



UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA DE INFORMAÇÃO E
COMUNICAÇÃO

Wellington Fernandes Silvano

**Registro distribuído IOTA e conectividade Sigfox como solução para
rastreabilidade e monitoramento seguro na cadeia de suprimentos**

Araranguá
2021

Wellington Fernandes Silvano

Registro distribuído IOTA e conectividade Sigfox como solução para rastreabilidade e monitoramento seguro na cadeia de suprimentos

Dissertação submetida ao Programa de Pós-Graduação em Tecnologia de Informação e Comunicação da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Tecnologia de Informação e comunicação.

Orientador: Prof. Roderval Marcelino, Dr.

Coorientador: Prof. Martin Augusto Gagliotti Vigil, Dr.

Araranguá
2021

**Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.**

Fernandes Silvano, Wellington

Registro distribuído IOTA e conectividade Sigfox como solução para rastreabilidade e monitoramento seguro na cadeia de suprimentos / Wellington Fernandes Silvano ; orientador, Roderval Marcelino, coorientador, Martin

Augusto Gagliotti Vigil,, 2021.

147 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Campus Araranguá, Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2021.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. IOTA. 3. Sigfox. 4. Cadeia de suprimentos. 5. Internet das coisas.
I. Marcelino, Roderval. II. Augusto Gagliotti Vigil,, Martin. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Tecnologias da Informação e Comunicação. IV. Título.

Wellington Fernandes Silvano

Registro distribuído IOTA e conectividade Sigfox como solução para rastreabilidade e monitoramento seguro na cadeia de suprimentos

O presente trabalho em nível de Mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Cristian Cechinel, Dr.
Universidade Federal de Santa Catarina

Prof. Vilson Gruber, Dr.
Universidade Federal de Santa Catarina

Olívia Terence Saa, Dra.
Fundação IOTA

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Tecnologia de Informação e comunicação.

Coordenação do Programa de
Pós-Graduação

Prof. Roderval Marcelino, Dr.
Orientador

Araranguá, 2021.

Este trabalho é dedicado a minha esposa Morgana e
meu filho Augusto, que ainda não nasceu.

AGRADECIMENTOS

Raramente conseguimos construir algo realmente sozinhos, comigo não foi diferente. Foram muitos envolvidos nessa jornada.

Agradeço a minha esposa Morgana Gonçalves de Souza Silvano pelo amor, imensa paciência e pelo apoio durante o processo de escrita.

Ao meu orientador Roderval Marcelino, pelo apoio, liberdade, e pelas trocas de experiências contínuas e revisões de estrutura e texto em todos os materiais escritos. Ao meu coorientador Martin Vigil, pelas conversas sobre sistemas distribuídos, revisões de texto e discussões marcantes e pertinentes.

Ao Hamilton Luiz Bez Batti Dias, pelas discussões relativas à estrutura da prova de conceito desenvolvida e pela parceria na construção do protótipo.

A Daniel de Michele (Carpincho) com quem passei muitos dias em chamadas de vídeo para escrever um dos artigos relacionados a esta dissertação. A Daniel Trauth por seu excelente trabalho e por ter compartilhado sua pesquisa realizada na Universidade Aachen/Alemanha.

Ao meu amigo André Grahl Pereira, professor/pesquisador da UFRGS, pela ajuda na concepção e estruturação de artigos escritos ao longo do mestrado e pelo rigor científico de seus apontamentos. Ao meu amigo, ilustrador, Eduardo Eising pelo empenho no desenvolvimento das ilustrações realizadas durante o mestrado, em artigos e na dissertação.

Agradeço também a empresa Ayga, pela doação do hardware WS-2 e pelo apoio durante a pesquisa. Agradecimentos especiais ao João Ricardo Wagner de Moraes pelas dicas e informações, ao Bruno Oliveira pelas e formalização e envio do dispositivo e ao Luiz Gerbase que prontamente se colocou a disposição para ajudar.

Por fim agradecer a Universidade Federal de Santa Catarina e a Fundação de Amparo à Pesquisa de Santa Catarina pelo financiamento, via bolsa de pesquisa.

“Vivemos numa sociedade dependente da ciência e da tecnologia, mas que não sabe quase nada disso.”
(SAGAN, 1996)

RESUMO

As atuais técnicas de trocas de informações durante o transporte de produtos na cadeia de suprimentos causam atrasos e erros humanos. As soluções computacionais, quando utilizadas, geralmente envolvem bancos de dados centralizados hospedados por uma das partes interessadas, onde o direito de acesso e possibilidade de alteração dos dados são questões que geram desconfiança entre as partes, em especial no transporte de cargas perecíveis como vacinas, carne e frutas. Esse contexto desperta o interesse por soluções distribuídas, confiáveis e seguras, como é o caso das tecnologias de registro distribuídas (DLT). Além disso, o registro de dados de cargas em movimento, requerem conectividade também móvel, porém os custos e consumo de bateria de redes celulares são elevados quando comparados com redes LPWANs. Estas questões favorecem pesquisas que busquem combinar tecnologias LPWANs e DLTs. Mas nem todas as DLTs são adequadas para o registro de dados de sensores, este trabalho estuda essa característica no DLT da criptomoeda IOTA, o Tangle, combinados com a rede LPWAN Sigfox. Dentre os resultados dessa dissertação ressalta-se a modelagem, implementação e avaliação experimental de uma solução que integra IOTA e Sigfox para monitoramento e rastreamento on-line na cadeia de suprimentos. Ao propor a solução, surgiram outras questões relacionadas ao hardware, em especial o mapeamento de rede wi-fi para obtenção de geolocalização. As características do hardware proposto foram avaliadas por meio de experimentações relacionadas a perda de sinal e exatidão da geolocalização. O sistema completo também foi analisado experimentalmente, identificando a latência do sistema e análise de viagens completas. Identificou-se que um ecossistema como o proposto fornece uma solução segura, transparente, de baixo custo e alto grau de imutabilidade para a cadeia de suprimentos. Mas possui limitações, que estão principalmente relacionadas a baixa cobertura Sigfox no Brasil e a identificação de um possível ponto de fragilidade, que um sistema como esse necessita, até que novas melhorias sejam implementadas.

Palavras-chave: IOTA. Sigfox. Cadeia de suprimentos. Blockchain. Internet das coisas.

ABSTRACT

Current techniques for exchanging information while transporting products in the supply chain cause delays and human errors. Computer solutions, when used, usually involve centralized databases hosted by one of the interested parties, where the right of access and the possibility of changing the data are issues that generate distrust between the parties, especially in the transport of perishable cargo such as vaccines, meat and fruit. This context arouses interest in distributed, reliable and secure solutions, such as distributed registry technologies (DLT). In addition, data logging of moving loads also requires mobile connectivity, but the costs and battery consumption of cellular networks are high when compared to LPWANs. These questions favor research that seeks to combine LPWANs and DLTs technologies. But not all DLTs are suitable for logging sensor data, this work studies this feature in the IOTA cryptocurrency DLT, the Tangle, combined with the LPWAN Sigfox network. Among the results of this dissertation, the modeling, implementation and experimental evaluation of a solution that integrates IOTA and Sigfox for online monitoring and tracking in the supply chain is highlighted. When proposing the solution, other issues related to the hardware arose, in particular the Wi-Fi network mapping to obtain geolocation. The characteristics of the proposed hardware were evaluated through experiments related to signal loss and geolocation accuracy. The complete system was also analyzed experimentally, identifying system latency and analysis of complete trips. It was identified that an ecosystem such as the one proposed provides a secure, transparent, low-cost and high degree of immutability solution for the supply chain. But it has limitations, which are mainly related to low Sigfox coverage in Brazil and the identification of a possible weak point, which such a system needs, until further improvements are implemented.

