade aos dados mantidos por ela.

A capacidade de processar um maior número de transações por segundo (TPS) em uma blockchain é essencial para atender aos requisitos de escalabilidade das aplicações de IoT. Em um ecossistema de IoT, inúmeros dispositivos geram e trocam constantemente dados, exigindo processamento rápido e eficiente. À medida que o número de dispositivos conectados e o volume de dados que eles produzem aumentam, a rede blockchain deve ser capaz de lidar com o crescente volume de transações [12].

No contexto contemporâneo da tecnologia, a convergência entre blockchain e IoT se apresenta como uma perspectiva promissora para otimizar o armazenamento de dados em

diversas áreas. Este projeto, intitulado "Integração da Tecnologia Blockchain em rede de sensores para IoT", surge como resposta à necessidade de aprimorar o armazenamento, acesso e compartilhamento de informações essenciais referentes aos dados coletados da rede de sensores.

Este projeto busca à implementação de um projeto focado no desenvolvimento de uma API robusta e eficiente utilizando o protocolo bitcoin que viabilize a integração de um sensor de temperatura com a tecnologia blockchain.

Ao unir as capacidades do sensor de temperatura com a segurança e imutabilidade proporcionadas pela tecnologia blockchain, espera-se contribuir significativamente para o avanço das soluções IoT, possibilitando uma gestão mais eficaz e segura dos dados de temperatura em diversas aplicações, como monitoramento ambiental, controle de processos industriais, e saúde.

Como resultado, espera-se disponibilizar uma API confiável e eficiente capaz de coletar os dados de temperatura fornecidos pelo sensor e registrá-los de maneira segura e imutável na cadeia de blocos. Esse sistema permitirá não apenas a captura precisa das informações de temperatura, mas também garantirá a sua rastreabilidade e autenticidade ao longo do tempo, proporcionando uma base sólida para aplicações que exijam alta confiabilidade e transparência nos dados.

1.1 Objetivo Geral

Desenvolver uma API que possibilite a integração de um sensor de temperatura com a tecnologia blockchain, visando criar um sistema capaz de coletar dados de temperatura do sensor e registrá-los de maneira segura e imutável na cadeia de blocos.

1.2 Objetivos Específicos

- Desenvolver a estrutura da API para facilitar a comunicação entre o sensor de temperatura com a tecnologia blockchain.
- Implementar funcionalidades na API para garantir o registro seguro e imutável dos dados de temperatura na cadeia de blocos, utilizando o bluetooth como meio de comunicação entre o arduino e o smartphone.

- Criar métodos na API para coletar os dados de temperatura do sensor conectado ao arduino de forma precisa e eficiente.
- Realizar testes extensivos da API em ambientes de desenvolvimento para verificar sua robustez e eficácia, considerando a integração com o arduino e o bluetooth.

1.3 Organização do Trabalho

Esta dissertação está estruturada da seguinte forma:

Capítulo 1: Introdução - Este capítulo destaca a importância da tecnologia blockchain aplicada ao setor de IoT, discutindo trabalhos publicados na literatura que abordam a aplicação de blockchain em IoT.

Capítulo 2: Referencial Teórico - Apresenta os fundamentos teóricos das técnicas utilizadas no desenvolvimento deste trabalho, incluindo suas arquiteturas, o desenvolvimento na segmentação de imagens e os métodos de otimização avaliados.

Capítulo 3: Materiais e Métodos - Detalha os materiais e métodos utilizados, abrangendo as características do hardware, software e componentes envolvidos na metodologia proposta.

Capítulo 4: Resultados e Discussões - Discute os resultados alcançados, oferecendo uma análise detalhada deles.

Capítulo 5: Conclusão e Trabalhos Futuros - Apresenta sugestões para trabalhos futuros, recomendando melhorias no método proposto.

1.4 Revisão da Literatura

Para verificar quais as técnicas adotadas para o desenvolvimento da dissertação intitulada como “Integração da Tecnologia Blockchain em Rede de Sensores para IoT”, foi necessário realizar uma pesquisa bibliográfica a respeito do tema. Para essa busca nas bases as seguintes strings foram utilizadas: ((Blockchain) AND (Internet das Coisas OR Internet of Things)) com anos da publicação de 2017 a 2023.

As pesquisas foram realizadas nas bases literárias IEEE Xplore, Web of Science e Engineering Village. Os artigos foram obtidos, com publicações datadas entre 2017 e 2023, seguindo a mesma estratégia de busca avançada, com as devidas conversões e adaptações. Priorizou-se a pesquisa por artigos de revistas, devido à sua maior credibilidade e confiabilidade.

1.5 Trabalhos Relacionados sobre a Integração de IoT e Blockchain

O Blockchain está incorporando as tecnologias mais recentes, como IA, IoT, computação em nuvem e outras. As indústrias estão adotando o conceito de blockchain juntamente com as tecnologias emergentes, como IoT, para viabilizar transações confiáveis. Bilhões de dispositivos estão conectados à IoT. Muitos estudos recentes demonstram a integração de IoT e Blockchain e abordam as vantagens e desafios dessa integração.

O artigo de pesquisa [13] afirma que os dados pessoais dos usuários são protegidos de forma imutável onde um usuário não precisa depender de terceiros confiáveis. O conceito de blockchain da bitcoin é utilizado para fornecer segurança aos dispositivos IoT usando um protocolo de prova de conceito.

O framework de acesso em [14] introduz novos tipos de transações que são utilizados para conceder, obter, delegar e revogar acesso na blockchain foram utilizados uma arquitetura distribuída e um framework que consiste em quatro camadas principais que são determinadas como objetivo, modelo, arquitetura e mecanismo.

Em 2017, foi desenvolvido um sistema IoT multicamadas utilizando blockchain [15]. Em vez de adotar o blockchain distribuído convencional, os pesquisadores propuseram o uso de um blockchain com várias camadas, o que aprimora a capacidade e a segurança dos dispositivos IoT, que permite a comunicação entre P2P e estabelece uma rede IoT segura e confiável. Além disso, destaca as desvantagens do blockchain com múltiplas camadas, incluindo aumento do custo total da rede, tempo de disponibilidade dos dispositivos e uso de recursos.

Em [16], foi proposta a arquitetura descentralizada de controle de acesso baseada em blockchain, denominada cadeia de controle que dispensa a necessidade de terceiros e oferece conexões transparentes, tolerantes a falhas, escaláveis, compatíveis e seguras entre dispositivos IoT.

Já em 2018 [17], a arquitetura IoT foi proposta para permitir acesso e autenticação seguros para dispositivos IoT. Os pesquisadores desenvolveram seu próprio mecanismo de prova de posse para realizar transações e armazenar dados no blockchain utilizando a plataforma Ethereum.

Em 2019, pesquisadores propuseram um método para reforçar a segurança dos dispositivos IoT e ampliar a conectividade com outros dispositivos IoT utilizando a tecnologia blockchain [18]. Conforme as observações ao aplicar este método declarado aos ambientes de

simulação de redes IoT, o número de dispositivos vulneráveis à segurança foi reduzido em 48,5% em comparação com os ambientes tradicionais de IoT.

Em 2020, foi proposta a arquitetura inteligência do bloco IoT [19], que combina os conceitos de blockchain, IoT e IA. Este documento também detalha como o blockchain impulsionado pela IA reduz os problemas do blockchain. Os pesquisadores também apontam as direções futuras com a arquitetura do bloco convergindo blockchain e IA para alcançar o objetivo de uma IoT escalável e segura com inteligência em nuvem, inteligência de borda e inteligência de dispositivo.

No estudo [20], os pesquisadores abordam o framework para saúde baseado em IoT integrado com a blockchain. Em decorrência do impacto da pandemia de 2019 causada pelo novo coronavírus, muitos sistemas de recorreram a aplicativos para auxiliar pessoas infectadas e obter suas informações de saúde por meio de dispositivos inteligentes. O artigo também explora diferentes aplicativos inteligentes para detectar o coronavírus, como Aarogya, Kwarantanna domowa, Tawakkalna, Trace Together, Lets Beat COVID e Covid Watch.

Para reforçar a segurança dos dispositivos IoT conectados, estão sendo desenvolvidas pesquisas em algoritmos de criptografia baseados em blockchain. Em 2021, os autores [21] simplificaram a blockchain baseado em grafo acíclico direcionado propondo um novo algoritmo AES-CBC, que altera periodicamente a chave privada e o valor do vetor IV. Os resultados dos experimentos conduzidos com 10 dispositivos IoT conectados por blockchain baseado em DAG concluem que o novo algoritmo AES-CBC proposto reduz o custo e o tempo requeridos pelo algoritmo AES-CBC convencional em 20%.

No artigo [22], os pesquisadores propuseram um mecanismo de blockchain híbrido baseado na grade inteligente 5G MEC e o implementaram em um servidor MEC usando blockchain público e privado. Esse mecanismo solucionou os problemas de codificação e identificação de dispositivos IoT em massa na grade inteligente. Além disso, o impacto do blockchain híbrido quando aplicado a vários algoritmos de consenso, como PoW, PoS e DPoS.

2 REFERENCIAL TEÓRICO

2.1 A Internet das Coisas

A Internet das Coisas (IoT) é uma área de pesquisa dominante que está impulsionando o mundo em direção à revolução digital, proporcionando uma ampla gama de aplicações, como residências inteligentes, cidades inteligentes, assistência médica inteligente, agricultura inteligente, transporte e logística inteligentes, entre outras. Em termos simples, a IoT, concebida por Kevin Ashton em 1999, é uma rede que interliga dispositivos diversos, facilitando não apenas a comunicação entre pessoas e máquinas, mas também promovendo a automação e a integração de sistemas em vários setores [23]

O primeiro eletrodoméstico que utilizava deste conceito surgiu em junho de 2000, no qual a empresa Life's Good apresentou ao público a primeira geladeira inteligente durante um evento na Coreia do Sul [24]. Em 2010 foi constatado que o número de "coisas" conectadas a internet já superava o número de habitantes na terra. Essa informação é amparada pelo levantamento da Cisco IBSG apresentado no White Paper de Evans [25].

De acordo com Figura 1 as previsões da Transforma Insights para 2033, o número de dispositivos IoT deverá quase triplicar, passando de 13,8 bilhões em 2022 para mais de 39,5 bilhões em 2033 [26].

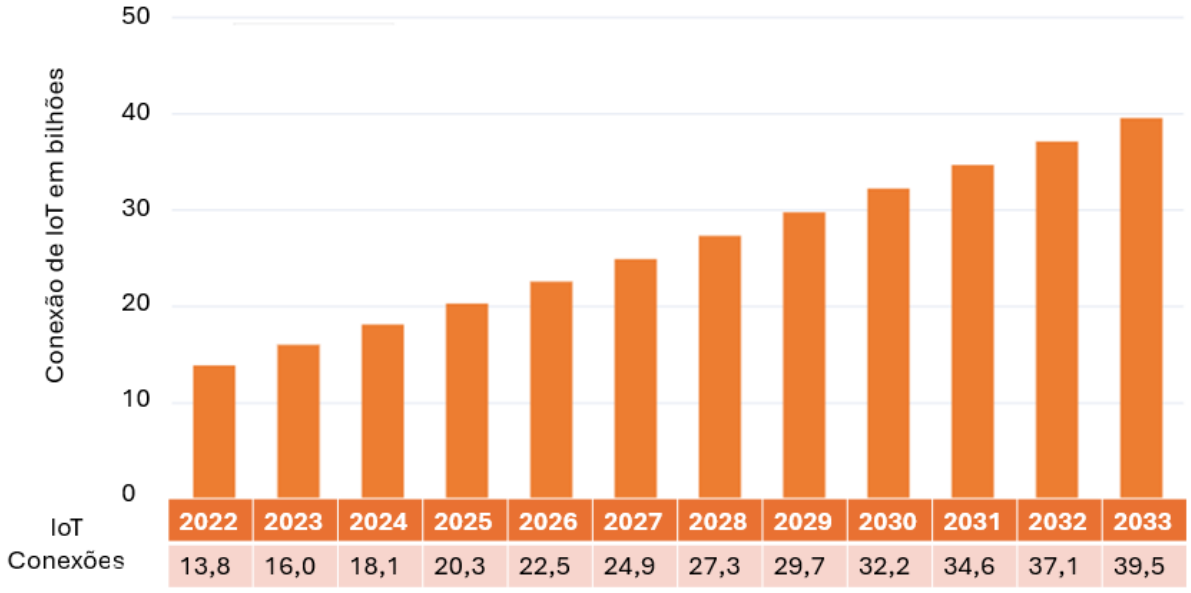

Figura 1- Previsão de dispositivos conectados à Internet das Coisas (IoT)
Fonte: Transforma Insights, 2024.

2.2 Arquitetura IoT

A arquitetura básica da IoT consiste em três camadas, conforme mostrado na Figura 2. Os principais componentes da arquitetura IoT são a camada de aplicação, camada de rede, e a camada de percepção [27-29].

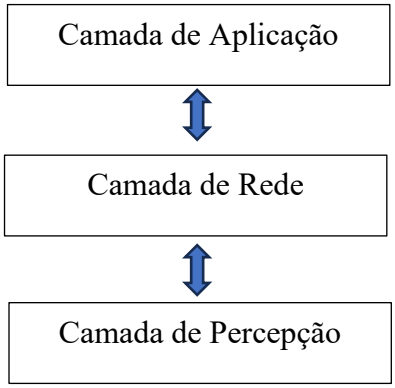

Figura 2 - Arquitetura básica da IoT
Fonte: Autoria própria, 2024.

A camada de percepção é a camada mais baixa da arquitetura da IoT, também conhecida como camada física que abrange os dispositivos como os sensores que coletam dados do ambiente físico.

A camada de rede é responsável por conectar a camada de percepção à camada de aplicação pois facilita a comunicação entre os dispositivos na camada de percepção e os servidores ou sistemas na camada de aplicação.

A camada de aplicação é a camada mais alta da arquitetura da IoT a qual é a responsável pela análise, processamento e utilização dos dados coletados pelos dispositivos sensores. Nesta camada, os dados são transformados em informações significativas e os serviços são fornecidos com base nesses dados processados.

2.3 História da Tecnologia Blockchain

O matemático Stuart Haber e o físico W. Scott Stornetta são considerados os precursores da tecnologia blockchain, tendo concebido os princípios fundamentais em 1991. Suas pesquisas pioneiras estabeleceram as bases para o desenvolvimento posterior dessa tecnologia revolucionária. Seu projeto inicial envolvia a criação de uma rede de blocos

protegidos por criptografia, onde o registro de data e hora dos documentos não poderiam ser adulterados. Nesse ano, Stuart Haber e o Scott Storneta publicaram um artigo pioneiro sobre o assunto [30].

Em 1992, eles atualizaram seu sistema para incluir árvores de Merkle, o que aumentou a eficiência ao permitir a inclusão de mais documentos em um único bloco [31]. O trabalho desses dois pesquisadores foi até mesmo referenciado por Nakamoto, o suposto criador da blockchain, em seu white paper. No entanto, foi em 2008 que a história da blockchain começou a ganhar relevância, conforme pode ser visto na Figura 3, graças ao trabalho de uma pessoa ou grupo conhecido como Satoshi Nakamoto. Em 2009, Nakamoto publicou o primeiro whitepaper sobre a tecnologia, detalhando como ela poderia melhorar a confiança digital com sua descentralização, o que significava que ninguém controlaria totalmente a rede.