Keywords: IOTA. Sigfox. Supply chain. Blockchain. Internet of things.

LISTA DE FIGURAS

Figura 1 – Quadro geral de desenvolvimento do trabalho	19
Figura 2 – Representação simplificada de blocos na Blockchain	24
Figura 3 – Grafo representativo de parte do Tangle. a) Estado em um tempo t qualquer b) Estado t+1, com uma transação nova p	28
Figura 4 – Peso acumulativo x tempo. Em regime de alta carga	30
Figura 5 – Exemplo de uma <i>Merkle Hash Tree — MHT</i>) com 4 folhas.	35
Figura 6 – Arquiteturas de rede possíveis para publicar dados de sensores no Tangle	39
Figura 7 – Taxa de dados vs alcance	41
Figura 8 – Comparação das características: Sigfox, LoRaWAN e NB-IoT	42
Figura 9 – Modulação de sinal de rádio frequência - Sigfox	46
Figura 10 – Comparação de sinais Sigfox x 3G	47
Figura 11 – Cronologia de uma comunicação Sigfox	48
Figura 12 – Arquitetura de rede Sigfox	49
Figura 13 – Tipos de chamadas - Sigfox	50
Figura 14 – Etapa 1: Pesquisas relacionadas a monitoramento na cadeia de suprimentos	55
Figura 15 – Etapa 2: Pesquisas relacionadas a Blockchain no monitoramento na cadeia de suprimentos	55
Figura 16 – Etapa 2: Tipos de documentos	56
Figura 17 – Etapa 4: Pesquisas relacionadas ao ledger distribuído da IOTA/Tangle	61
Figura 18 – IOTA - Abordagem e tipos de aplicação dos artigos	62
Figura 19 – Etapa 5: Pesquisas relacionadas à rede LPWAN Sigfox	64
Figura 20 – Etapas da pesquisa tecnológica	73
Figura 21 – Arquitetura proposta	74
Figura 22 – Inserção de dados utilizando MAM	74
Figura 23 – Visualização dos dados	75
Figura 24 – Arquitetura da dissertação	76
Figura 25 – WACS 2	77
Figura 26 – WACS 2: ilustração dos componentes	78
Figura 27 – WACS 2: foto real	79
Figura 28 – Carro Google	80
Figura 29 – Comunicação de dados	83
Figura 30 – Dados de temperatura e localização recebidos da AYGA em formato Json	85
Figura 31 – Encaminhamento para attachToTangle	86
Figura 32 – Função attachToTangle	86

Figura 33 – MongoDB - Coleções criadas	87
Figura 34 – Tela inicial - Login	88
Figura 35 – Dashboard após o login	88
Figura 36 – Cadastro de viagem	89
Figura 37 – Requisição de dados de um canal MAM para um IOTA Fullnode	90
Figura 38 – Visualização da viagem: temperatura das cargas	90
Figura 39 – Visualização da viagem: localização das cargas	91
Figura 40 – Área de cobertura para testes estáticos	93
Figura 41 – Área de cobertura para testes dinâmicos	94
Figura 42 – Área de cobertura Sigfox entre Araranguá/SC - Baurú/SP	97
Figura 43 – Área de cobertura Sigfox Araçatuba/SP e região	98
Figura 44 – Resultados experimentais de Geolocalização: Triangulação de sinal Wi-fi	101
Figura 45 – Precisão das medidas de Latitude e Longitude	102
Figura 46 – Latênciam do ecossistema	106
Figura 47 – Dados de localização - Viagem Araranguá/SC -> Baurú/SP	107
Figura 48 – Dados de temperatura - Viagem Araranguá/SC -> Baurú/SP	107
Figura 49 – Maior área sem registro de dados	108
Figura 50 – Dados de temperatura - Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP	109
Figura 51 – Dados de localização - Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP	110
Figura 52 – Consumo de bateria: viagem 1 e 2	110

LISTA DE TABELAS

Tabela 1 – Artigos	57
Tabela 2 – Artigos (continuação)	58
Tabela 3 – Artigos (continuação)	59
Tabela 4 – Soluções - Blockchain no monitoramento da cadeia de suprimentos	60
Tabela 5 – Artigos - IOTA	63
Tabela 6 – Artigos - Sigfox	65
Tabela 7 – Ayga Wacs 2	78
Tabela 8 – Validação experimental Geolocalização - MAC adress e API Here	92
Tabela 9 – Validação experimental - perda de pacotes de mensagem	95
Tabela 10 – Validação experimental - perda de pacotes de mensagem	96
Tabela 11 – Validação experimental - perda de pacotes de mensagem	97
Tabela 12 – Resultados experimentais: Geolocalização MAC adress Wi-fi	100
Tabela 13 – Testes estáticos: Intensidade de sinal Sigfox entre Araranguá e Criciúma	103
Tabela 14 – Testes dinâmicos: Intensidade de sinal Sigfox entre Araranguá e Criciúma	104
Tabela 15 – Latência do ecossistema	105

SUMÁRIO

1	INTRODUÇÃO	15
1.1	HIPÓTESES	17
1.2	OBJETIVOS	17
1.2.1	Objetivo Geral	17
1.2.2	Objetivos Específicos	17
1.3	ADERÊNCIA DO OBJETO DE PESQUISA AO PPGTIC	18
1.4	METODOLOGIA	18
1.5	CONTRIBUIÇÕES PARA LITERATURA	20
1.5.1	Distinções	20
2	TECNOLOGIA DE REGISTRO DISTRIBUÍDO	22
2.1	CONTEXTUALIZAÇÃO: BITCOIN E BLOCKCHAIN	23
2.1.1	Limitações da Blockchain	24
2.1.1.1	Escalabilidade	24
2.1.1.2	Consumo de energia	25
2.1.1.3	Taxas para transações	25
2.1.1.4	Redundância	26
2.2	ECOSSISTEMA IOTA/TANGLE	26
2.2.1	Tangle	27
2.2.2	Coordenador	30
2.2.3	Wallet	31
2.2.4	Light Node e FullNode	32
2.2.5	Snapshot	33
2.2.6	Permanode	33
2.2.7	Masked Authenticated Messaging	33
2.2.8	Bibliotecas e ferramentas	35
2.2.8.1	Mainnet, Devnet e Spamnet	36
2.2.8.2	IOTA Tangle Explorer	36
2.2.8.3	IOTA Reference Implementation	36
2.2.8.4	IOTA client	36
2.2.8.5	MAM client	37
2.3	CONSIDERAÇÕES FINAIS SOBRE AS CARACTERÍSTICAS DA IOTA	37
3	REDE LPWAN SIGFOX	40
3.1	CONTEXTUALIZAÇÃO: TECNOLOGIAS LPWAN	40
3.1.1	NB-IoT	42
3.1.2	LoRaWAN	43
3.2	ECOSSISTEMA SIGFOX	44
3.2.1	Número de mensagens por dia	44