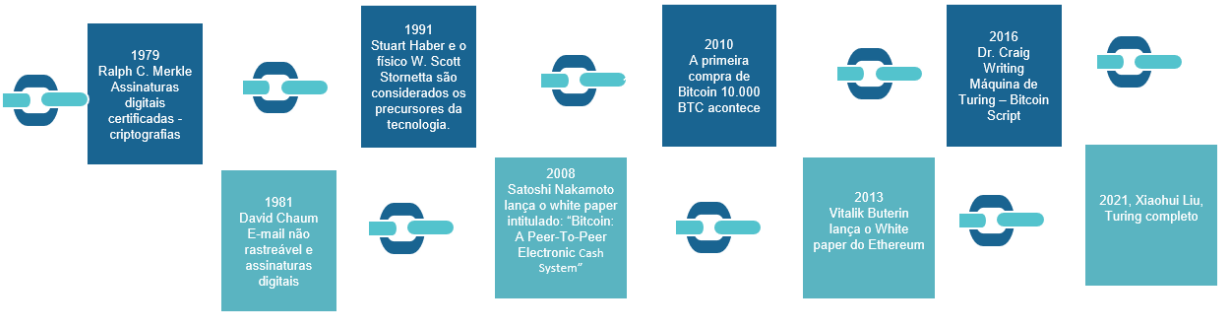

Figura 3 - Linha do tempo da Blockchain
Fonte: Autoria própria, 2024.

Antes do advento do bitcoin em 2009, a tecnologia não tinha sido amplamente aplicada em casos de uso significativos. O Bitcoin Cash (BTC) foi, portanto, a primeira aplicação notável do blockchain.

Com a ascensão do bitcoin, a blockchain emergiu como uma tecnologia de destaque, destacando-se como uma das mais promissoras da atualidade.

Embora seja fundamental para as criptomoedas, a blockchain também oferece possibilidades em outras áreas, como a criação de contratos inteligentes e o aprimoramento da segurança em transações financeiras e de saúde conforme pode ser visto na Figura 4 a evolução das fases da blockchain.

Figura 4 - Evolução das fases da Blockchain
Fonte: Autoria própria, 2024.

Além disso, a blockchain é uma tecnologia que proporciona suporte distribuído e confiável para a realização de transações. Considerada uma tecnologia disruptiva que tem o potencial de substituir entidades certificadoras e centralizadoras de transações comerciais, como bancos, governos e cartórios [32].

2.3.1 Fase 1 - Blockchain 1.0: Transações

Embora muitas pessoas associem bitcoin e blockchain como sendo a mesma coisa, essa percepção não é precisa. Na realidade, a blockchain é a tecnologia subjacente que impulsiona a maioria das aplicações, das quais as criptomoedas são apenas uma.

O Bitcoin emergiu em 2008 como a primeira implementação da tecnologia blockchain. Satoshi Nakamoto, em seu whitepaper, descreveu-o como um sistema eletrônico P2P, "peer-to-peer". Nakamoto criou o bloco de gênese, a partir do qual outros blocos foram minerados e interligados, formando uma das maiores cadeias de blocos que registram diversas informações e transações.

A Figura 5 ilustra a proposta de Nakamoto, destacando a cadeia de blocos gerada em cada transação dentro da estrutura do blockchain.

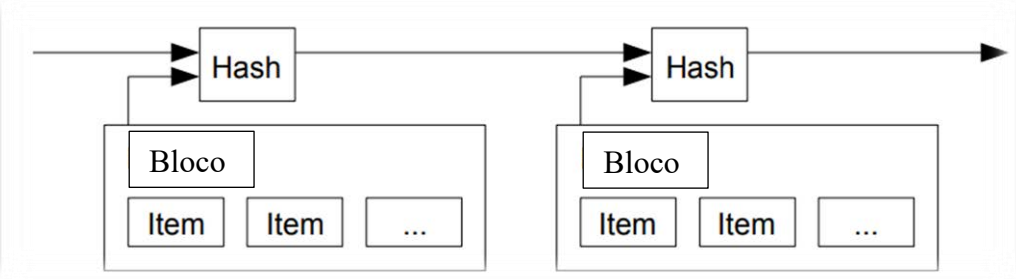

Figura 5 - Estrutura básica da Blockchain
Fonte: Nakamoto, 2008.

Desde que o bitcoin, como uma aplicação da blockchain, capturou a atenção dos desenvolvedores, uma série de outras aplicações foram desenvolvidas, todas buscando aproveitar os princípios e as capacidades da tecnologia de contabilidade digital. Consequentemente, o ecossistema da blockchain tem visto uma longa lista de novas aplicações surgirem com o avanço da tecnologia [36-37].

2.3.2 Fase 2 - Blockchain 2.0: Contratos inteligentes

Vitalik Buterin foi um dos primeiros colaboradores do bitcoin e percebeu que a criptomoeda não explorava completamente todas as possibilidades oferecidas pela rede blockchain.

Preocupado com as limitações do bitcoin, Buterin começou a trabalhar em uma blockchain mais flexível que pudesse executar diversas funções. Assim, o Ethereum nasceu como uma nova blockchain pública em 2013, apresentando funcionalidades adicionais em comparação com o bitcoin, o que representou um marco importante na história da tecnologia blockchain [36-37].

Buterin diferenciou o Ethereum da blockchain do bitcoin ao habilitar uma função que permitia às pessoas registrar outros ativos, como contratos inteligentes e slogans. Esse novo recurso expandiu as capacidades do Ethereum, transformando-o de uma simples criptomoeda para uma plataforma completa para o desenvolvimento de aplicativos descentralizados.

Oficialmente lançada em 2015, a blockchain do Ethereum evoluiu para se tornar uma das maiores aplicações da tecnologia blockchain, graças à sua capacidade de suportar contratos inteligentes que são usados para executar diversas funções. Além disso, a plataforma blockchain do Ethereum conseguiu reunir uma comunidade ativa de desenvolvedores, estabelecendo um verdadeiro ecossistema ao seu redor.

A blockchain do Ethereum processa o maior número de transações diárias devido à sua capacidade de suportar contratos inteligentes e aplicativos descentralizados. Seu valor de mercado também aumentou significativamente no espaço das criptomoedas.

Em 2015, a Linux Foundation lançou um projeto de blockchain de código aberto chamado Umbrella. Posteriormente, este projeto foi renomeado para Hyperledger e continua a ser uma iniciativa de desenvolvimento colaborativo de registros distribuídos até os dias de hoje. Sob a liderança de Brian Behlendorf, a Hyperledger busca facilitar a colaboração entre diferentes indústrias para o avanço da tecnologia blockchain e dos registros distribuídos.

O objetivo principal da Hyperledger é promover a adoção da tecnologia blockchain para melhorar o desempenho e a confiabilidade dos sistemas existentes, com vistas a suportar transações comerciais globais de forma mais eficiente. [38-39]

2.3.3 Fase 3 - Blockchain 3.0: Aplicações

A progressão da tecnologia blockchain não se limitam ao ethereum e ao bitcoin. Nos últimos anos, vários projetos emergiram, explorando todos os recursos da tecnologia blockchain e buscando resolver algumas das deficiências do bitcoin e do ethereum, ao mesmo tempo em que introduzem novos recursos para potencializar a blockchain.

Entre as novas aplicações da blockchain está a NEO, apresentada como a primeira blockchain com plataforma de código aberto e descentralizada lançada na China. Apesar da proibição das criptomoedas no país, a China permanece ativa no campo das inovações em blockchain. A NEO é conhecida como o "Ethereum chinês". Na corrida para impulsionar o desenvolvimento da Internet das Coisas, alguns desenvolvedores estão explorando a integração da tecnologia blockchain, resultando na plataforma chamada IoTA.

Esta criptomoeda é otimizada para o ecossistema da Internet das Coisas e se esforça para fornecer taxas de transação zero, juntamente com processos de verificação exclusivos. Além disso, aborda alguns dos problemas de escalabilidade associados à primeira geração da blockchain e ao bitcoin.

2.4 Como funciona a Blockchain

A tecnologia blockchain é um banco de dados devido à sua capacidade de fornecer um registro imutável e seguro de transações. Consiste em uma cadeia de blocos interconectados, onde cada bloco contém um registro de transações protegido por criptografia. Uma vez que as informações são registradas em um bloco que não podem ser alteradas retroativamente, garantindo assim a integridade dos dados, conforme pode ser visto na Figura 6.

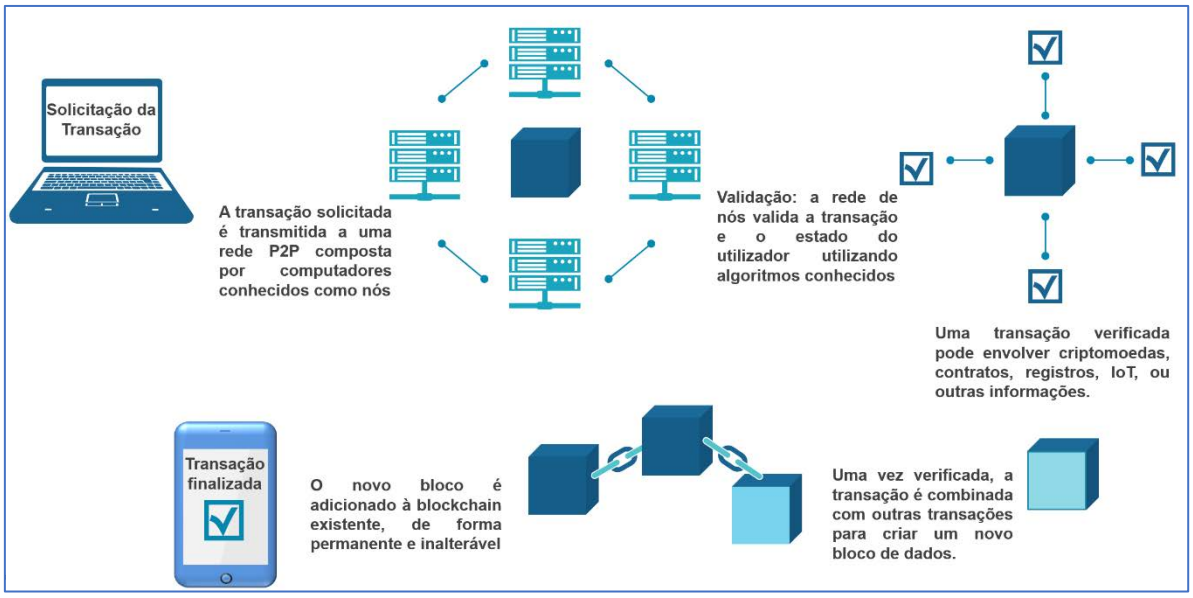

Figura 6 - Funcionamento da Blockchain
Fonte: Autoria própria, 2024.

Para viabilizar esta tecnologia, diversos elementos foram combinados de forma harmoniosa, estabelecendo as bases para aplicações descentralizadas. Estes elementos incluem [40-42]:

- Criptografia que garante a segurança do sistema e das aplicações. Entre os recursos mais utilizados estão as funções de hash criptográficas e as assinaturas digitais.

- Consenso distribuído o qual permite que participantes distribuídos coordenem suas ações para alcançar decisões compartilhadas, assegurando a consistência de seus estados e o progresso do sistema, mesmo em caso de falhas.

- Livro-razão distribuído é uma estrutura de dados imutável onde as transações são registradas e o estado global do sistema é replicado em todos os nós da rede P2P. Esta combinação de propriedades garante inovações significativas no desenvolvimento de novas soluções tecnológicas, incluindo as aplicações descentralizadas (DApps).

De acordo com [43], a blockchain possui uma arquitetura dividida em quatro camadas conforme a Figura 7 ilustra essa divisão:

(i) a camada de dados, que abrange os blocos, o armazenamento de dados e a estrutura de árvore utilizada;

(ii) Rede, que inclui a rede P2P e os mecanismos de comunicação;

(iii) Consenso, onde estão naturalmente os protocolos de consenso;

(iv) Aplicação, que abrange os contratos inteligentes, e as criptomoedas.

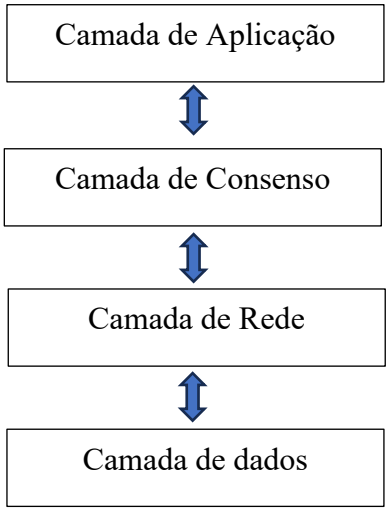

Figura 7 - Arquitetura da Blockchain em 4 camadas
Fonte: Autoria própria, 2024.

Na camada de dados, são definidas a estrutura, organização e armazenamento dos dados. Aspectos como desempenho e acessibilidade são essenciais para a rede blockchain, sendo que cada uma destas redes utiliza estruturas distintas. A rede Bitcoin usa a árvore de Merkle como forma de organizar e armazenar as informações, enquanto a Ethereum usa a Merkle Patricia Tree.

A camada de rede da blockchain é mantida e gerenciada de forma autônoma por uma rede P2P, composta por mineradores e usuários. Trata-se de uma estrutura descentralizada que não requer controle centralizado de entrada e saída, com tolerância a falhas. A comunicação e autenticação devem ser protegidas contra-ataques.

A camada de consenso é de fundamental importância em uma rede blockchain. Alcançar um consenso não é uma tarefa trivial, e muitos algoritmos foram propostos para esse fim [44]. Esses algoritmos ou mecanismos podem ser classificados como: PoW (Proof-of-Work, prova de trabalho) e PoS (Proof-of-Stake, prova de participação), juntamente com suas variantes; além de BFT (Bizantine Fault Tolerance, tolerância a falhas bizantinas) e suas variantes.

Por último, a camada de aplicação amplia as capacidades da blockchain e facilita para os desenvolvedores construir aplicativos blockchain através de contratos inteligentes, bem como por meio de sidechains e o uso de BaaS (Blockchain as a Service, Blockchain como um Serviço) [45], por exemplo. Nessa camada também estão as criptomoedas e uma variedade de aplicações, incluindo seguros, pagamentos, governança, entre outros. Há até mesmo a

possibilidade de integração com inteligência artificial, big data, computação quântica, IoT, entre outros.

Os componentes principais de um bloco consistem no cabeçalho e nas transações, sendo estas o conjunto de dados armazenados no bloco. O cabeçalho, por sua vez, contém vários campos, dos quais os mais essenciais para o seu funcionamento incluem: versão, hash do bloco anterior, raiz merkle, timestamp, dificuldade, nonce. Além desses, é fundamental compreender duas características do bloco: tamanho do bloco e hash do cabeçalho, que são registrados para identificar o bloco e sua posição na cadeia. Estes elementos serão delineados a seguir, para a compreensão adequada da blockchain. [46].

Tamanho do bloco: representa o tamanho em bytes das informações contidas no bloco.

Cabeçalho do bloco: contém informações que identificam o bloco atual.

Versão: indica a versão das diretrizes de validação dos blocos, ou seja, as normas a serem seguidas para alcançar consenso entre os blocos.

Timestamp: conhecido como o registro de data e hora do bloco. Essa marcação assegura a ordem cronológica de criação.

Raiz Merkle: é um tipo de hash utilizado para verificar a validade das transações contidas nos blocos sem a necessidade de verificar todas as informações das transações.

Nonce: é um valor utilizado como uma variável para ajustar a saída da função hash presente. Sua função reside em validar a atividade do minerador, assegurando que o bloco inserido satisfaça os critérios estabelecidos pela tecnologia blockchain.

Dificuldade: representa o número de bits 0 necessário à esquerda do hash do bloco para que atenda as exigências do sistema, é o nível de dificuldade de mineração da rede. Este é um valor que é modificado automaticamente pela rede para controlar a velocidade de geração de blocos;

Hash do bloco anterior: Cada bloco contém a informação da hash anterior, estabelecendo assim uma cadeia na qual a conexão entre eles é estabelecida. O hash anterior é fundamental para identificar o bloco predecessor. Atualmente, o hash utiliza um tamanho de 256 bits, baseado no algoritmo hash 256 desenvolvido pelo National Institute of Standards and Technology (NIST). O hash atual possibilita que o bloco sucessor tenha acesso ao bloco atual.