3.2.2	Dispositivos Sigfox	45
3.2.3	Protocolo de transmissão das informações	45
3.2.4	Segurança	48
3.2.5	Arquitetura de rede	48
3.2.6	Backend Sigfox	49
3.2.6.1	Callbacks	50
3.2.6.2	API Rest	50
4	ESTADO DA ARTE	52
4.1	METODOLOGIA DA PESQUISA BIBLIOGRÁFICA	52
4.1.1	Bases de dados	52
4.1.2	Palavras-chave	53
4.1.3	Filtro de qualidade	53
4.1.4	Análise exploratória	54
4.2	RESULTADOS DE PESQUISA	54
4.2.1	Etapa 1: Monitoramento na cadeia de suprimentos	54
4.2.2	Etapa 2 - Blockchain e monitoramento na cadeia de suprimentos	54
4.2.3	Etapa 4 - IOTA	60
4.2.4	Etapa 5 - Sigfox	64
4.3	ANÁLISE DESCRIPTIVA	65
4.3.1	IOTA/Tangle	65
4.3.2	Sigfox	66
4.3.3	Blockchain no monitoramento e rastreamento da cadeia de suprimentos	67
4.3.3.1	Monitoramento durante a custódia	68
4.3.3.2	Monitoramento não definido	68
4.3.3.3	Monitoramento contínuo	68
4.3.4	Diferenciais do trabalho proposto	72
5	METODOLOGIA DA PESQUISA	73
5.1	ARQUITETURA DO ECOSISTEMA	73
5.2	TECNOLOGIAS ENVOLVIDAS	75
5.2.1	Sistema Embocado	75
5.2.1.1	AYGA WACS-2	77
5.2.2	API Here - Geolocalização	80
5.2.3	Sistema Web	81
5.2.3.1	MongoDB	81
5.2.3.2	React	81
5.2.3.3	Node	81
5.2.3.4	Express	82
5.3	DESENVOLVIMENTO DA PROVA DE CONCEITO	82

5.3.1	Aquisição de sinais	82
5.3.2	Envio dos dados ao IOTA/Tangle	83
5.3.2.1	Backend da plataforma Web	84
5.3.2.2	Front-end da plataforma Web	87
6	DELINAMENTO EXPERIMENTAL	92
6.0.1	Precisão da geolocalização com MAC address de redes Wi-fi	92
6.0.1.1	Ambiente de pesquisa	92
6.0.1.2	Coleta de dados	92
6.0.2	Perda de pacotes Sigfox em movimento	93
6.0.2.1	Ambiente de pesquisa	94
6.0.2.2	Metodologia de coleta de dados	95
6.0.3	Latência do sistema	95
6.0.3.1	Ambiente de pesquisa	95
6.0.3.2	Metodologia de coleta de dados	95
6.0.4	Validação da prova de conceito - Viagem	96
6.0.4.1	Ambiente de pesquisa	96
6.0.4.2	Metodologia de coleta de dados	96
7	RESULTADOS E DISCUSSÕES	99
7.1	GEOLOCALIZAÇÃO	99
7.2	PERDA DE PACOTES SIGFOX EM MOVIMENTO	102
7.3	LATÊNCIA	103
7.4	VALIDAÇÃO DA PROVA DE CONCEITO - VIAGEM	106
7.4.1	Viagem 1: Araranguá/SC - Baurú/SP	106
7.4.2	Viagem 2: Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP	109
7.4.3	Consumo de bateria	110
7.4.4	Outras considerações	111
7.5	CUSTO	111
7.6	DISCUSSÃO INFORMAL SOBRE IMUTABILIDADE	113
8	CONCLUSÃO	116
	REFERÊNCIAS	120
	APÊNDICE A – TABELA DE LOCALIZAÇÃO - VIAGEM 1	132
	APÊNDICE B – TABELA DE TEMPERATURA - VIAGEM 1	138
	APÊNDICE C – TABELA DE LOCALIZAÇÃO - VIAGEM 2	145
	APÊNDICE D – TABELA DE TEMPERATURA - VIAGEM 2	146

1 INTRODUÇÃO

Tecnologias de registro distribuídos (*Distributed Ledger Technologies — DLT*), tem se popularizado especialmente com o surgimento do Bitcoin, e sua tecnologia adjacente à Blockchain. Em sistemas como esse existe um forte grau de imutabilidade da informação inserida na rede o que proporcionou grande interesse de vários campos, incluindo áreas não financeiras e Internet das coisas (*Internet of Things — IoT*) (LIN *et al.*, 2019). As DLTs têm despertado o interesse de governos, instituições financeiras, empresas de alta tecnologia e inclusive o mercado de capitais por soluções onde a imutabilidade e transparência dos dados também são de grande valia, onde as partes envolvidas não necessariamente precisam confiar uns nos outros (YUAN; WANG, 2018) (MONDRAGON *et al.*, 2018). Um dos campos com maior ganho potencial para esse tipo de solução está na cadeia de suprimentos.

A cadeia de suprimentos requer fluxos de informações contínuos, processamento de informações *on-line* e comunicação transparente entre os envolvidos, se quisermos as melhores tomadas de decisão (LAMBERT; COOPER, 2000).

No entanto, atualmente as informações são compartilhadas de maneira semi-digital como e-mails, telefone e aplicativos de banco de dados centralizados (SLUIJS, 2017) (IMERI; KHADRAOUI, 2018). Com informações centralizadas, o dono do banco de dados detém o controle da informação e seu direito de acesso pode ir além do monitoramento, possibilitando qualquer alteração. Portanto, soluções que possibilitem ampliar a confiabilidade entre as partes e que favoreçam o monitoramento e compartilhamento de dados na cadeia de suprimentos devem ser favorecidas.

Apesar dos potenciais da Blockchain para resolver problemas da cadeia de suprimentos, algumas limitações relativas ao seu design inviabilizam esse tipo de aplicação. Ao mesmo tempo que a imutabilidade e a descentralização seriam relevantes para o compartilhamento de dados de forma segura, transparente e imutável, os custos e tempos envolvidos dificultam sua implantação (YEOW *et al.*, 2018). A Blockchain pública exige incentivos para favorecer uma transação perante outras (oferta e demanda), inviabilizando o armazenamento de transações muito pequenas, de pouco valor agregado quando lidos de maneira individual (MARINO *et al.*, 2019). Esse é o caso de dados de sensores que fazem medições da situação de cargas de produtos, especialmente aqueles que exigem controle e/ou são perecíveis. Como garantir que uma carga seja adequadamente transportada? Por exemplo, como garantir que uma vacina ou carne foi adequadamente refrigerada, ou que a fruta está em boas condições de consumo devido ao amadurecimento prematuro relacionado a falta de cuidados no transporte?

O surgimento de tecnologias de registro distribuídas e limitações de design de sistemas Blockchain para alguns tipos de aplicações levaram ao desenvolvimento

de criptomoedas alternativas para vários fins. Dentre as soluções destaca-se a IOTA, com sua nova arquitetura chamada Tangle, que promete alta escalabilidade, sem taxas e transferências rápidas, com foco nas soluções de IoT (POPOV, 2016)(DIVYA; BIRADAR, 2018)(ZHENG *et al.*, 2019). Além disso, suas fortes parcerias chamam a atenção como é o caso das empresas Jaguar | Land Rover, Dell Technologies, Linux Foundation, entre muitas outras (MARINO *et al.*, 2019). Dentre os focos de desenvolvimento do protocolo está o objetivo de criar uma infraestrutura aberta para economia digital, pronta para humanos e dispositivos (MARINO *et al.*, 2019). Isso inclui o comércio global e cadeia de suprimentos. A IOTA possuí uma camada para troca de dados, não apenas valores como era de se esperar para uma criptomoeda (HANDY, 2017).

Ao tratar da transmissão de dados de sensores para a rede Tangle da IOTA, é importante discutir também a conectividade. São muitas as tecnologias disponíveis para conectar-se à internet, mas nenhuma consegue resolver todos os requisitos para qualquer tipo de aplicação. A escolha de uma arquitetura de rede depende dos requisitos de largura de banda, confiabilidade e custo-benefício necessários para o projeto (OGBODO *et al.*, 2017). Tecnologias celulares como 2G, 3G, 4G e *Long Term Evolution (LTE)* são tecnologias bem estabelecidas e adequadas para aplicativos que precisam de longo alcance e alta taxa de transferência de dados (GADDAM; RAI, 2018). Aplicações IoT requerem tecnologia de comunicação com longo alcance e baixo consumo de energia. Redes LPWAN (*Low Power Wide Area Network*) propiciam que dispositivos usem baixo consumo de energia ou longa duração de bateria, oferecendo baixa taxa de transferência de dados e dados podem ser enviados a longas distâncias, diminuindo custos de implantação (GADDAM; RAI, 2018). Essa tecnologia é uma representação das várias tecnologias que estão sendo usadas atualmente na conexão de sensores e controladores à internet sem a intervenção das redes *Wi-Fi* ou celulares tradicionais existentes. Entre essas tecnologias promissoras estão a SigFox, Ingenu RPMA e LoRa (GADDAM; RAI, 2018). Dentre esses, Sigfox apresenta os dispositivos de menor custo, menor consumo de energia e maior distância de transmissão de dados (GADDAM; RAI, 2018). Uma estação base pode cobrir 10 km em áreas urbanas e 40 km em regiões rurais, ideal para aplicações de longo alcance com baixa taxa de dados e baixa carga útil (SIGFOX, S., 2020) (MEKKI *et al.*, 2018).

O cenário descrito evidencia que uma combinação entre IOTA e Sigfox na cadeia de suprimentos é promissora, em especial na questão logística de transporte, pois demonstra perspectivas onde a troca de dados em rede, seguros transparentes e imutáveis são desejáveis. No contexto desse trabalho, buscou-se avaliar as possibilidades e potencialidades de monitorar produtos durante o transporte, utilizando uma arquitetura que permita fácil auditabilidade por qualquer ator da cadeia de suprimento, habilitando maior confiança, cuidado com o transporte e melhor uso dos recursos. O

panorama aqui apresentado contribui para o surgimento do seguinte problema de pesquisa: **é possível rastrear cargas em movimento e monitorar dados de sensores de maneira imutável com IOTA e Sigfox?**

1.1 HIPÓTESES

- a) A tecnologia de registro distribuído IOTA é capaz de suplantar o registro de dados de sensores de maneira imutável e auditável.
- b) A rede LPWAN Sigfox possibilita conectividade de baixo custo e ampla área de cobertura.
- c) A rede LPWAN Sigfox permite envios de mensagens em movimento.
- d) É possível construir um hardware com antena Sigfox, com baixo consumo de energia, e portanto baixo custo e manutenção, para obtenção de geolocalização.
- e) Um ecossistema que possa unir IOTA e Sigfox é capaz viabilizar o registro imutável, auditável, seguro e aplicado a logística na cadeia de suprimentos.

1.2 OBJETIVOS

Nas seções abaixo estão descritos o objetivo geral e os objetivos específicos.

1.2.1 Objetivo Geral

O objetivo geral desta dissertação visa modelar, implementar e analisar um protótipo para monitoramento e rastreamento de cargas perecíveis em movimento usando a DLT baseada em DAG, IOTA/Tangle, combinado com rede LPWAN Sigfox.

1.2.2 Objetivos Específicos

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

- a) identificar características da tecnologia baseada em DAG da IOTA;
- b) identificar características da tecnologia da rede LPWAN Sigfox;
- c) desenvolver um protótipo como prova de conceito baseada no Tangle da IOTA usando SigFox para comunicação e rastreamento de cargas móveis;
- d) avaliar as potencialidades e limitações do protótipo na cadeia de suprimentos para rastreamento e monitoramento de cargas móveis;

1.3 ADERÊNCIA DO OBJETO DE PESQUISA AO PPGTIC

O Programa de Pós-Graduação em Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC) tem como área de concentração Tecnologia e Inovação, dividida em três linhas de pesquisa, são elas: Tecnologia Computacional, Tecnologia Educacional e Tecnologia, Gestão e Inovação.

O objetivo da linha de pesquisa em “Tecnologia Computacional”, é desenvolver modelos, técnicas e ferramentas computacionais auxiliando na resolução de problemas de natureza interdisciplinar. Especificamente, esta linha de pesquisa procura desenvolver novas tecnologias computacionais para aplicação nas áreas de educação e gestão (PPGTIC, 2020).

A linha de pesquisa “Tecnologia, Gestão e Inovação” trabalha com novas tecnologias da informação e comunicação para o desenvolvimento de novas metodologias, técnicas e processos para a gestão das organizações (PPGTIC, 2020).

Este trabalho tem aderência às duas linhas de pesquisas citadas, “Tecnologia, Gestão e Inovação” e “Tecnologia Computacional”. O projeto está relacionado à melhoria de gestão na cadeia de suprimentos a partir de uma série de novas tecnologias, como O *ledger* distribuído da criptomoeda IOTA e rede LPWAN sigfox, bem como implementações de software e hardware caracterizando também a aproximação com a linha computacional.

Os trabalhos com produções dentro do PPGTIC que mais se relacionam com a pesquisa apresentada neste trabalho são:

- ROSA, Reginaldo José da. Modelo de logística reversa baseado em contabilidade distribuída - Blockchain. Dissertação (Mestrado em Tecnologia de Informação e Comunicação), Universidade Federal de Santa Catarina. Araranguá, p. 136. 2019.
JULIANO OLIVEIRA DE ALMEIDA

- ALMEIDA, Juliano Oliveira de. Metodologia de avaliação técnico-científica de aplicações Blockchain: um estudo de caso no setor elétrico. Dissertação (Mestrado em Tecnologia de Informação e Comunicação), Universidade Federal de Santa Catarina. Araranguá, p. 170. 2021.