Transações: São conjuntos de dados que registram as interações, como a troca de valores, entre os usuários de uma rede que utiliza a blockchain. Cada interação engloba uma assinatura digital da mensagem enviada pelo remetente ao endereço do destinatário, juntamente

com entradas e saídas que detalham os valores transacionados, especialmente em aplicações envolvendo criptomoedas [47].

Na figura 8 mostra a estrutura interna de um bloco da blockchain.

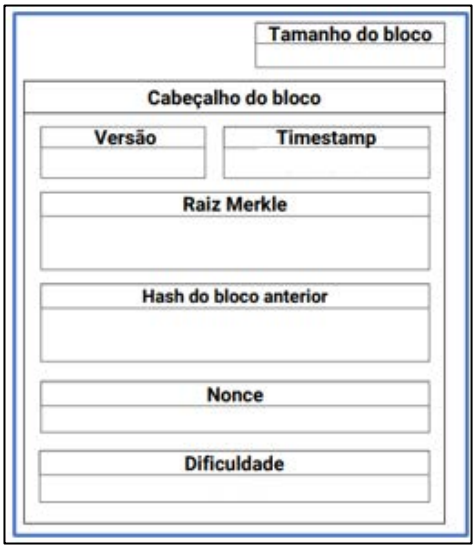

Figura 8 - Estrutura interna de um bloco da Blockchain
Fonte: Watanabe, 2016.

Mineração: A mineração desempenha o papel fundamental de adicionar um novo bloco a blockchain. A terminologia "minerador" teve origem com bitcoin, principalmente devido ao seu contexto de transações financeiras. Durante o processo de mineração, os mineradores incorporam as transações em um bloco específico e produzem um cabeçalho válido (hash) para esse conjunto de transações. Para gerar esse cabeçalho, os mineradores precisam calcular a árvore hash, validar a dificuldade estipulada, incorporar o timestamp e conduzir uma sequência de cálculos para descobrir um nonce que atenda aos requisitos da dificuldade vigente. Estas características discorreram sobre a relevância da dificuldade, abordando como ela se adapta automaticamente.

O processo principal da blockchain opera ao reunir as transações transmitidas pela rede por meio de broadcast. Essas transações geralmente residem em um pool de transações, de onde um nó seleciona algumas para verificação e inclusão em um novo bloco. Conforme descrito por [47], se uma mensagem (transação) for validada, ela é armazenada no bloco juntamente com as demais. Quando o nó atinge o critério estabelecido para o número máximo de transações a serem incluídas, procede ao cálculo do valor hash de todas as transações. E com isso, é formada a Árvore de Merkle com base nesses valores será inserido no cabeçalho do bloco.

2.5 Tipos de Blockchain

A blockchain pública é a primeira variante desse tipo de tecnologia, e, como o nome sugere, refere-se a blockchains acessíveis ao público em geral. Esses blockchains permitem que qualquer pessoa participe, seja como usuário, minerador ou administrador de um nó [48]. A operação da rede é totalmente aberta e transparente, com todos os dados disponíveis desde o início, sem restrições [49]. Não há entidades centralizadas; as redes públicas são totalmente descentralizadas, e não existe uma autoridade central que regule seu funcionamento. Exemplos notáveis de blockchains públicos incluem Bitcoin BSV, Ethereum e Dash.

A evolução da tecnologia blockchain fez com que, muitas empresas se interessassem por ela, dando origem a soluções de blockchain privadas [50]. Este tipo de soluções tem os mesmos elementos de um blockchain público, mas ao contrário dos blockchains públicos, os blockchains privados dependem de um sistema central que controla todas as ações associadas ao blockchain. Esta unidade central controla o acesso aos utilizadores e as suas funções e permissões dentro do blockchain. Esse tipo de blockchain é frequentemente utilizado para atender a interesses corporativos, nos quais as características se alinham adequadamente a esse contexto. É exemplo de blockchain privado o Hyperledger.

Para assegurar os princípios da segurança da informação, emprega-se uma arquitetura de rede descentralizada de computadores do tipo peer-to-peer (P2P) na construção de um blockchain [51]. Uma rede P2P é constituída por nós interligados que atuam tanto como clientes quanto como servidores, configurando assim uma rede distribuída.

Em uma configuração P2P na qual cada nó da rede mantém uma cópia da cadeia de blocos. Nesse contexto, caso ocorra um ataque a um nó que resulte na alteração de um bloco da blockchain, como uma transação, é implementado um protocolo de consenso capaz de restaurar o estado anterior da blockchain antes do ataque.

Com o intuito de reforçar a segurança e confiabilidade de uma rede blockchain, é implementado o mecanismo de consenso, um algoritmo projetado para ampliar a tolerância a falhas. Em outras palavras, esse mecanismo previne a existência de blockchains divergentes entre os nós da rede e é empregado na validação dos dados antes de sua inclusão no blockchain [52].

A finalidade de um algoritmo de consenso na blockchain é assegurar que todos os nós envolvidos estejam de acordo com as transações efetuadas na rede, resultando em um histórico serializado na forma de uma blockchain.

Existem inúmeros algoritmos de consenso para blockchain [53], os dois mais conhecidos são:

Proof of Work (PoW) ou prova de trabalho que representa um tipo de mecanismo de consenso utilizado na mineração das criptomoedas mais renomadas, como Ethereum e bitcoin. Em termos simples, trata-se de um algoritmo que gera dados utilizados para validar a legitimidade da criptomoeda.

Dessa forma, o PoW viabiliza o consenso, a aprovação das transações nas criptomoedas, e assegura a integridade dos processos, prevenindo problemas como o gasto duplo que é a situação que ocorre quando o usuário tenta gastar dinheiro duas vezes pela mesma criptomoeda.

Para que uma criptomoeda seja aceita após a fase de mineração, os mineradores precisam concluir com sucesso o Proof of Work, realizando a verificação de todas as transações nos blocos.

Durante o processo de mineração, um número aleatório chamado nonce é gerado e adicionado ao final de cada bloco, juntamente com o hash. Esse procedimento não apenas fortalece a segurança, mas também representa uma oportunidade de lucro.

O minerador tem a responsabilidade de buscar e encontrar o nonce. Contudo, esse é um procedimento de tentativa e erro, no qual a máquina realiza uma série de cálculos até encontrar o número correto, que é então adicionado ao bloco. Este bloco é composto por: hash; nonce e informação aprovada pelo PoW.

Este método envolve a busca pelo valor de hash do cabeçalho do bloco, de modo a cumprir os parâmetros estabelecidos pela dificuldade configurada. A essência desse protocolo reside na necessidade de atender à dificuldade definida pela rede blockchain para a criação de um novo bloco. Esse parâmetro determina a quantidade de zeros que o hash deve conter à esquerda.

Proof of Stake (PoS) ou Prova de Participação: Este método envolve a seleção do nó pelo minerador o qual terá a capacidade de criar um novo bloco. Geralmente, é realizado um sorteio em que a probabilidade de vencer é proporcional à quantidade de blocos que o nó já contribuiu para a rede, refletindo a confiabilidade desse nó. O procedimento opera da seguinte maneira os validadores comprometem uma porção de suas criptomoedas como uma forma de ingressar na rede. Posteriormente, eles iniciam o processo de validação dos blocos. Esse processo envolve os validadores apostando caso identifiquem um bloco que consideram adequado para ser adicionado à rede. Dessa forma, todos os validadores recebem recompensas

proporcionais às suas contribuições. No desfecho, um validador é selecionado para gerar um novo bloco, sendo essa escolha baseada em sua participação na rede.

PoW e PoS por serem os dois tipos mais populares de mecanismos de consenso, eles desempenham funções nas redes, embora de maneiras distintas. O Proof of Work foi adotado nas primeiras criptomoedas, como o bitcoin, enquanto o Proof of Stake foi a escolha predominante para as altcoins, ou seja, as moedas alternativas.

A principal diferença entre esses mecanismos de consenso reside no consumo de energia. Enquanto o PoW exige que os usuários resolvam problemas matemáticos complexos, o PoS não necessita desse tipo de resolução, tornando-se uma abordagem mais sustentável em termos de validação [54].

Essa eficiência decorre do fato de que o PoS não demanda equipamentos complexos e robustos por parte dos usuários para a implementação do consenso, contribuindo assim para a redução do consumo de energia. A tabela 1 mostra um comparativo entre os algoritmos de consensos Pow e PoS.

Tabela 1 - Comparação entre PoW e PoS

Aspecto	**Proof of Work (PoW)**	**Proof of Stake (PoS)**
Segurança	**Alta**, devido à necessidade de poder computacional para encontrar sequências de hashes específicos.	**Moderada**, baseada na quantidade de criptomoeda apostada como garantia.
Eficiência Energética	**Baixa**, pois requer grande quantidade de energia para alimentar o poder computacional necessário.	**Alta**, pois não requer o mesmo nível de poder computacional, sendo menos intensivo em energia.
Adoção	Bitcoin e BSV.	Ganhando mais adoção, com projetos como Tezos, Cardano, Polkadot e Ethereum 2.0.

2.5.1 Bitcoin (BTC)

Em 31 de outubro de 2008, um indivíduo ou grupo anônimo identificado como Satoshi Nakamoto divulgou um artigo intitulado “A peer-to-peer electronic cash system ".

Esse documento inovador, que teve um impacto global, introduziu a arquitetura para a criptomoeda descentralizada de código aberto juntamente com a tecnologia revolucionária blockchain que a viabiliza. A invenção do bitcoin é revolucionária, uma vez que pela primeira vez soluciona o problema do gasto duplo sem depender de uma entidade intermediária.

O bitcoin compartilha o essencial registro histórico com todos os usuários do sistema por meio de uma rede ponto a ponto, composta por milhares de usuários, tornando-se, assim, o próprio intermediário [55].

O bitcoin utiliza um esquema de hash chamado Secure Hash Algorithm (SHA-256), que é apenas uma das várias funções de hash empregadas por diversas blockchains em funcionamento. Para efetivar transações, o detentor de um endereço utiliza a chave privada correspondente para autorizar as operações. Sua blockchain permite um número predefinido de transações, sendo que a menor transação possui o tamanho de 83 bytes, o que possibilitaria aproximadamente 10.000 transações por bloco. Uma transação comum possui cerca de 250 bytes, resultando em aproximadamente 4.000 transações. O número de transações que podem ser incluídas em um único bloco depende do limite de tamanho estabelecido para um bloco. Até 2019, o limite de tamanho para um bloco de Bitcoin era de dois megabytes. Uma característica significativa é que o tempo médio para a confirmação de bloco no Bitcoin é de 10 minutos, e o fornecimento máximo é de 21 milhões de moedas.

2.5.2 Bitcoin Satoshi Vision (BSV)

O Bitcoin SV, "Bitcoin Satoshi Vison (BSV)", é uma criptomoeda originada em 2018 como resultado de um fork (bifurcação) do Bitcoin Cash. Seu desenvolvimento teve como propósito restaurar o protocolo original do bitcoin concebido por Satoshi Nakamoto. O BSV busca aprimorar a escalabilidade e a capacidade de processamento em relação ao seu precursor, refletindo em blocos de maior tamanho e transações mais rápidas.

Ao longo do tempo, usuários e desenvolvedores de ativos digitais descobrem aspectos que podem ser modificados ou atualizados nos protocolos, blockchains e até mesmo nas criptomoedas, assim como ocorre com dispositivos móveis que requerem atualizações regulares.

No universo das criptomoedas, esse processo não é diferente. Essas modificações são denominadas "fork", representando bifurcações do sistema original. Quando alterações são

implementadas no protocolo ou na cadeia (chain), a bifurcação é referida como "soft fork", pois é reversível e compatível com a versão original.

Por outro lado, se ocorrerem muitas mudanças que comprometam o funcionamento da cadeia, ocorre uma bifurcação mais substancial conhecida como "hard fork". Esta atua como uma espécie de cadeia paralela e não é compatível com a versão original, sendo irrecuperável uma vez efetivada [56].

O Bitcoin SV (BSV) originou-se como um hard fork do Bitcoin Cash (BCH), que, por sua vez, é um hard fork do Bitcoin (BTC). A versão Bitcoin Cash (BCH) buscou aumentar o tamanho do bloco de 1 MB para 32 MB, visando incrementar a capacidade de transações.

Por sua vez, a moeda BSV apresenta blocos de 128 MB, conferindo ainda maior escalabilidade às operações. De acordo com o criador, Craig Wright, essa abordagem busca se aproximar do conceito que Satoshi Nakamoto tinha ao criar o Bitcoin, visando mais transações e taxas mais baixas.

Como o BSV é um hard fork do BCH, a abordagem de mineração da Bitcoin SV permanece a mesma: Proof of Work (PoW). Consequentemente, computadores e máquinas especializadas devem resolver cálculos complexos para criar um bloco na blockchain, sendo recompensados com um token.

No contexto da BSV, que processa mais informações por segundo do que o bitcoin, os mineradores PoW não necessitam dedicar longas horas com os computadores ligados para efetuar a mineração de uma moeda. Isso implica que, nesse cenário, é consumida menos energia para a mineração deste hard fork do Bitcoin.

2.5.3 Etherum (ETH)

O Ethereum teve sua concepção em 2013 por Vitalik Buterin e colaboradores um programador canadense anteriormente envolvido com o Bitcoin. Lançado em 2015, o Ethereum é a segunda maior criptomoeda em valor de mercado, logo atrás do Bitcoin. Conforme a documentação oficial do Ethereum, a plataforma é descrita como uma plataforma blockchain aberta que permite que programadores construa contratos inteligentes e várias aplicações descentralizdas (Dapp) executados na tecnologia blockchain [57]. O Ethereum emite a sua própria criptomoeda, o Ether (ETH).

O Ethereum adota a tecnologia blockchain de maneira semelhante ao Bitcoin. A criptomoeda ETH pode ser empregada para realizar pagamentos e, adicionalmente, permite a criação de contratos inteligentes independentes de intervenção de terceiros.

Principais características do Ethereum:

Contratos Inteligentes: Os contratos inteligentes são programas autoexecutáveis que rodam na blockchain Ethereum. Eles podem ser usados para automatizar uma ampla gama de transações e processos, incluindo pagamentos, votações, registros de propriedade e muito mais. Os contratos inteligentes são escritos em uma linguagem de programação Turing-completa chamada Solidity.

Aplicativos Descentralizados (dApps): O Ethereum permite o desenvolvimento de dApps, que são aplicativos que funcionam na blockchain e são executados de forma descentralizada, sem a necessidade de um servidor centralizado. Isso os torna imunes a censura e falhas de infraestrutura.

Token ERC-20: O Ethereum introduziu o padrão ERC-20, que define uma interface para contratos inteligentes que representam tokens fungíveis. Isso possibilitou o lançamento de uma infinidade de tokens na blockchain Ethereum, impulsionando o crescimento do ecossistema de criptomoedas e tokens.

Ethereum Virtual Machine (EVM): A EVM é uma máquina virtual que executa os contratos inteligentes na blockchain Ethereum. Ela fornece um ambiente de execução isolado e seguro para garantir que os contratos inteligentes sejam executados de maneira previsível e segura.

Proof of Stake (PoS): O Ethereum está migrando de um algoritmo de consenso baseado em Proof of Work (PoW) para Proof of Stake (PoS) com a implementação do Ethereum 2.0. Isso visa aumentar a eficiência energética e escalabilidade da rede, permitindo aos detentores de Ether apostar suas moedas para validar transações e garantir a segurança da rede.

A blockchain mantém um histórico completo de todas as transações realizadas. A BSV Blockchain realiza em torno 50k transações por segundo enquanto a Etherum Blockchain realiza em torno de 14,5 transações por segundo.