- DA ROSA, Reginaldo José et al. TECNOLOGIAS DE CONTABILIDADE DISTRIBUÍDAS (DLTS): EVOLUÇÃO, DIFERENÇAS, SIMILARIDADES E VANTAGENS. Humanidades Inovação, v. 7, n. 9, p. 231-243, 2020.

1.4 METODOLOGIA

Este é um projeto de natureza aplicada, com objetivos exploratórios e procedimentos experimentais, estas características se enquadram em uma pesquisa tecnológica. Consistindo na utilização de conhecimento da pesquisa básica e da tecnologia para se obter aplicações práticas em produtos e processos. A metodologia empregada

para o desenvolvimento do trabalho é classificada em oito etapas, que são mostradas na Figura 1.

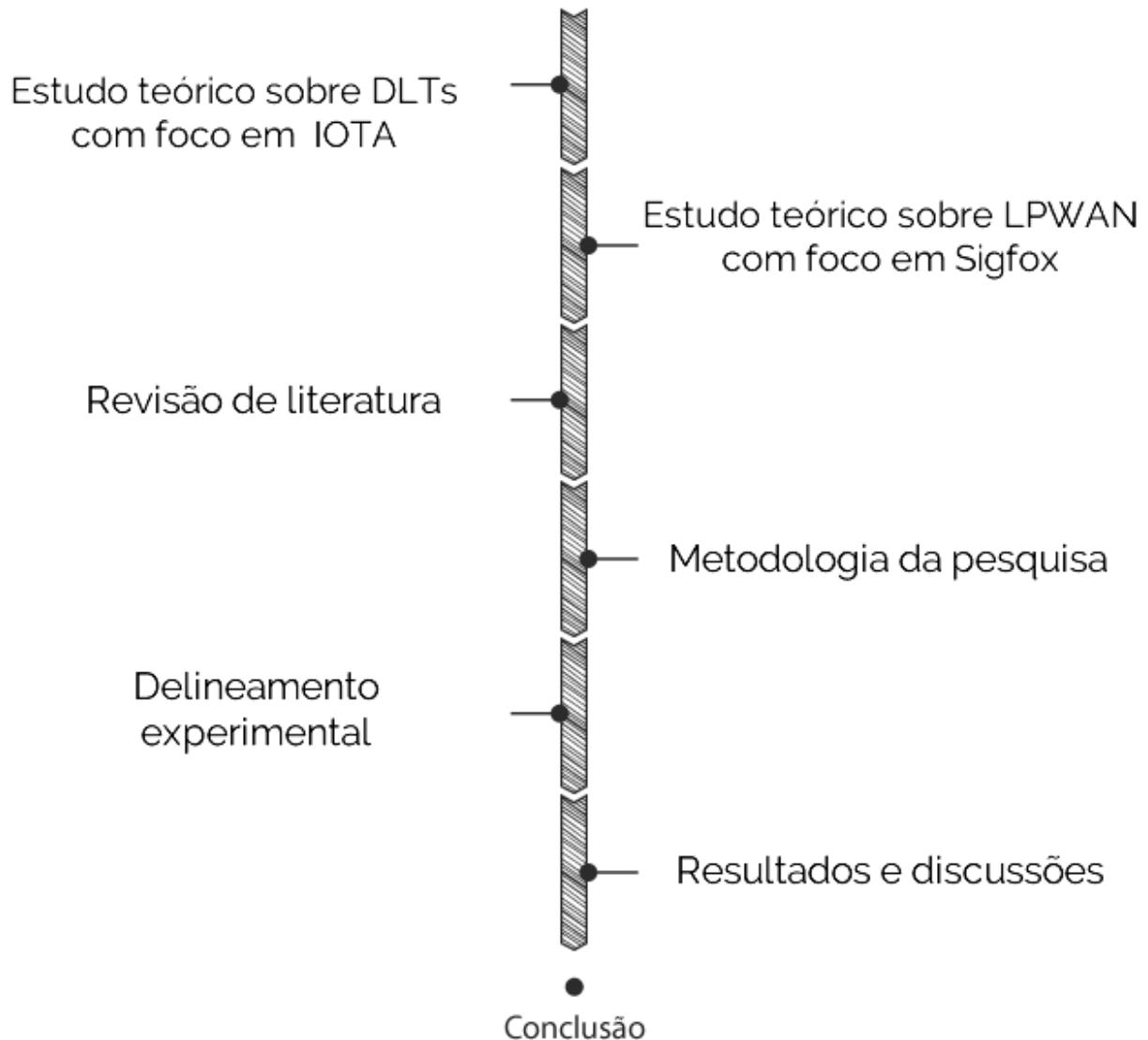


Figura 1 – Quadro geral de desenvolvimento do trabalho

Para realização dos estudos teóricos (Capítulos 2 e 3), serão realizadas pesquisas que contribuam para o bom entendimento da tecnologia. Com especial foco nas documentações fornecidas pelos seus desenvolvedores, a fim de compreender melhor o sistema como um todo;

A revisão de literatura (Capítulo 4), irá indicar caminhos que a pesquisa relacionada a este trabalho está sendo feita, com isso também irá localizar o trabalho proposto e suas possíveis contribuições científicas, além de embasar as discussões

posteiros;

A metodologia da pesquisa (Capítulo 5), destaca a arquitetura do protótipo, tecnologias envolvidas e desenvolvimento do protótipo;

O delineamento experimental (capítulo 6), apresenta os métodos experimentais propostos para validação, compreensão e identificação de limitações do sistema proposto.

Em resultados e discussões (Capítulo 7) é onde encontram-se documentados os resultados e implicações das experimentações. As experimentações visam investigar as escolhas de hardware e desenvolvimento do software, bem como avaliar o ecossistema proposto.

A conclusão (Capítulo 8) sintetiza os resultados, responde à pergunta de pesquisa e hipóteses, bem como apresenta outras potencialidades e possibilidades descobertas ao longo do processo de pesquisa.

1.5 CONTRIBUIÇÕES PARA LITERATURA

As publicações científicas consideradas para o cumprimento parcial dos requisitos do Mestrado:

- SILVANO, Wellington Fernandes; MARCELINO, Roderval. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future Generation Computer Systems, v. 112, p. 307-319, 2020.

- SILVANO, Wellington Fernandes; DANIEL, De Michele; DANIEL, Trauth ; RODERVAL, Marcelino. IoT sensors integrated with the distributed protocol IOTA/Tangle: Bosch XDK110 use case. X Brazilian Symposium on Computing Systems Engineering (SBESC). IEEE, 2020. p. 1-8.

- SILVANO, Wellington Fernandes; MARCELINO, Roderval; VIGIL, Martin Augusto Gagliotti. Tecnologia Blockchain - IOTA aplicada a rastreabilidade de produtos. Revista Tecnologia e Sociedade, v. 17, n. 46, p. 201-215, 2021.

1.5.1 Distinções

- O artigo “A cryptocurrency to communicate Internet-of-Things data”, foi escolhido pelo editor da Future Generation Computer Systems como um dos três artigos de maior interesse da comunidade no semestre, concedendo-lhe acesso aberto. Disponível em: <https://www.sciencedirect.com/journal/future-generation-computer-systems/special-issue/10CTWKXFT8R>

- Segundo melhor artigo do X Brazilian Symposium on Computing Systems Engineering (SBESC). Disponível em: <https://sbesc.lisha.ufsc.br/sbesc2020>

2 TECNOLOGIA DE REGISTRO DISTRIBUÍDO

As DLTs atraíram atenção com a introdução da Blockchain do Bitcoin em transações financeiras. Um dos principais objetivos dos DLTs é possibilitar que mesmo usuários que não confiam uns nos outros possam interagir sem a necessidade de um terceiro confiável (WALPORT, 2016). As DLTs são relevantes em cenários onde existe um certo grau de desconfiança entre as partes, como parceiros de negócios ou entidades anônimas (PAHL *et al.*, 2018). Por design, DLTs adicionam um nível de transparência, rastreabilidade e segurança a este tipo de ambiente (EL IOINI; PAHL, 2018). Em sua essência, DLTs são estruturas de dados para registrar transações e um conjunto de funções para manipulá-las. Cada DLT se diferencia usando diferentes modelos de dados e tecnologias, geralmente, todas as DLTs são baseadas em três tecnologias bem conhecidas, (1) criptografia de chave pública, (2) redes *peer-to-peer* distribuídas e (3) mecanismos de consenso, que são combinados de uma forma única e inovadora. Como o objetivo é operar em um ambiente não confiável, a criptografia de chave pública é usada para estabelecer uma identidade digital segura para cada participante. Cada participante é equipado com um par de chaves (uma pública, outra privada) para poder registrar as transações no *Ledger Distribuído* (EL IOINI; PAHL, 2018). Uma rede ponto a ponto é empregada para ser capaz de expandir a rede, evitar um único ponto de falha e impedir que um único ou pequeno grupo de participantes assuma o controle da rede. Um protocolo de consenso permite que todos os participantes, ou seja, todos os nós da DLT, concordem com a versão da verdade, sem a necessidade de um terceiro de confiança (EL IOINI; PAHL, 2018). Um DLT portanto, fornece um livro razão imutável que não pode ser alterado e elimina a necessidade de um terceiro confiável.

O Bitcoin é a primeira criptomoeda descentralizada, surgiu em uma lista de discussão de criptografia no ano de 2008, no entanto, começou a operar em janeiro de 2009 (NAKAMOTO, 2018) (HILEMAN; RAUCHS, 2017). A segunda criptomoeda emergiu dois anos depois, em abril de 2011, com o nome de Namecoin (HILEMAN; RAUCHS, 2017). Hoje, existem mais de 6000 criptomoedas com valor de mercado (CAPITALIZATIONS, 2020). O elemento comum da maioria das criptomoedas é a utilização do que se convencionou chamar de Blockchain, o sistema por trás do Bitcoin e outras criptomoedas. A rede Blockchain é um tipo de DLT (FLOREA, Bogdan Cristian; TARALUNGA, 2020).

No entanto, alguns desafios e limitações da Blockchain favoreceram o surgimento de criptomoedas baseadas em grafos acíclicos dirigidos (Directed Acyclic Graph — DAG), por volta de 2014. Essas soluções buscam resolver algumas limitações da Blockchain, como o consumo maciço de energia, atraso na validação das transações e alta taxas financeiras (PARK *et al.*, 2019). São exemplos de criptomoedas baseadas

em DAG: IOTA, Dagcoin, Nano, Byteball, NXT, XDAG e Orumesh (YEOW *et al.*, 2018) (FERRARO *et al.*, 2018) (PERVEZ *et al.*, 2018).

IOTA é um sistema público, distribuído, criado para fornecer amparo para internet das coisas (IOTA, 2020), na forma de uma criptomoeda (POPOV, 2016). O sistema da IOTA foi conceituado pela primeira vez em 2014, sua origem está intimamente relacionada a internet das coisas e computação distribuída na forma de criptomoedas.

Esse capítulo tem por objetivo apresentar brevemente a Blockchain e suas limitações para IoT e o protocolo distribuído Tangle da IOTA. Primeiramente são apresentados conceitos básicos e limitações da Blockchain, em seguida são descritos os fundamentos e características do ecossistema IOTA/Tangle. Por fim, são apresentadas as principais bibliotecas e ferramentas que viabilizam o desenvolvimento de uma prova de conceito capaz de explorar os potenciais desta tecnologia para registro de dados de dispositivos IoT.

2.1 CONTEXTUALIZAÇÃO: BITCOIN E BLOCKCHAIN

O *paper* intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System” deu origem aos fundamentos do Bitcoin (NAKAMOTO, 2008). O Bitcoin é descrito como uma versão de dinheiro eletrônico que permite realizar pagamentos *on-line* diretamente de uma parte para outra, sem a necessidade de passar por uma instituição financeira, de forma a transacionar valores sem intermediários (NAKAMOTO, 2008). O conjunto de soluções que tornou isso possível, é o que conhecemos hoje por Blockchain.

A Blockchain pode ser entendida como uma tecnologia de transferência e armazenamento de dados transparente e seguro, que funciona sem um órgão de controle central (LEE, J.-H.; PILKINGTON, 2017). Em particular, a Blockchain foi desenhada para resolver o problema das moedas digitais descentralizadas, o problema dos gastos duplos (“se não há autoridade central, o que impede uma parte mal-intencionada de gastar a mesma unidade de moeda várias vezes?”) (SIIM, 2018). Em uma rede Blockchain, qualquer alteração dos dados é refletida em toda a rede (WALPORT, 2016) através de um mecanismo de consenso, para que as informações replicadas não possam ser alteradas por um usuário ou um grupo de usuários (FLOREA, B. C., 2018). Um Blockchain é um tipo de banco de dados distribuído, com alto grau de imutabilidade e segurança, uma ideia que remonta, pelo menos, a década de 1970 (SHERMAN *et al.*, 2019). Dentre as propriedades intrínsecas, destacam-se: operação sem necessidade de confiança, imutabilidade, transparência, fácil verificação, segurança criptográfica, audibilidade e independência de terceiros (BARTOLOMEU *et al.*, 2018).

A origem do nome Blockchain (ou cadeia de blocos) denúncia parte do funcionamento do sistema. Em síntese, transações são agrupadas em blocos que são encadeados(ligados) uns aos outros de forma linear (NAKAMOTO, 2008). Um bloco, possui ao menos: informações gerais; *hash* anterior; e *hash* atual. Onde o *hash* é um

identificador único do bloco. A Figura 2 apresenta uma versão simplificada dos blocos na Blockchain.