A tabela 2 permite uma compreensão mais completa sobre a natureza das diferentes redes blockchain e pode ajudar na seleção da melhor opção para determinadas aplicações ou necessidades específicas.

Tabela 2 - Comparação entre as diferentes Blockchains

Blockchain	Propósito	Segurança	Escalabilidade	Custo	TPS	Algoritmo	Tipo	Ecossistema
Bitcoin (BTC)	Moeda digital P2P para transações	Altamente seguro devido ao uso extensivo de prova de trabalho	Limitado em TPS, resultando em tempos de confirmação mais longos	Taxas de transação podem ser altas durante períodos de congestionamento	7 TPS	Prova de Trabalho (PoW)	Pública	Vasto ecossistema de desenvolvimento e adoção
Ethereum (ETH)	Plataforma para contratos inteligentes e dApps	Menos seguro devido a ataques de 51% e problemas de escalabilidade	Limitado em TPS, com soluções em desenvolvimento como Ethereum 2.0	Taxas de transação podem ser altas durante períodos de congestionamento	21 TPS	Prova de Trabalho (PoW), migração para Prova de Participação (PoS) com Ethereum 2.0	Pública	Um dos maiores ecossistemas de dApps e tokens
Bitcoin Cash (BCH)	Oferecer uma blockchain mais escalável para pagamentos	Segurança semelhante ao Bitcoin, mas com uma abordagem diferente para escalabilidade	Maior capacidade de TPS em comparação com o Bitcoin original	Taxas de transação geralmente mais baixas do que o Bitcoin	60 TPS	Prova de Trabalho (PoW)	Pública	Menos desenvolvido em comparação com Bitcoin e Ethereum, mas em crescimento
Bitcoin SV (BSV)	Seguir a visão original do Bitcoin como um sistema de dinheiro eletrônico escalável	Herda a segurança do Bitcoin, com maior escalabilidade	Capacidade teórica muito maior de TPS do que o Bitcoin original	Taxas de transação geralmente mais baixas do que o Bitcoin	50KTPS	Prova de Trabalho (PoW)	Pública	Ainda em desenvolvimento, com foco em aplicações empresariais e escalabilidade

3 MATERIAIS E MÉTODOS

3.1 Metodologia

A metodologia empregada neste estudo foi estruturada em cinco etapas distintas:

Revisão da Literatura: Inicialmente, realizou-se um levantamento na literatura existente para identificar trabalhos semelhantes e adquirir um entendimento aprofundado dos principais conceitos relacionados ao tema da pesquisa.

Referencial Teórico: Com base nos resultados da revisão da literatura, foi desenvolvido um referencial teórico que fundamentou o estudo, fornecendo uma base conceitual sólida para a análise e discussão dos resultados. Foram abordados o funcionamento básico da Blockchain e a teoria do Bitcoin, destacando aspectos técnicos que compõem a essência da tecnologia. Isso incluiu uma explanação sobre Funções de Hash, que são algoritmos matemáticos utilizados para garantir a integridade dos dados na Blockchain, além de assinaturas digitais, que são métodos criptográficos empregados para verificar a autenticidade das transações.

Além disso, foram discutidos os princípios das árvores de merkle, uma estrutura de dados utilizada para garantir a eficiência e a segurança na verificação das transações na blockchain. No contexto da arquitetura de computação, foram explorados conceitos como o protocolo de consenso, que define as regras para validar novos blocos na cadeia, e as redes peer-to-peer, que possibilitam a comunicação direta entre os nós da rede sem a necessidade de um servidor centralizado.

Esses elementos fundamentais foram analisados para fornecer uma compreensão abrangente sobre o funcionamento da blockchain e sua aplicação no contexto do Bitcoin, preparando o ambiente para a discussão mais aprofundada sobre a implementação e os desafios associados à utilização dessa tecnologia.

Seleção do modelo de rede Blockchain: Nesta etapa, foram avaliados e comparados diferentes modelos de rede Blockchain disponíveis, levando em consideração suas características, arquiteturas e aplicabilidades específicas ao contexto da pesquisa.

Foi adotado o modelo da rede Blockchain BSV. Esta rede tem se destacado por sua abordagem inovadora na busca por soluções que visam escalabilidade e aumento da capacidade de gerenciamento de grandes volumes de dados. Notavelmente, na área do IoT, a BSV tem

recebido reconhecimento e adoção devido ao seu compromisso com a privacidade e segurança das informações.

Seleção do protocolo de consenso: Foi realizada a escolha do protocolo de consenso mais adequado às necessidades e objetivos do estudo. Diversos protocolos de consenso foram considerados, como o Proof of Work (PoW), Proof of Stake (PoS), entre outros, com uma análise cuidadosa de suas vantagens e limitações.

O protocolo de consenso é essencial em uma estrutura descentralizada, onde a confiança entre os pares é fundamental. Ele é aplicado para estabelecer confiança na validação dos blocos que serão adicionados à cadeia. No contexto do Bitcoin, o protocolo de Prova de Trabalho (Proof of Work) é utilizado, caracterizando-se pela competição entre os nós para resolver problemas matemáticos complexos.

Essa competição envolve a resolução de problemas computacionais intensivos, garantindo que os nós demonstrem uma quantidade significativa de trabalho realizado para validar transações e adicionar novos blocos à blockchain. Esse processo é fundamental para manter a segurança e a integridade da rede.

Portanto, o protocolo de Prova de Trabalho desempenha um papel crucial no Bitcoin, assegurando a confiabilidade e a segurança da rede em um ambiente descentralizado, onde a confiança entre os participantes é estabelecida por meio do trabalho computacional realizado para validar transações.

Seleção do ambiente de desenvolvimento: Por fim, selecionou-se o ambiente de desenvolvimento que melhor se adequava para à implementação do modelo de rede Blockchain BSV. Critérios como compatibilidade, recursos oferecidos e facilidade de uso foram considerados nesta seleção.

O ambiente escolhido para o desenvolvimento da aplicação foi o sistema do Android Studio, o qual é construído sobre a base do IntelliJ IDEA, uma popular IDE de desenvolvimento Java, e é específico para desenvolvimento de aplicativos android. Ele fornece uma variedade de ferramentas e recursos para facilitar o desenvolvimento de aplicativos para integrar com tecnologia blockchain na rede BSV. Portanto, é uma plataforma de desenvolvimento que facilita a interação entre o protocolo básico do Bitcoin e os desenvolvedores de aplicações, fornecendo assim uma camada de implementação.

Essas etapas foram essenciais para guiar o desenvolvimento da pesquisa, garantindo uma abordagem sistemática e fundamentada na escolha dos elementos chave para a realização do estudo.

3.2 Composição inicial e básica do sistema

A composição inicial e básica do sistema consiste em dois microcontroladores arduino uno (M1 e M2), dois smartphones android (A1 e A2), conforme mostrado na Figura 9. M1 e M2 se conectam com A1 e A2, respectivamente, via bluetooth para comunicar o estado dos sensores que monitoram para receber instruções para qualquer tipo de tarefa que devem executar.

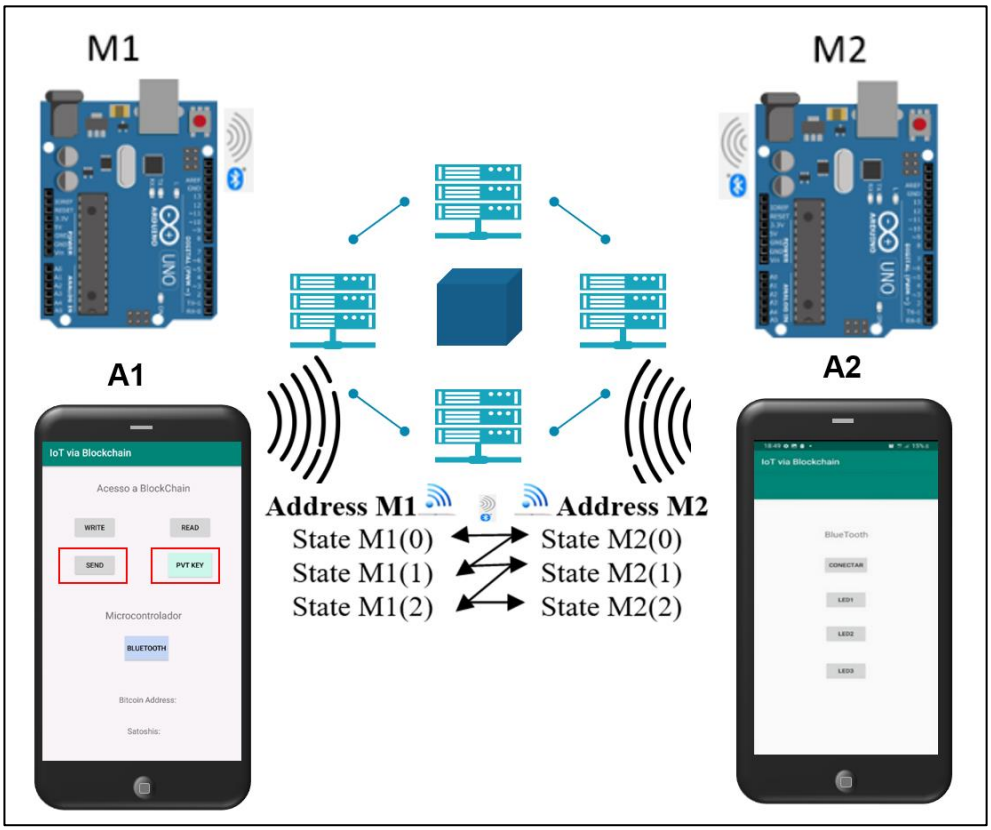

Figura 9 - Interconexão entre dispositivos do sistema
Fonte: Autoria própria, 2024.

O sistema funciona da seguinte forma: M1 e M2 se conectam com seus respectivos dispositivos Android, A1 e A2, que possibilitam o acesso à Blockchain. Cada microcontrolador

possui sua própria chave privada que permite escrever e armazenar informações em um endereço específico na blockchain.

Na aplicação aqui apresentada, cada microcontrolador permanece atento ao endereço de seu par para conhecer as instruções da próxima tarefa a ser realizada. O estado dos sensores em M1 determina as tarefas subsequentes para M2, e vice-versa. Após concluir sua tarefa, cada microcontrolador lê o estado de seus sensores e informa à blockchain, e o próximo ciclo de tarefas é determinado. Essa troca mútua de informações permite que os microcontroladores sincronizem suas ações com base nos dados dos sensores, facilitando operações coordenadas entre os dois dispositivos.

A figura 10 mostra um esquema simples de como o processo ocorre. Suponha que, no início, M1 transmite seu estado para a blockchain, de modo que a última transação no Endereço 1 conterá as informações Estado M1(0). Agora, M1 continua ouvindo o Endereço M2 para saber o que fazer em seguida. Como M2 está ouvindo o Endereço M1, percebe uma nova transação contendo as informações Estado M1(0). Esses dados trazem as instruções da próxima tarefa que deve ser executada. Portanto, M2 realiza as tarefas necessárias, lê o estado de seus sensores e transmite para a blockchain uma nova transação para o Endereço M2 contendo as informações Estado M2(0). Como M1 está ouvindo o Endereço M2, percebe uma nova transação e verifica que há uma nova instrução a ser executada, e o ciclo se repete. Dessa forma, ambas as redes de sensores se mantêm sincronizadas por meio da blockchain.

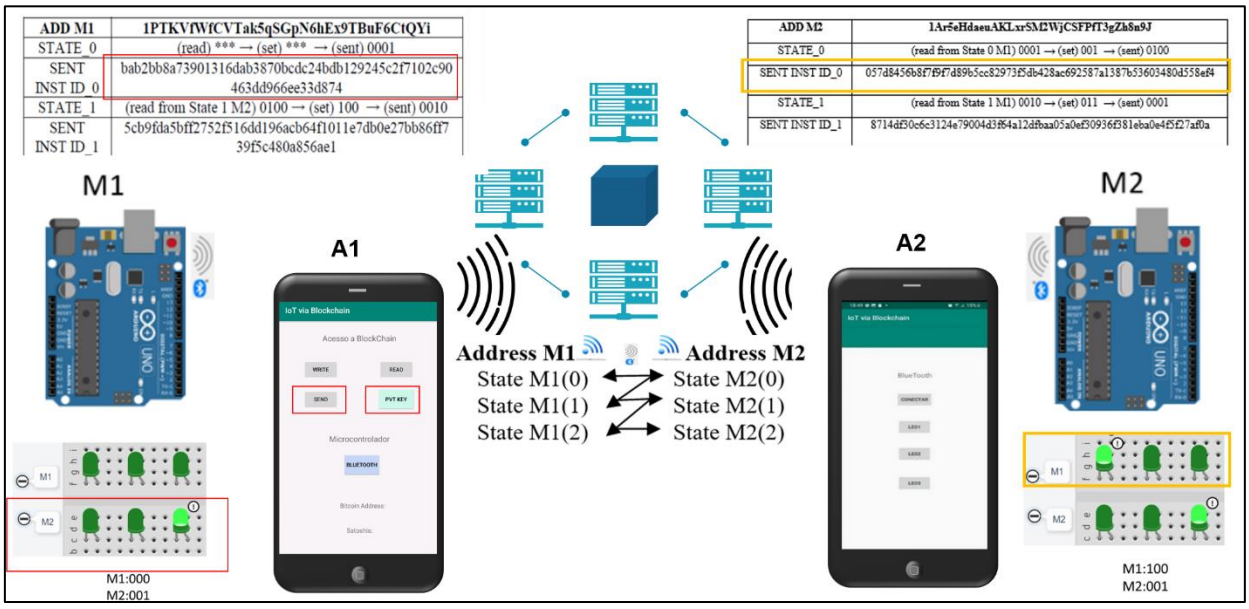

Figura 10 - Estados armazenados na Blockchain
Fonte: Autoria própria, 2024.

A blockchain BSV oferece não apenas recursos de escalabilidade, mas também a capacidade de incluir tipos arbitrários de dados dentro de transações. Isso significa que qualquer tipo de dado pode ser inserido em uma transação e posteriormente recuperado usando o ID exclusivo da transação por meio de qualquer serviço de recuperação acessível dentro da rede. Para ilustrar esse conceito, um exemplo de recuperação de dados é mostrado na Figura 11, destacando o processo contínuo de acesso à informação desejada.

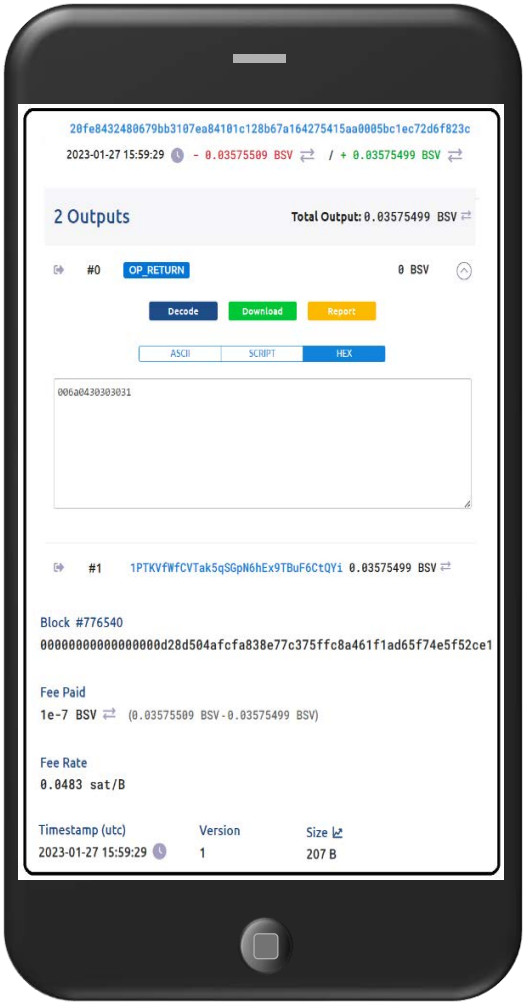

Figura 11 - Exemplo de dados do sistema proposto
Fonte: Autoria própria, 2024.

Para desenvolver uma API que atenda às metas de interoperabilidade é utilizada a arquitetura, o qual é seguido uma abordagem modular e escalável. A Figura 12 mostra a arquitetura proposta que visa uma API para integrar a tecnologia blockchain com o sensor de temperatura DHT22.

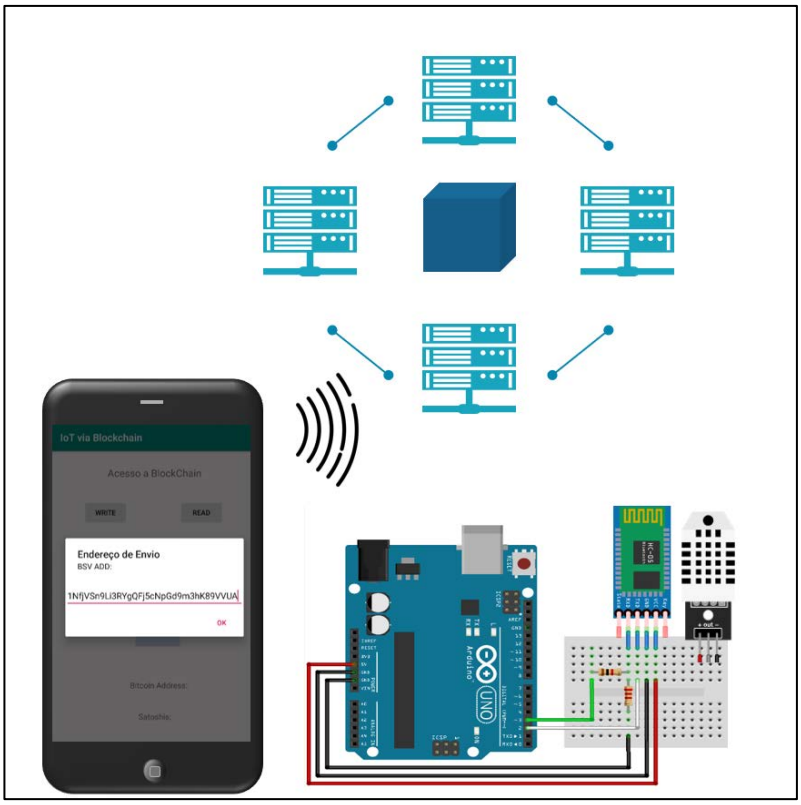

Figura 12 - Arquitetura do sistema da API
Fonte: Autoria própria, 2024.

3.3 Placa Arduino Uno

O arduino é uma plataforma de prototipagem eletrônica de código aberto, conforme visto na Figura 13, composta por uma placa única.

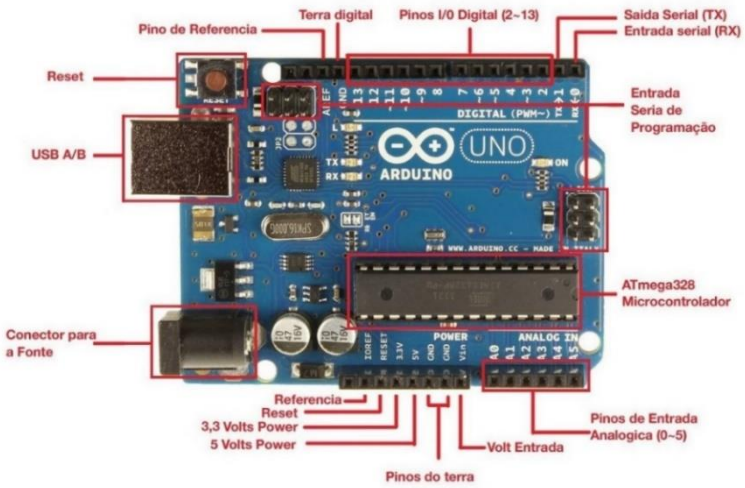

Figura 13 - Esquema de entradas e saídas
Fonte: Souza, 2016.

É projetado com um microcontrolador baseado no chip ATmega328, responsável pelo processamento das entradas e saídas. Os pinos de E/S permitem a conexão de dispositivos externos, com algumas portas digitais capazes de operar como saídas PWM, além de entradas analógicas disponíveis. O arduino oferece suporte embutido para E/S e utiliza uma linguagem de programação padrão. A placa é equipada com um cristal oscilador de 16MHz para sincronização de tempo, uma conexão USB para comunicação com o computador e uma entrada de alimentação para fornecer energia, uma conexão ICSP (In-Circuit Serial Programming) e um botão de reset [58].

3.4 Módulo de Temperatura DHT 22 para o arduino

O sensor de temperatura e umidade DHT22, Figura 14, foi integrado ao arduino para possibilitar a leitura precisa das condições ambientais. Esse sensor, conectado ao arduino, permite que o dispositivo obtenha informações atualizadas sobre a temperatura e umidade do ambiente em que está instalado. Esses dados são então utilizados para diversas finalidades, como controle de ambiente, monitoramento climático ou até mesmo para acionar dispositivos de refrigeração ou aquecimento quando necessário. A integração do DHT22 com o arduino oferece uma solução versátil e acessível para projetos que demandam o monitoramento desses parâmetros ambientais.

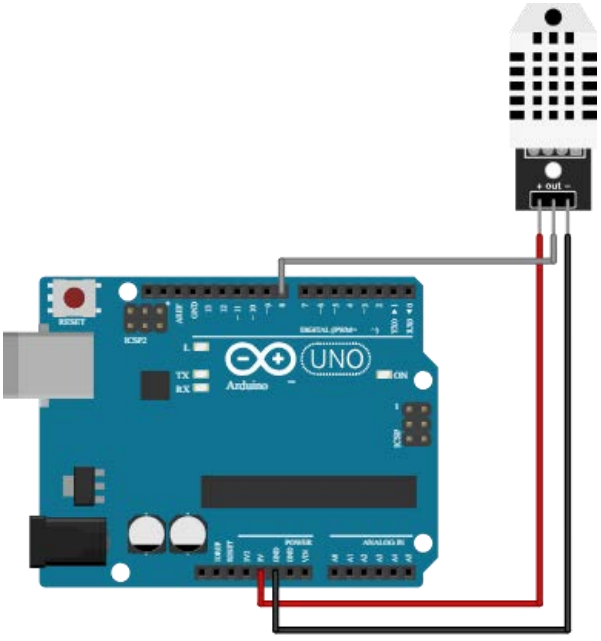

Figura 14 - Módulo DHT22
Fonte: Autoria própria, 2024.

3.5 Módulo de Comunicação Bluetooth

Bluetooth é o nome dado a um protocolo de comunicação sem fio, que utiliza frequências de 2,402 GHz a 2,48 GHz, lançado em 1999 na sua versão 1.0, com o intuito de substituir alguns usos da transmissão de dados utilizando cabo. A comunicação bluetooth é voltada para uma distância de curto alcance, chegando em alguns casos a transmitir dados entre dispositivos situados à 100m de distância. O módulo HC-05 integra componentes que permitem utilizar a comunicação bluetooth, tanto em dispositivos mestres, bem como dispositivos escravos [59].

O módulo bluetooth HC-05 é o módulo mestre conforme a Figura 15, o qual apresenta 6 pinos que permitem realizar a conexão. O nível de tensão nos pinos de transmissão de dados deve ser observado, já que no módulo HC- 05 operam em 3.3V, enquanto no arduino operam em 5V [60].

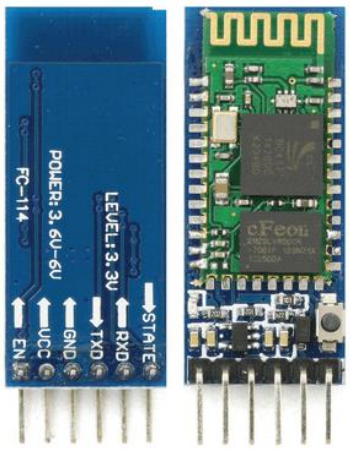

Figura 15 - Módulo bluetooth HC-05
Fonte: Fetzner, 2015.

Este módulo gerencia a comunicação bluetooth entre o arduino e o dispositivo android. Sendo desenvolvido como parte do aplicativo android, utilizando as APIs bluetooth disponíveis no pacote Android SDK. O modelo HC-05 possui algumas variações no mercado, podendo apresentar o controle do pino KEY através de um botão na placa ou um pino externo. Interpreta como comandos os dados recebidos no período de 1 segundo. Portanto, digitar caractere por caractere é praticamente impossível neste curto espaço de tempo.

Utilizamos os pinos 2 e 3 para a comunicação serial com o Arduino UNO. Em função da placa escolhida, esses pinos podem ser incompatíveis com a comunicação Software Serial. Como o nível lógico do módulo Bluetooth é 3,3V, recomendamos usar um divisor de tensão para o pino RX do módulo para reduzir a tensão de 5V do Arduino. (1k de resistência entre pin3 e Rx; 2k Ohm entre Rx e GND). Conforme abordado no esquema de ligação da Figura 16.

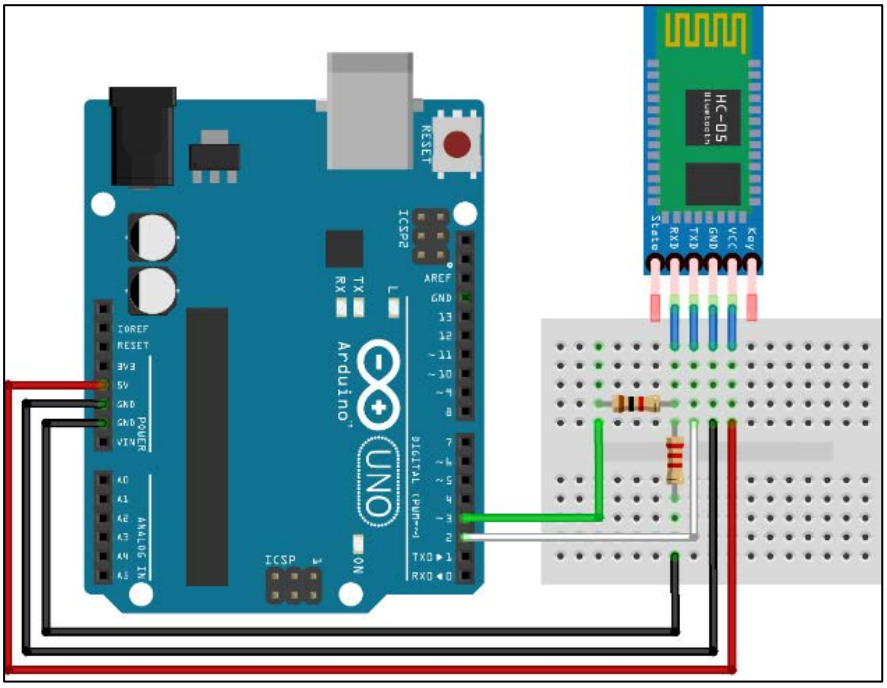

Figura 16 - Esquema de ligações para o Arduino.
Fonte: Autoria própria, 2024.

Assim que o módulo estiver alimentado, seu LED piscará. Se ele continuar piscando rápido significa que o módulo não está em comunicação com nenhum dispositivo. Caso ele permaneça ligado isso significa que o módulo está conectado a outro dispositivo.

3.6 Seleção do Ambiente do Arduino Uno

Para programar o arduino utilizamos o aplicativo IDE, figura 17. A programação do arduino dá-se através de uma linguagem própria, baseada em linguagem C [58-59].

A programação e interação em tempo real são realizadas através dessa interface de programação IDE, que pode ser escrita em várias linguagens, sendo a mais utilizada a própria linguagem do arduino.

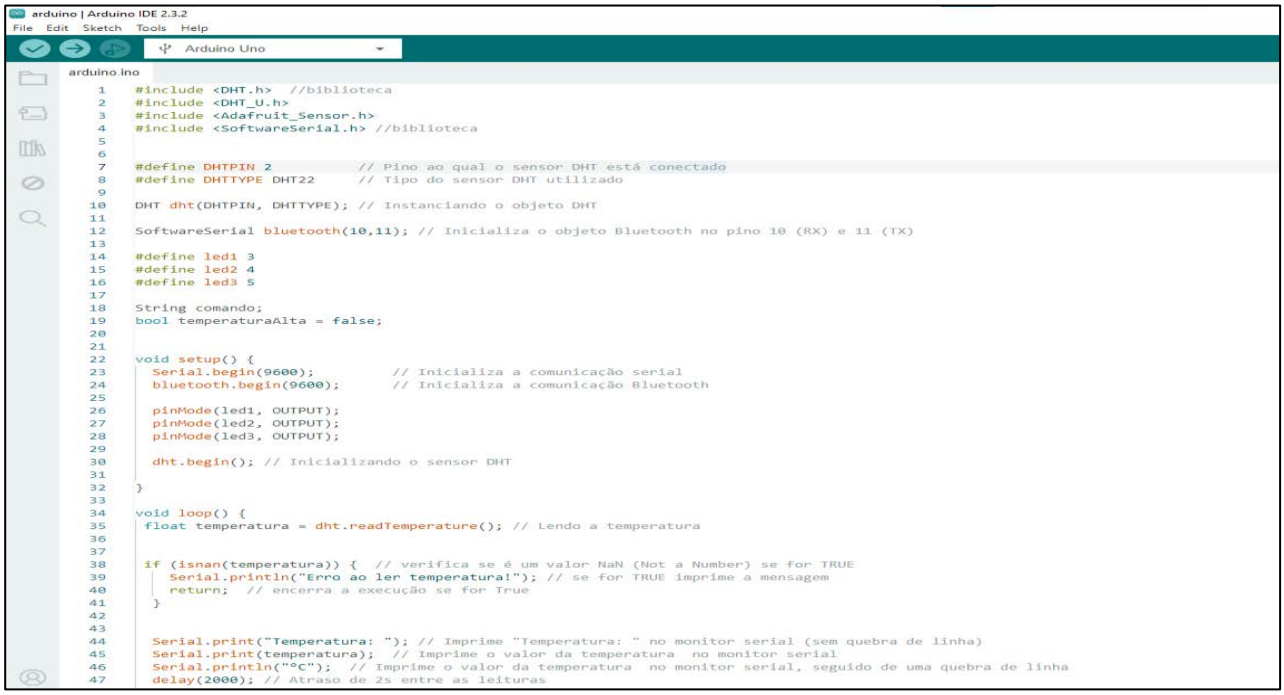

Figura 17 - IDE do Arduino
Fonte: Autoria própria, 2024.

Antes de programar é importante configurar o aplicativo IDE para o modelo de placa a ser utilizada, este estará pronto para receber o código da programação. Quando a programação estiver completa basta clicar em Upload para finalizar e carregar o programa no Arduino. O IDE faz uma compilação do código, verifica se não há erros de comandos na programação e caso haja ele cancela o upload e gera um aviso na tela, do contrário carrega o código compilado no arduino.

Sobre o protocolo bluetooth e o módulo HC-05 que junto com o arduino utiliza esse meio de comunicação para transmitir dados entre dispositivos sem utilizar fios. O arduino pode comunicar-se com outros dispositivos (smartphone, computador ou algum outro microcontrolador) via conexão bluetooth utilizando um módulo HC-05. Desse modo, é possível conectar a sua placa arduino a outros sistemas, para enviar e receber dados. A comunicação por bluetooth possibilita por meio de uma aplicação para smartphone, exibir as medidas de um sensor no seu computador ou ainda permitir que outros dispositivos comuniquem-se entre si.