Figura 2 – Representação simplificada de blocos na Blockchain



Fonte – (SILVANO, W., 2019)

Assim, cada bloco é vinculado ao anterior de modo a formar uma lista vinculada. No protocolo Bitcoin Core, um bloco é gerado a cada 10 minutos, o tamanho de um bloco é limitado a 1MB de tamanho, permitindo até 4.000 transações no bloco(GÖBEL; KRZESINSKI, 2017). Os mineradores (computadores participantes da rede Blockchain) fazem a validação de transações; gastam seu poder computacional para validar e guardar o histórico dessas, e por isso recebem incentivos financeiros, via taxas e criação de novas moedas a cada novo bloco gerado. O sistema descrito por Nakamoto, também inclui detalhes de como os blocos são encadeados, como se dá o algoritmo de consenso, como são propagados os incentivos financeiros e como são evitados gastos duplos (NAKAMOTO, 2008).

2.1.1 Limitações da Blockchain

Há quatro principais limitações da Blockchain para armazenamento de dados de dispositivos IoT.

2.1.1.1 Escalabilidade

Apesar das potencialidades, a Blockchain possui dificuldades intrínsecas de serem “descentralizadas”, “seguras” e “escalonáveis” ao mesmo tempo. A princípio os sistemas Blockchain podem ter, no máximo, duas dessas três propriedades, um problema conhecido como “Trilema da escalabilidade” (BUTERIN, 2018). A estrutura

sequencial das Blockchains permitem rastrear qualquer registro armazenado no histórico, por outro lado, também é o que dificulta significativamente o rendimento da transação; a natureza de uma lista linear de blocos é o maior gargalo em sua capacidade de escalar (PERVEZ *et al.*, 2018). Com o aumento da demanda, a escalabilidade da Blockchain se mostra limitada, pois as transações podem demorar muito a entrarem na rede, visto a quantidade limitada de informações por bloco e o tempo médio de novas validações (GÖBEL; KRZESINSKI, 2017).

Protocolos Blockchain podem aumentar o tamanho do bloco, ou diminuir o tempo médio de transação. No entanto, essa restrição é resultado de uma decisão de construir uma rede Blockchain descentralizada, em que mais computadores possam participar e armazenar todo o histórico de transações em seu computador. Há várias soluções sendo desenvolvidas, baseadas em Blockchain, para resolver limitações, incluindo canais de pagamento fora da cadeia, como o Lightning Network que aumenta os tamanhos dos blocos, como o Bitcoin Cash faz ou como o Dash usa os nós mestres para validar transações instantaneamente (DIVYA; BIRADAR, 2018). Embora essas soluções possam funcionar, o que está acontecendo de fato, é um aumento da centralização em favor de maior escalabilidade, elas não alteram o fato de que o design das Blockchains não se adaptam bem nativamente.

2.1.1.2 Consumo de energia

O aumento da rede Blockchain resulta também, em consumo alto de energia elétrica (FLOREA, B. C., 2018). Essa relação existe, pois é necessário realizar uma prova de trabalho (*Proof-of-Work — PoW*) para gerar o próximo bloco(FLOREA, B. C., 2018). Em setembro de 2018, a Bitcoin chegou a consumir mais de 73 TWh de energia por dia, mais do que a quantidade consumida pela Suíça(SHERMAN *et al.*, 2019). A Power compare, fez um estudo do gasto energético com atividades de mineração, alegando que em novembro de 2017 o consumo de energia do Bitcoin representou cerca de 0,13% de toda a geração de energia do mundo, naquele momento se o Bitcoin fossem um país, ele seria o 61º (COMPARE, 2019).

2.1.1.3 Taxas para transações

Uma desvantagem notável é o conceito de uma taxa de transação para transações de qualquer valor. Existem dois tipos distintos de participantes no sistema, aqueles que emitem transações e aqueles que aprovam transações, os mineradores. As recompensas dadas aos mineradores são variáveis, com o aumento da demanda há também um aumento do tempo médio de validação da transação o que ocasiona taxas ainda mais altas pois garantem atrasos menores (MARINO *et al.*, 2019). A importância dos micro pagamentos aumentará no setor de IoT em rápido desenvolvimento.

Pagar uma taxa maior que a quantidade de valor transferida não é lógico (POPOV, 2016) (PERVEZ *et al.*, 2018).

2.1.1.4 Redundância

Ter uma cópia de todas as transações com todos os pares da rede é muito caro e redundante. Uma das principais vantagens do Blockchain foi a eliminação dos intermediários e a introdução do modelo de auto governança envolvendo apenas os participantes. Ironicamente, essa eliminação dos intermediários resultou na introdução de uma rede altamente redundante (AMMOUS, 2016).

É importante destacar que redes que usam Blockchain de maneira privada, não permissionada, minimizam esse impacto. Quanto maior a quantidade de nós minadores na rede Blockchain, maior a relevância desse fator.

2.2 ECOSSISTEMA IOTA/TANGLE

IOTA é uma criptomoeda que promete alta escalabilidade, transferências rápidas a custo zero focada em soluções para IoT (POPOV, 2016). A tecnologia distribuída baseada em DAG da IOTA, foi apresentada primeiramente por Popov (2016). O título do artigo original foi chamado de “Tangle” e revisado muitas vezes com o nome de “The Tangle”(POPOV, 2016). No entanto, a Fundação Iota, responsável pelo desenvolvimento do protocolo distribuído Tangle, separou didaticamente as etapas de desenvolvimento do projeto em 3 grupos, “IOTA 1.0”, “IOTA 1.5” e “IOTA 2.0” (FOUNDATION, 2020); no entanto o primeiro *Whitepaper* disponibilizado pela equipe não foi completamente implementado e no contexto desse trabalho será chamado de “IOTA 0”. A fundação IOTA está finalizando a versão 1.5 (IOTA, 2019). As principais modificações das versões posteriores estão relacionadas a eliminação de uma certa centralização do protocolo.

Independentemente da versão do protocolo as premissas do “IOTA 0” continuam válidas, em vez de encadear blocos (que contêm transações) de maneira linear, no Tangle são encadeadas transações. Cada nova transação na rede Tangle possui referência a duas transações anteriores. Sempre que um participante quiser adicionar uma nova transação no Tangle, deverá ser realizada uma pequena prova de trabalho e aprovar duas previamente anexadas. Quando uma nova transação aprova duas transações anteriores, é como se existisse uma declaração “Certifico que essas transações são verificadas, assim como todos os seus antecessores, e seu sucesso está atrelado ao meu sucesso” (POPOV, 2016). À medida que novas transações são inseridas, mais transações são autorizadas/validadas e inseridas, resultando em uma rede distribuída de transações duplamente verificadas.

O consenso, portanto, está relacionado ao número de aprovações que uma

determinada transação possui. A transação que recebe aprovações adicionais tem um nível mais alto de confiança (POPOV, 2016). O que é radicalmente diferente da Blockchain, pois não há mineradores, São os próprios usuários da rede que validam as transações (SARFRAZ *et al.*, 2019) (POPOV, 2016). Todos os participantes da rede são responsáveis pelo consenso. Portanto, o custo de uma transação envolve apenas o custo computacional da validação de duas outras transações.