3.7 Seleção do ambiente da API para o dispositivo Android

A API recebe os dados de temperatura transmitidos pelo arduino via bluetooth conforme visto na Figura 18. Foi implementado como parte do aplicativo no android que processa os dados recebidos e fornece uma interface para que o dispositivo envie os dados de temperatura para o blockchain.

Foi desenvolvido como parte do backend, que utiliza uma biblioteca compatível com a blockchain BSV para criar transações e gravar dados na blockchain.

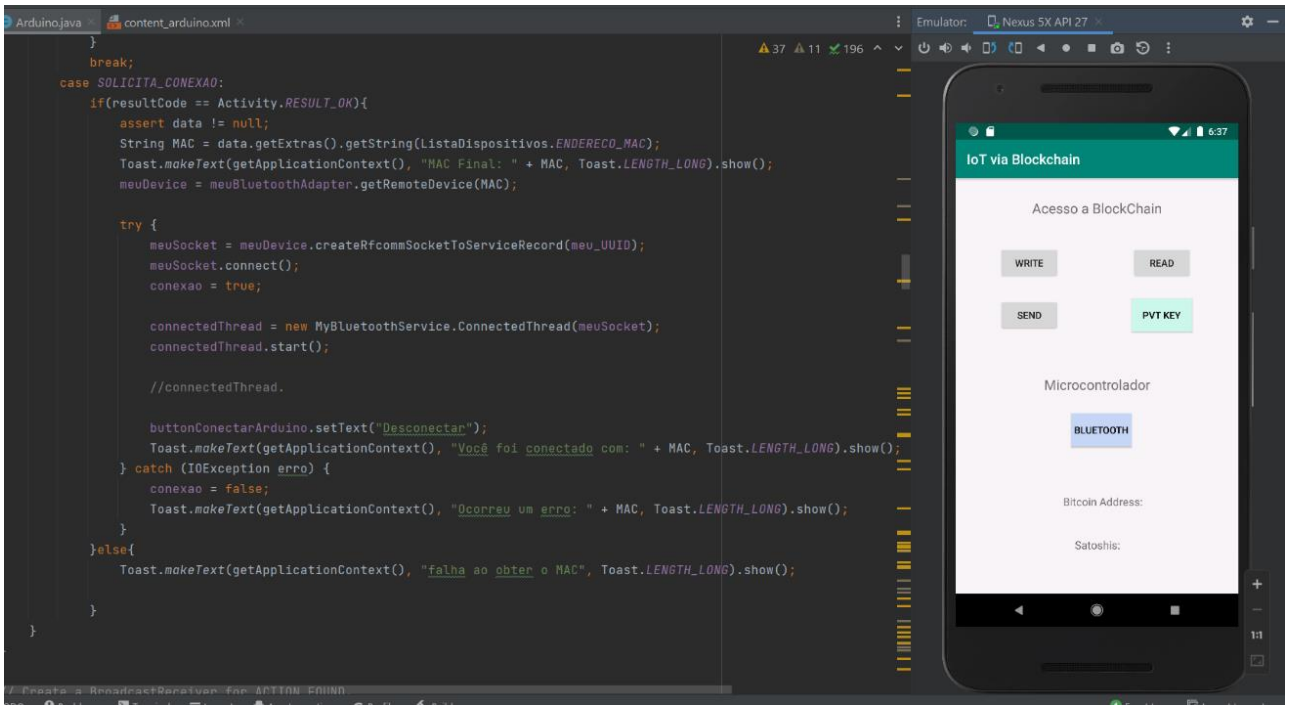

Figura 18 - Backend e API
Fonte: Autoria própria, 2024.

3.8 Dados armazenados na Blockchain BSV

A blockain recebe os dados de temperatura e os grava na blockchain BSV. Com essa arquitetura, cada etapa do fluxo descrito é tratada por um módulo separado, permitindo uma maior flexibilidade e escalabilidade. Além disso, a separação dos módulos facilita a manutenção e a evolução do sistema, permitindo que cada componente seja atualizado ou substituído.

A blockchain BSV serve como uma camada segura e imutável para armazenar as informações criptográficas, garantindo a integridade e a disponibilidade dos dados.

4 RESULTADOS E DISCUSSÕES

4.1 Apresentação

Neste estudo, foi desenvolvido uma aplicação utilizando o sistema do Android Studio para estabelecer comunicação bidirecional entre um dispositivo android e uma placa arduino por meio do bluetooth. A interface do usuário contém a inclusão da aplicação de carteira embutida o qual simplifica significativamente o processo conforme é mostrado na Figura 19. Basta inserir a chave privada no microcontrolador vinculado a cada dispositivo arduino para se conectar a blockchain. Uma vez conectado à blockchain, a interface principal apresentará prontamente o endereço do dispositivo respectivo, facilitando o controle e gerenciamento de seus dispositivos de maneira eficaz.

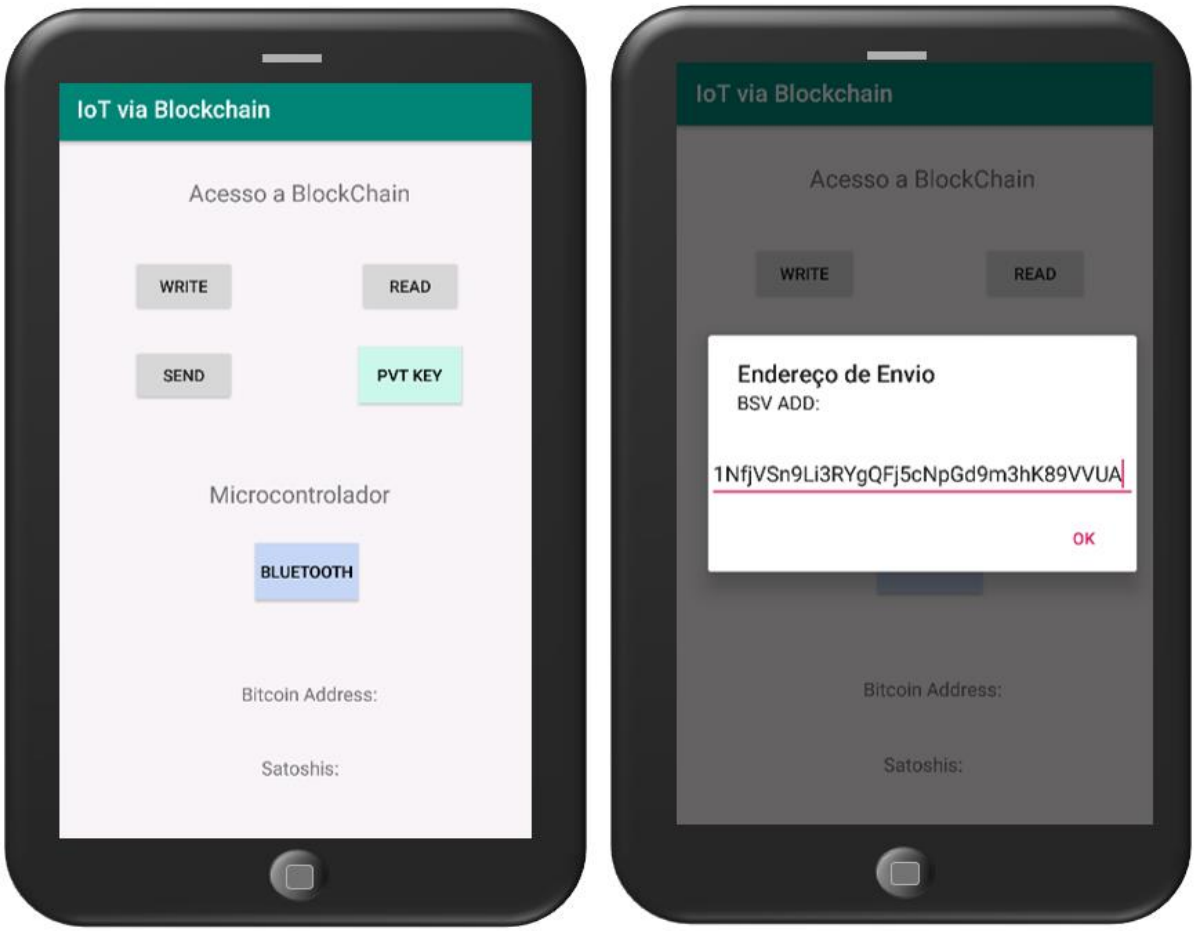

Figura 19 - Interface do usuário com carteira embutida
Fonte: Autoria própria, 2024.

4.2 Resultados da Sincronização

A Tabela 3 fornece uma visão geral dos principais componentes de hardware utilizados no projeto para obter os resultados. O modelo dos microcontroladores e dos módulos bluetooth é o mesmo para ambas as redes de sensores, enquanto os modelos dos dispositivos android eram diferentes para cada nó.

Tabela 3 - Componentes do Sistema

Dispositivos	**Modelo**
Microcontrolador M1	Arduino Uno
Módulo Bluetooth M1	HC-05
Android 1	A14 Samsung
Microcontrolador M2	Arduino Uno
Módulo Bluetooth M2	HC-05
Android 2	A03 Samsung

Cada arduino é responsável tanto por definir quanto por ler o estado de três variáveis distintas. O status dessas variáveis é visualmente transmitido por meio de três LEDs separados, que indicam claramente se cada varável está atualmente ativo ou inativo. O próximo estado de cada rede será determinado pelo estado atual de seu par, conforme apresentado na Tabela 4 para o microcontrolador M1 e a Tabela 5 para o microcontrolador M2.

Tabela 4 - Atividades de M1 durante a sincronização

ADD M1	**1PTKVfWfCVTak5qSGpN6hEx9TBuF6CtQYi**
STATE_0	(read) *** → (set) *** → (sent) 0001
SENT INST ID_0	bab2bb8a73901316dab3870bcdc24bdb129245c2f7102c90463dd966ee33d874
STATE_1	(read from State 1 M2) 0100 → (set) 100 → (sent) 0010
SENT INST ID_1	5cb9fda5bff2752f516dd196acb64f1011e7db0e27bb86ff739f5c480a856ae1
STATE_2	(read from State 2 M2) 0001 → (set) 101 → (sent) 0100
SENT INST ID_2	2219074d7d82acf48cae6bc77905686a6aca9b61c78c12861dfac4749667a498
STATE_3	(read from State 3 M2) 0010 → (set) 111 → (sent) 0001
SENT INST ID_3	20fe8432480679bb3107ea84101c128b67a164275415aa0005bc1ec72d6f823c
STATE_4	(read from State 4 M2) 0100 → (set) 011 → (sent) 0010
SENT INST ID_4	a9ed34d209fc6cf7688e226ca50c85261b3cf149ce6752d71cc2d07e21a5a11d
STATE_5	(read from State 5 M2) 0001 → (set) 010 → (sent) 0100
SENT INST ID_5	54f6ae717409f18ef2bdd9d8b229ae5dd2dddc3bbab90ebf5a6fa225bc5da7cc
STATE_6	(read from State 6 M2) 0010 → (set) 000 → (sent) ***

Tabela 5 - Atividades de M2 durante a sincronização

ADD M2	**1Ar5eHdaeuAKLxrSM2WjCSFPfT3gZh8n9J**
STATE_0	(read from State 0 M1) 0001 → (set) 001 → (sent) 0100
SENT INST ID_0	057d8456b8f7f9f7d89b5cc82973f5db428ac692587a1387b53603480d558ef4
STATE_1	(read from State 1 M1) 0010 → (set) 011 → (sent) 0001
SENT INST ID_1	8714df30c6c3124e79004d3f64a12dfbaa05a0ef30936f381eba0e4f5f27af0a
STATE_2	(read from State 2 M1) 0100 → (set) 111 → (sent) 0010
SENT INST ID_2	c7db4dd10e944b132357d7d4b9b422458441cc6716025b41898e578c01a32422
STATE_3	(read from State 3 M1) 0001 → (set) 110 → (sent) 0100
SENT INST ID_3	fd0269b004103af50842c82db36e330d3beb898f30e042b57446f4304b629fbc
STATE_4	(read from State 4 M1) 0010 → (set) 100 → (sent) 0001
SENT INST ID_4	3a23364db9b03927a7dd75bd973da354c13502dc8a4ae8196d10b393d7025018
STATE_5	(read from State 5 M1) 0100 → (set) 000 → (sent) 0010
SENT INST ID_5	8056c5d86989fb69f35267ba0aa38332069b206c3a0add573b4d7b81ff9eeed7
STATE_6	(read) **** → (set) *** → (sent) ***

Na Tabela 4 é indicado todas as atividades realizadas pelo microcontrolador M1 ao longo de um ciclo completo de teste. A designação ADD M1 representa o endereço específico que M1 utiliza para transmitir dados para a blockchain.

O STATE_0 na coluna ADD M1 não corresponde a um estado da rede de sensores gerenciada por M1. Em vez disso, significa o estado inicial do sistema como um todo, definido diretamente pelo usuário na blockchain, transmitindo o ponto de partida pretendido para a rede. Já o SENT INST ID_0 corresponde ao ID da transação enviada pelo usuário para o endereço de M1 para estabelecer o estado do sistema.

O usuário enviou a informação 0001 o qual resultou a transação o ID bab2bb8a73901316dab3870bcdc24bdb129245c2f7102c90463dd966ee33d874, Figura 20.

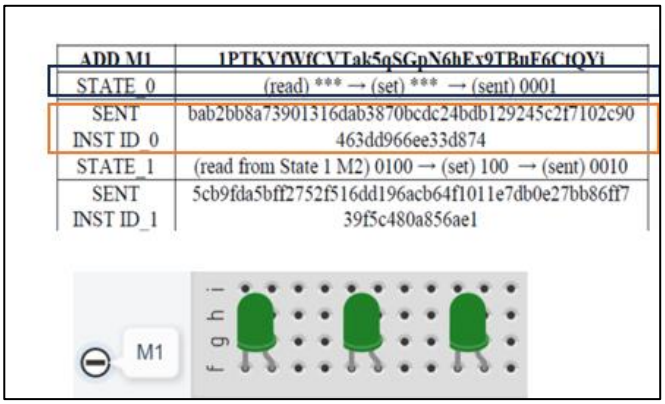

Figura 20 - Estado inicial da sincronização
Fonte: Autoria própria, 2024.

Assim que o sistema é iniciado, M1 e M2 começam a monitorar os endereços um do outro para detectar quaisquer instruções sinalizando uma mudança em seus estados de rede respectivos.

Neste teste específico de sincronização, M2 detecta a primeira instrução, rotulada como "SENT INST ID_0", no endereço de M1. Consequentemente, M2 atualiza seu próprio estado de rede de 000 para 001. Em seguida, M2 envia uma transação (sent: 0100) para a blockchain, notificando M1 do próximo estado pretendido e logo M1 responde modificando seu estado de rede de 000 para 100 e gera um novo estado específico para M1, conforme mostrado na Figura 21. Esse processo sincronizado continua através da blockchain até que ambas as redes voltem ao estado nulo 000.

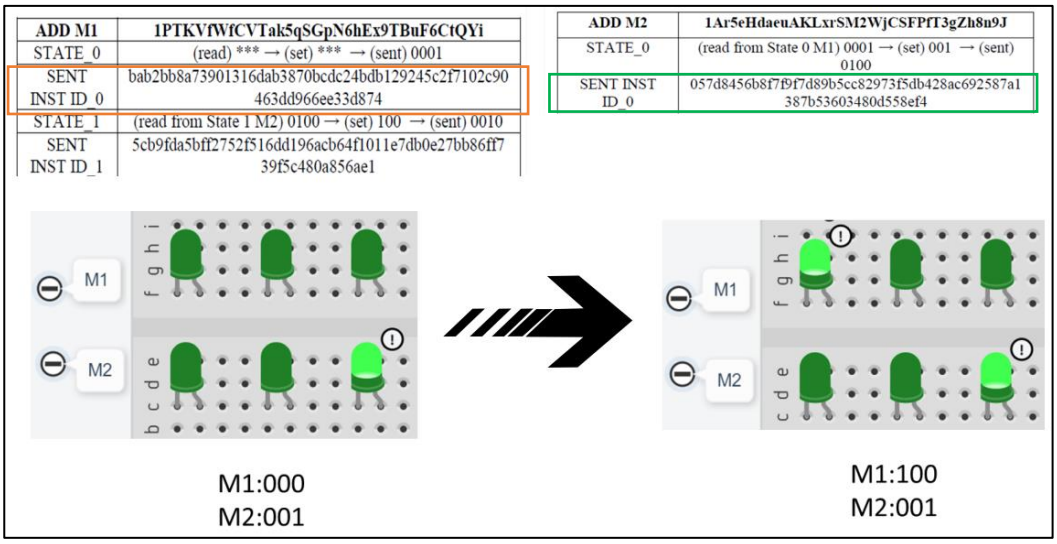

Figura 21 - Sincronização de M1 com M2
Fonte: Autoria própria, 2024.

A totalidade do histórico das operações do sistema é perpetuamente registrado na blockchain, permitindo que a história abrangente do funcionamento do sistema seja recuperada. Essa recuperação pode ser realizada referenciando os IDs de transação transmitidos pelos microcontroladores à blockchain. Embora o histórico de transações possa ser obtido por meio do endereço do microcontrolador, é aconselhável manter um banco de dados personalizado que preserve os IDs de transações significativas para facilitar referência e análise. Os endereços e IDs de transação na Tabela 4 e Tabela 5 podem ser utilizados em buscas em um explorador BSV para obter detalhes adicionais dessas transações. Para garantir a eficiência na escalabilidade de um sistema lidando com um volume substancial de transações, é crucial que o sistema mantenha seu próprio nó completo na blockchain. No entanto, se o volume de

transações não justificar a necessidade de um nó completo, pode ser mais vantajoso aproveitar os serviços oferecidos pelos nós existentes. A avaliação cuidadosa do volume de transações e dos custos associados é fundamental para determinar se a implantação de um nó completo dedicado é necessária para escalabilidade eficiente, ou se depender dos serviços de outros nós de rede é uma opção mais viável.

4.3 Resultados do Acionamento por Temperatura

O Arduino foi configurado para ler os dados de temperatura de um sensor DHT22 e transmiti-los ao dispositivo Android. Em seguida, os dados de temperatura foram enviados para uma API desenvolvida para processar e interagir com a blockchain, o arduino é responsável tanto por definir quanto por ler o estado de três variáveis distintas. O status dessas variáveis é visualmente transmitido por meio de três LEDs separados, que indicam claramente se cada variável está atualmente ativo ou inativo conforme pode ser visto na Figura 22.

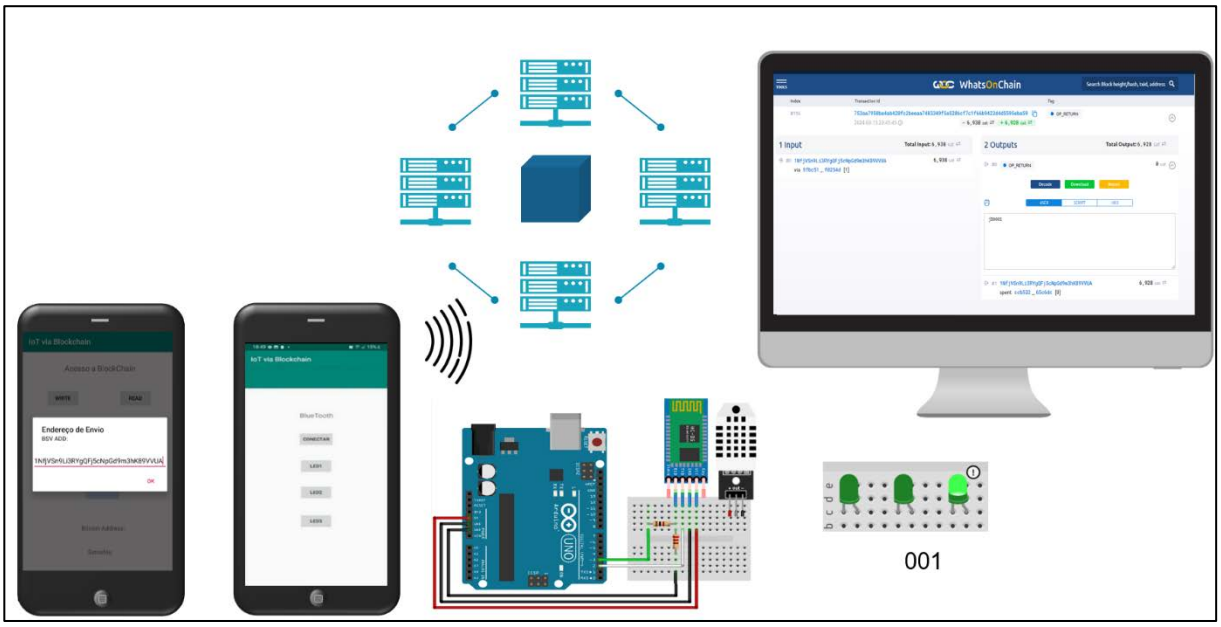

Figura 22 - Estados do LED 001
Fonte: Autoria própria, 2024.

A comunicação entre o Arduino e o dispositivo Android via Bluetooth foi estabelecida com sucesso, permitindo a transmissão dos dados de temperatura em tempo real. Isso proporciona uma maneira eficaz de coletar dados ambientais sem a necessidade de fios ou conexões físicas diretas.

A API desenvolvida foi responsável por receber os dados de temperatura do dispositivo Android e encaminhá-los para a blockchain. Essa camada intermediária é essencial para processar os dados recebidos, validar sua integridade e enviar os dados de maneira adequada para a blockchain.

A blockchain BSV oferece não apenas recursos de escalabilidade, mas também a capacidade de incluir tipos arbitrários de dados dentro de transações. Isso significa que qualquer tipo de dado pode ser inserido em uma transação e posteriormente recuperado usando o ID exclusivo da transação por meio de qualquer serviço de recuperação acessível dentro da rede. Para ilustrar esse conceito, um exemplo de recuperação de dados é mostrado na Figura 23, destacando o processo contínuo de acesso à informação desejada.

A integração entre a API e a blockchain foi bem-sucedida, permitindo que os dados de temperatura fossem recebidos pela API e posteriormente gravados na blockchain. Isso estabelece uma conexão direta entre os dados coletados do mundo físico e seu armazenamento em uma rede descentralizada, o que é crucial para aplicativos que exigem alta confiabilidade e transparência nos dados.

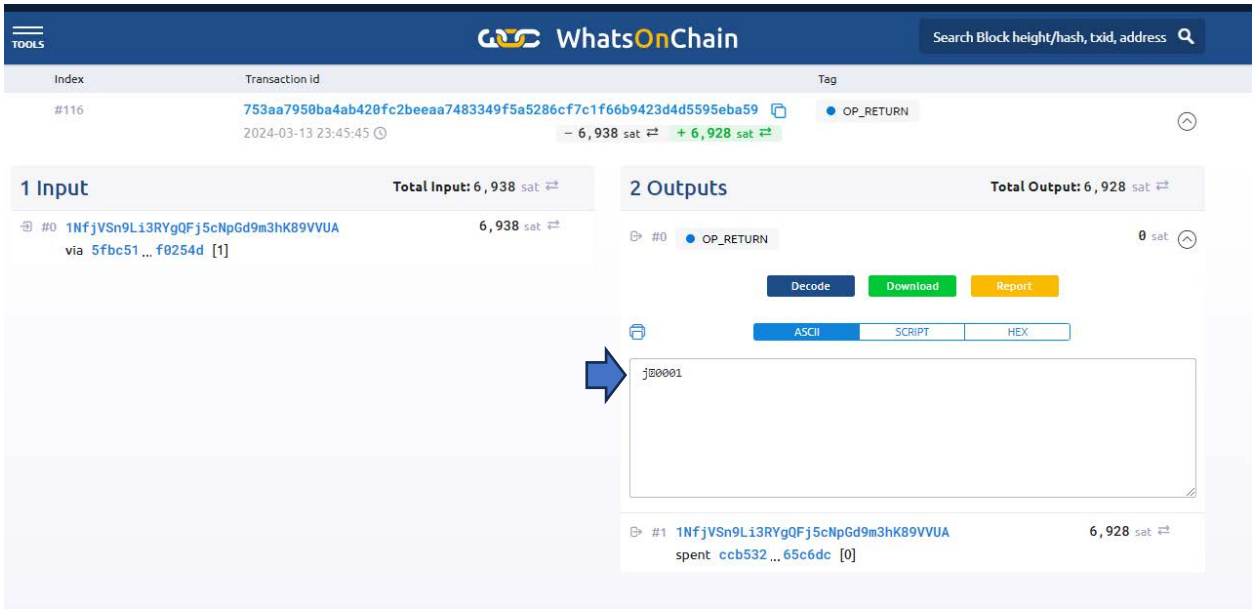

Figura 23 - Dados dos estados do LED 001 gravados na Blockchain
Fonte: Autoria própria, 2024.

A blockchain, neste caso, a Blockchain BSV, serviu como um registro seguro e imutável para armazenar os dados de temperatura. Ao gravar os dados na blockchain,

garantimos sua integridade e disponibilidade a longo prazo, pois eles não podem ser alterados ou apagados após a gravação.

A totalidade do histórico das operações do sistema é perpetuamente registrado na blockchain, permitindo que todos os registros abrangentes do funcionamento do sistema sejam recuperados. Essa recuperação pode ser realizada referenciando os IDs de transação transmitidos pelos microcontroladores à blockchain. Embora o histórico de transações possa ser obtido por meio do endereço do microcontrolador, é importante manter um banco de dados personalizado que preserve os IDs de transações significativas para facilitar referência e análise. O endereço "1NfjVSn9Li3RYgQFj5cNpGd9m3hK89VVUA" pode ser utilizado no explorador BSV https://whatsonchain.com/address/1NfjVSn9Li3RYgQFj5cNpGd9m3hK89VVUA para obter detalhes adicionais dessas transações do projeto, conforme pode ser visto na Figura 24.

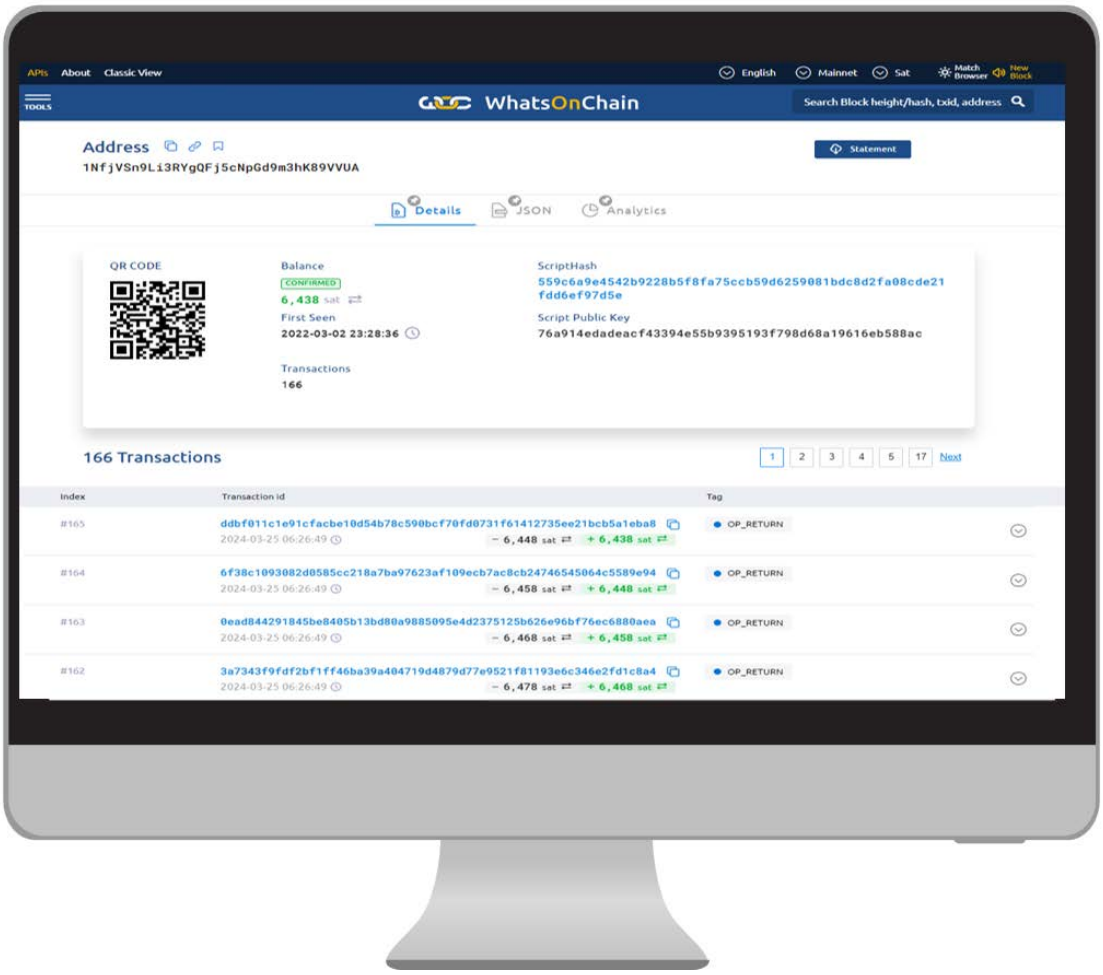

Figura 24 - Informações gravados na Blockchain
Fonte: Autoria própria, 2024.

As informações recuperadas incluem: ID da transação; endereço do microcontrolador; saída da transação, sendo que uma delas contém os dados do nosso sistema em formato hexadecimal; o número do bloco em que a transação foi incluída; o hash do bloco; e o carimbo de data e hora em que o bloco foi criado pelos validadores da transação.

Para garantir a validação e inclusão de uma transação em um bloco, é imperativo incluir uma taxa de transação para os validadores. Esses validadores, que competem entre si, são responsáveis por criar blocos dentro do sistema. Até o momento a taxa média de transação na blockchain BSV é de 0,05 Satoshi por byte.

Para simplificar e focar no conceito de proof of work, o sensor utilizado neste estudo foi limitado ao DHT22. Ao empregar esse sensor, a ênfase foi colocada na validação dos princípios fundamentais e da funcionalidade do sistema. A escolha de detectores de ligar e desligar permitiu uma demonstração clara e concisa das capacidades centrais do sistema.

Na aplicação proposta, utilizamos um aplicativo de carteira embutida que reduz a necessidade de criar uma conta adicional em outra plataforma apenas para executar a aplicação. Ao integrar uma carteira diretamente na aplicação, os usuários obtêm a conveniência de acesso contínuo e unificado às funcionalidades da blockchain. Eles não precisam mais depender de carteiras externas, simplificando a jornada do usuário e reduzindo possíveis obstáculos à adoção. Conforme visto na Figura 25.

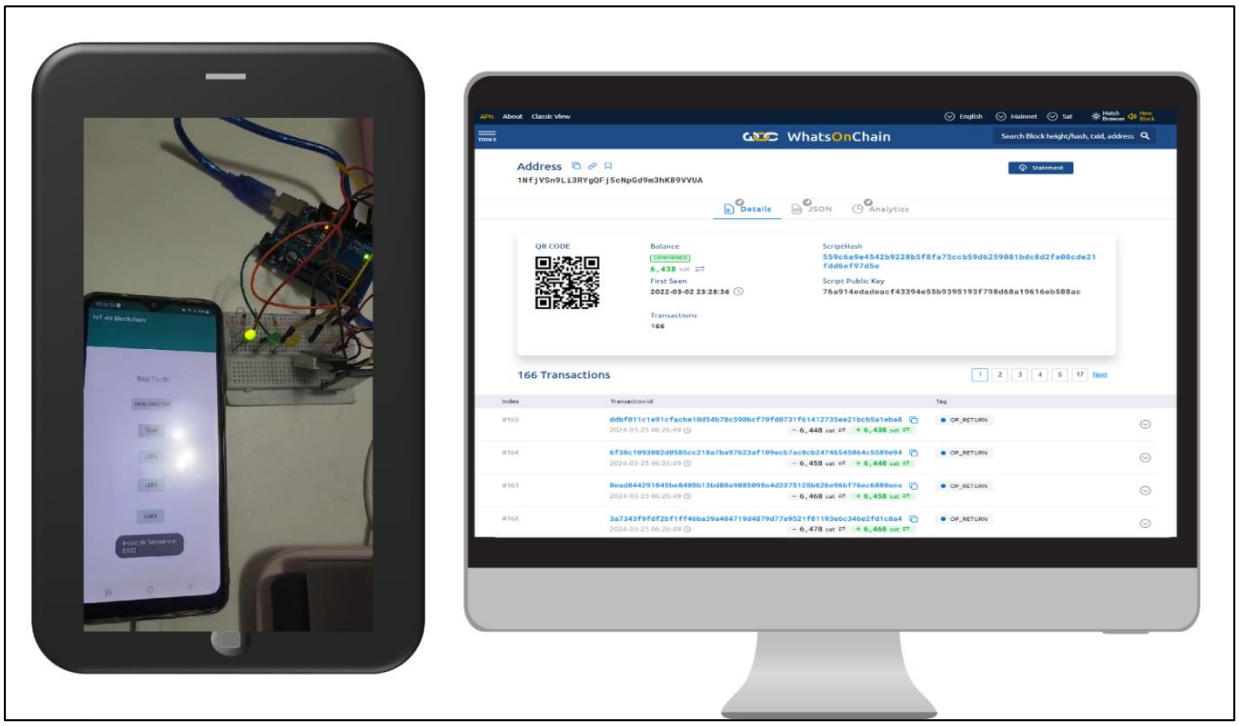

Figura 25 - Resultado do acionamento por temperatura
Fonte: Autoria própria, 2024.

5 CONCLUSÃO E TRABALHOS FUTUROS

A integração das tecnologias deste trabalho oferece uma solução eficaz para a coleta e armazenamento de dados de temperatura em tempo real. O arduino foi programado para capturar os dados de temperatura provenientes de um sensor DHT22. Posteriormente, esses dados foram encaminhados para uma API específica via bluetooth que permite uma conexão sem fio entre os dispositivos, facilitando a implementação em diferentes cenários. Além disso, a utilização da blockchain BSV garante a segurança e a integridade dos dados coletados, tornando-os imutáveis e disponíveis para consulta futura.

Em resumo, este estudo demonstrou a viabilidade de utilizar a tecnologia Bluetooth para transmitir dados de sensores Arduino para dispositivos Android, e posteriormente, enviar esses dados para uma blockchain, garantindo assim a segurança e a integridade dos dados coletados. Essa abordagem pode ter aplicações significativas em áreas como monitoramento ambiental, saúde e segurança, onde é essencial garantir a precisão e a confiabilidade dos dados coletados.

Trabalhos Futuros:

Melhorias na Interface do Usuário: Explorar formas de melhorar a interface do aplicativo Android para torná-lo mais intuitivo e fácil de usar.

Expansão das Funcionalidades: Investigar a possibilidade de coletar e armazenar outros tipos de dados além da temperatura, como umidade ou pressão atmosférica.

Integração com Outras Blockchains: Explorar a possibilidade de integrar a aplicação com outras blockchains além da BSV para oferecer mais opções aos usuários.

Testes em Ambientes Diversos: Realizar testes em ambientes diversos para verificar a robustez e a confiabilidade da solução em diferentes condições.

Estudo de Casos de Uso Específicos: Investigar casos de uso específicos para a aplicação, como monitoramento ambiental em ambientes industriais ou acompanhamento de pacientes em instalações de saúde.

Em suma, este estudo fornece uma base sólida para futuras pesquisas e desenvolvimentos na área de coleta e armazenamento de dados utilizando tecnologias de comunicação sem fio e blockchain. Com a contínua evolução dessas tecnologias, é possível explorar novas aplicações e expandir os recursos da solução proposta para atender às necessidades de diferentes setores e cenários.

Vale ressaltar que um dos desafios associados às aplicações de sistemas baseados em blockchain é a necessidade de uma conexão à internet forte e confiável para garantir o desempenho ideal do sistema. Uma conexão à internet estável e de alta velocidade é essencial para uma comunicação e interação contínuas com a rede blockchain. No entanto, é importante reconhecer que a dependência de uma conexão à internet robusta pode ser considerada uma desvantagem desses sistemas. Em cenários em que a conectividade à internet é limitada, pode resultar em interrupções ou atrasos nas operações do sistema.

6 REFERÊNCIAS BIBLIOGRÁFICAS

[1] Oliveira, Jéssica M.C.; Guedes, João V.F.; Pinheiro, Talita C.; Neves, Jonathas T.; Cruz, Carlos A.M. IoT and Automation via Blockchain – A Simple Solution. Conference SBAI - SBE, Manaus, AM, Brazil, 15-18 October 2023.

[2] Abdi, A.I.; Eassa, F.E.; Jambi, K.; Almarhabi, K.; Khemakhem, M.; Basuhail, A.; Yamin, M. Hierarchical Blockchain-Based Multi-Chain code Access Control for Securing IoT Systems. Electronics 2022, 11, 711.

[3] Islam, M.A.; Madria, S. A Permissioned Blockchain Based Access Control System for IOT. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14-17 July 2019; pp. 469–476.

[4] Xu, R.; Chen, Y.; Blasch, E.; Chen, G. BlendCAC: A BLockchain-Enabled Decentralized Capability-based Access Control for IoTs. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.

[5] Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things. Sensors 2020, 11, 1793.

[6] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: https://bitcoin.org/bitcoin.pdf [Acessado 21 de Agosto de 2023].

[7] Lin, I. C.; Liao, T. C. A survey of blockchain security issues and challenges. International Journal of Network Security, vol 19, n. num 5, p. pp.653–659, September 2017.

[8] N. Rodrigues, “Concessão de Permissão a Dados de Saúde Baseada em Blockchain,” Sociedade Brasileira de Computação, 263 - 274. Mar. 2019

[9] Chang, T. H. and Svetinovic, D. (2016). Data analysis of digital currency networks: Na-mecoin case study. In2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS), pages 122–125.

[10] Min, X., Li, Q., Liu, L., and Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size. In 2016 IEEE Trust-com/BigDataSE/ISPA, pages 90–96.

[11] Moura, T. and Gomes, A. (2017). Blockchain voting and its effects on election transparency and voter confidence. In Proceedings of the 18th Annual International Conference on Digital Government Research, dg.o ’17, pages 574–575, New York, NY,USA. ACM.

[12] Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., and Akutsu, A. (2015). The blockchain-based digital content distribution system. In2015 IEEE Fifth International Conference on Big Data and Cloud Computing, pages 187–190.

[13] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchainfor medical data access and permission management. In2016 2nd International Con-ference on Open and Big Data (OBD), pages 25–30.

[14] Zyskind, G., Nathan, O. and Pentland, A., 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops.

[15] Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A., 2016. FairAccess: a new Blockchain40 Technium Vol. 3, Issue 8 pp.32-41 (2021) ISSN: 2668-778X www.techniumscience.com based access control framework for the Internet of Things. Security and Communication Networks, 9(18), pp.5943-5964.

[16] Li, C. and Zhang, L., 2017. A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. 2017 IEEE International Congress on Internet of Things (ICIOT).

[17] Pinno, O., Gregio, A. and De Bona, L., 2017. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. GLOBECOM 2017 - 2017 IEEE Global Communications Conference.

[18] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L. and Zanichelli, F., 2018. IoTChain: A blockchain security architecture for the Internet of Things. 2018 IEEE Wireless Communications and Networking Conference (WCNC),.

[19] Choi, Y., Kang, H. and Lee, I., 2019. Scalable and Secure Internet of Things Connectivity. Electronics, 8(7), p.752.

[20] Singh, S., Rathore, S. and Park, J., 2020. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Generation Computer Systems, 110, pp.721-743.

[21] Alam, T., 2020. Internet of Things and Blockchain-Based Framework for Coronavirus (COVID19) Disease. SSRN Electronic Journal.

[22] Lee, S. and Sim, K., 2021. Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security. Electronics, 10(9), p.1127.

[23] Wang, D., Wang, H. and Fu, Y., 2021. Blockchain-based IoT device identification and management in 5G smart grid. EURASIP Journal on Wireless Communications and Networking, 2021(1).

[24] ethereum.org. 2023. Introduction to smart contracts | ethereum.org. [online] Disponível em: https://ethereum.org/en/developers/docs/smart-contracts/ [Acessado 24 de Setembro de 2023].

[25] Singer, Talita. Tudo conectado: conceitos e representações da internet das coisas. In: SIMSOCIAL - Simpósio em Tecnologias digitais e sociabilidade. 2012, Salvador. Anais do SIMSOCIAL, 2012.

[26] Evans, D. (2011) The Internet of Things How the Next Evolution of the Internet is Changing Everything. [online] Disponível em:

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Acessado 20 de Novembro de 2023].

[27] Transforma Insights. 2024. Topic: Internet of Things (IoT). [online] Disponível em: https://transformainsights.com/research/forecast/highlights [Acessado 04 de Janeiro de 2024].

[28] Nartey, C., Tchao, E., Gadze, J., Keelson, E., Klogo, G., Kommey, B. and Diawuo, K., 2021. On Blockchain and IoT Integration Platforms: Current Implementation Challenges and Future Perspectives. Wireless Communications and Mobile Computing, 2021, pp.1-25, Article ID 6672482.

[29] Stergiou, C., Psannis, K., Kim, B. and Gupta, B., 2018. Secure integration of IoT and Cloud Computing. Future Generation Computer Systems, 78, pp.964-975.

[30] Zyskind, G., Nathan, O. and Pentland, A., 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops.

[31] Shiksha. 2023. Evolution of Blockchain: 1991 to 2024. [online] Disponível em: https://www.shiksha.com/online-courses/articles/evolution-of-blockchain-technology/ [Acessado 08 de Fevereiro de 2024].

[32] Antonopoulos, Andreas M; Wood, Gavin. Mastering ethereum: building smart contracts and dapps. [S.l.]: O'reilly Media, 2018.

[33] Abdi, A.I.; Eassa, F.E.; Jambi, K.; Almarhabi, K.; Khemakhem, M.; Basuhail, A.; Yamin, M. Hierarchical Blockchain-Based Multi-Chaincode Access Control for Securing IoT Systems. Electronics 2022, 11, 711.

[34] Ghorbel, O.; Frikha, T.; Hajji, A.; Alabdali, R.; Ayadi, R.; Elmasry, M.A. Blockchain-Based Supply Chain System for Olive Fields Using WSNs. Comput. Intell. Neurosci. 2022, 2022, 9776776.

[35] Sztajnberg, A., da Silva Macedo, R., e Stutzel, M. (2018). Protocolos de aplicação para a internet das coisas: conceitos e aspectos práticos. Soci edade Brasileira de Computação.

[36] Li, C. and Zhang, L., 2017. A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. 2017 IEEE International Congress on Internet of Things (ICIOT).

[37] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L. and Zanichelli, F., 2018. IoTChain: A blockchain security architecture for the Internet of Things. 2018 IEEE Wireless Communications and Networking Conference (WCNC).

[38] Pinno, O., Gregio, A. and De Bona, L., 2017. ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. GLOBECOM 2017 - 2017 IEEE Global Communications Conference.

[39] 101Blockchains. 2023. Topic: A História da Tecnologia Blockchain. [online] Disponível em: https://101blockchains.com/pt/historia-da-tecnologia-blockchain/ [Acessado 09 de Fevereiro de 2024].

[40] shiksha. 2023. Topic: Merkle Tree in Blockchain. [online] Disponível em: https://www.shiksha.com/online-courses/articles/merkle-tree-in-blockchain/ [Acessado 08 de Fevereiro de 2024].

[41] Greve, F. G., Sampaio, L. S., Abijaude, J. A., Coutinho, A. C., Valcy, Í. V., e Queiroz, S. Q. (2018). Blockchain e a revolução do consenso sob demanda. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos.

[42] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., e Rong, C. (2019). A comprehensive survey of blockchain: From theory to iot applications and beyond. IEEE Internet of Things Journal, 6(5):8114-8154.

[43] Saweros, E. e Song, Y.-T. (2019). Connecting heterogeneous electronic health record systems using tangle. In International Conference on Ubiquitous Information Management and Communication, pages 858-869. Springer.

[44] Santos, B. P., Silva, L. A., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N., e Loureiro, A. (2016). Internet das coisas: da teoria à prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos, 31.

[45] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., e Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4):352-375.

[46] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.: Blockchain contract: Securing a blockchain applied to smart contracts. In: 2016 IEEE Int. Conference on Consumer Electronics (ICCE). pp. 467–468 (2016).

[47] SANKAR, L. S.; SINDHU, M.; SETHUMADHAVAN, M. Survey of consensus protocols on blockchain applications. 4th International Conference on Advanced Computing and Communication Systems (ICACCS), p. 1–5, 2017.

[48] Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart Contract-Based Access Control for the Internet of Things. IEEE Internet Things J. 2019, 6, 1594–1605.

[49] Ulrich, Fernando. Bitcoin: a moeda na era digital. [S.l.]: LVM Editora, 2017.

[50] Buterin, Vitalik et al. A next-generation smart contract and decentralized application platform. white paper, v. 3, n. 37, p. 2–1, 2014.

[51] Haque, B.; Hasan, R.; Zihad, O.M. SmartOil: Blockchain and smart contract-based oil supply chain management. IET Blockchain 2021, 1, 95–104.

[52] Mcroberts, M. Arduino Básico, São Paulo, Novatec, 2011.

[53] Haque, B.; Hasan, R.; Zihad, O.M. SmartOil: Blockchain and smart contract-based oil supply chain management. IET Blockchain 2021, 1, 95–104.

[54] Sankar, L. S.; Sindhu, M.; Sethumadhavan, M. Survey of consensus protocols on blockchain applications. 4th International Conference on Advanced Computing and Communication Systems (ICACCS), p. 1–5, 2017.
[55] Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J. 2018, 5, 1184–1195.

[56] SOUZA, A, R. PAIXÃO, A, C. UZÊDA, D, D. DIAS, M, A. DUARTE, S. AMORIM, H, S. A placa Arduino: uma opção de baixo custo para experiências de física assistidas pelo PC. Revista Brasileira de Ensino de Física, v. 33, n. 1, 1702 (2011).

[57] DEITEL, H. M. C++: Como programar. v.5, São Paulo: Pearson Prentice Hall, 2006.

[58] UNESCO/COL. Open Educational Resources and Change in Higher Education: Reflections from Practice. Commonwealth of Learning: Vancouver, 2012.

[59] FETZNER, G. F.; Experimentos de baixo custo para o ensino de F´ısica em N´ıvel M´edio usando a placa Arduino-UNO. Porto Alegre: UFRGS, 2015. Disserta¸c˜ao (Mestrado Profissional em Ensino de F´ısica) - Programa de P´os-Gradua¸c˜ao em Ensino de F´ısica, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015.

[60] KIRIANAKI, N. et al.; Data Acquisition and Signal Processing for Smart Sensors. Baffins Lane: John Wiley & Sons Ltd, 2002.