O problema de gasto duplo é fator determinante para criptomoedas distribuídas (CHOHAN, 2017). Esse desafio está relacionado a uma possível falha potencial em uma criptomoeda, na qual o mesmo *token* digital possa ser gasto mais de uma vez. O problema do gasto duplo levanta questões sobre a proteção de uma moeda digital, da mesma maneira que as moedas tradicionais devem ser protegidas. A fraude precisa ser evitada, com questões subjacentes de segurança na proteção de uma informação digital. O problema de gasto duplo exerce pressão inflacionária ao criar uma nova oferta de moeda fraudulenta que não existia anteriormente, degradando assim o valor da moeda digital em relação ao nível geral de preços. Por sua vez, isso compromete a governança e a responsabilidade associadas à confiança do usuário na moeda (CHOHAN, 2017) (ROSENFIELD, 2014). O cerne da questão está relacionado à como obter consenso, de maneira segura, o que também acaba impactando na segurança em trocas de dados.

As características únicas da rede Tangle viabilizam micro transações e trocas de dados na rede distribuída. A escalabilidade também é impulsionada, visto que não é necessário esperar pelo próximo “bloco” como na Blockchain. Em teoria, quanto maior a quantidade de transações, menor será a latência entre transações. Para entender o consenso e como o Tangle lida com o problema dos gastos duplos, é essencial conhecer mais profundamente a tecnologia.

A implementação do Tangle na rede IOTA envolve uma série de dificuldades, soluções e conceitos, que impactam em características únicas. O ecossistema da rede IOTA envolve conceitos como “*tip*”, “peso acumulado”, “*snapshot*”, “*permanode*”, “*FullNode*”, “*LighNodes*”, “*Masked Authenticated Messaging*”, “*private key*”, “*public key*” e “coordenador”. Tais conceitos e soluções são descritos a seguir.

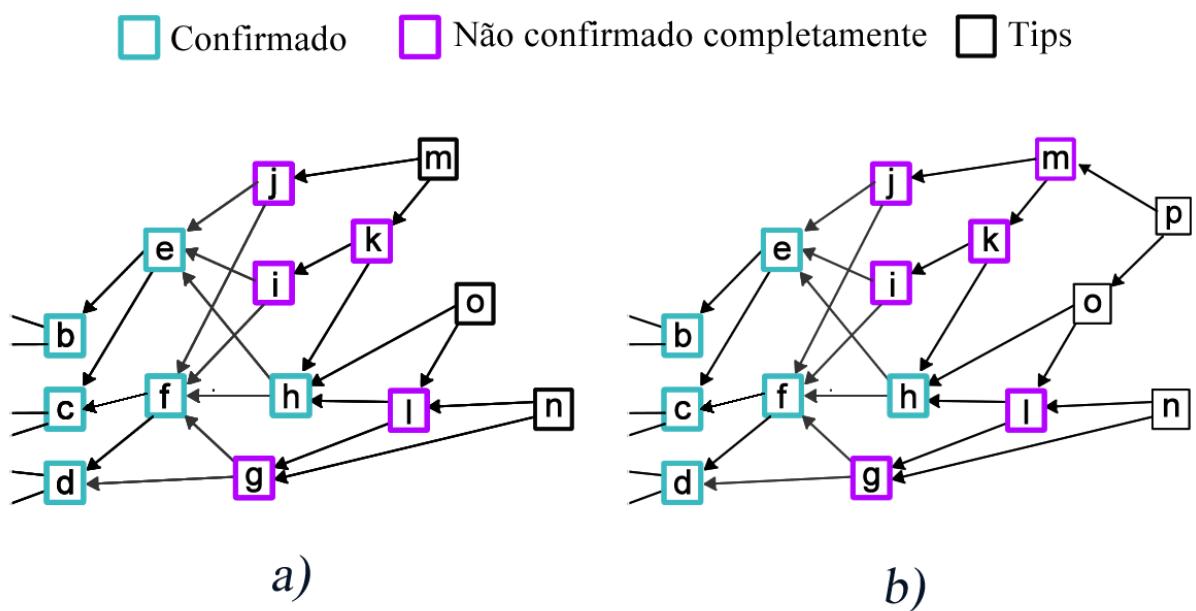
2.2.1 Tangle

As principais características da rede Tangle foram descritas por Popov (2016) e é base dessa subseção. A rede Tangle é composta por nós que são entidades que emitem e validam transações no Tangle, cada nó também representa uma transação (POPOV, 2016). O processo de anexar uma transação ao Tangle é o seguinte: (1) um nó escolhe duas outras transações para aprovar, de acordo com um algoritmo de seleção de ponta Markov Chain Monte Carlo (MCMC); (2) o nó verifica se às duas transações estão ou não em conflito e desaprova transações conflitantes (gastos du-

plos); (3) para que o nó emita uma transação válida, ele deve resolver um tipo de prova de trabalho (PoW), isso é conseguido encontrando um nonce (POPOV, 2016), esse esforço computacional é uma versão muito mais leve que a realizada pela Blockchain (FERRARO *et al.*, 2018); (4) depois disso, o usuário envia sua transação para a rede, e ela se torna uma “tip”(transação não aprovada); (5) a transação aguarda confirmação por aprovação direta ou indireta até que seu peso acumulado atinja o limiar predefinido.

As transações no Tangle ocorrem de forma assíncrona, os nós frequentemente não veem o conjunto de todas as transações. Na figura Figura 3a, o nó “m”, não sabe dos acontecimentos no ramos que contêm as transações “o”, “n”, “l” e “g”, no entanto validou as transações “k” e “j”. A implicação da assincronicidade é a possibilidade da existência de transações conflitantes, seria possível que a transação “k” esteja em conflito com a transação “g” visto que em nenhum momento ambos passaram por verificação juntos.

Figura 3 – Grafo representativo de parte do Tangle. a) Estado em um tempo t qualquer
b) Estado t+1, com uma transação nova p



Fonte – O autor (2020)

No momento que a transação “p” valida “m” e “o” na Figura 3b, existe uma verificação de cada uma das transações vinculadas direta ou indiretamente, incluindo “k” e “g”; nesse momento, caso haja conflito (gastar o mesmo valor duas vezes), ele é identificado, e seria necessário escolher qual ramo ficará órfão. Segundo Popov (2016), para decidir qual ramo deve ser abandonado a regra é executar o algoritmo de seleção de pontas muitas vezes, identificando qual das duas transações têm maior probabilidade de ser indiretamente aprovada pela “tip” selecionada. O ramo que tiver

maior probabilidade é escolhido, e o outro abandonado.

O algoritmo de seleção de pontas é útil para escolher transações a serem validadas, e também tem protagonismo para resolução de conflitos, daí a necessidade de priorizar um ramo do Tangle utilizando uma métrica (em “IOTA 0 e IOTA 1” o peso (*weights*) das transações). O consenso no Tangle está relacionado ao peso acumulado. Para Popov (2016), peso é proporcional a quantidade de trabalho investida para validar a transação, na implementação atual 3^n ; para um n inteiro positivo. A ideia é que uma transação com maior peso seja mais importante. O peso acumulado é definido como o peso da transação mais a soma dos pesos de todas as transações que direta ou indiretamente aprovarem ela. O que significa que a cadeira de maior peso acumulado tende a crescer, enquanto os outros ramos tendem a ficarem isolados, com baixa probabilidade de certeza. Outra consequência é que as “*tips*” tendem a ser aquelas selecionadas para serem validadas.

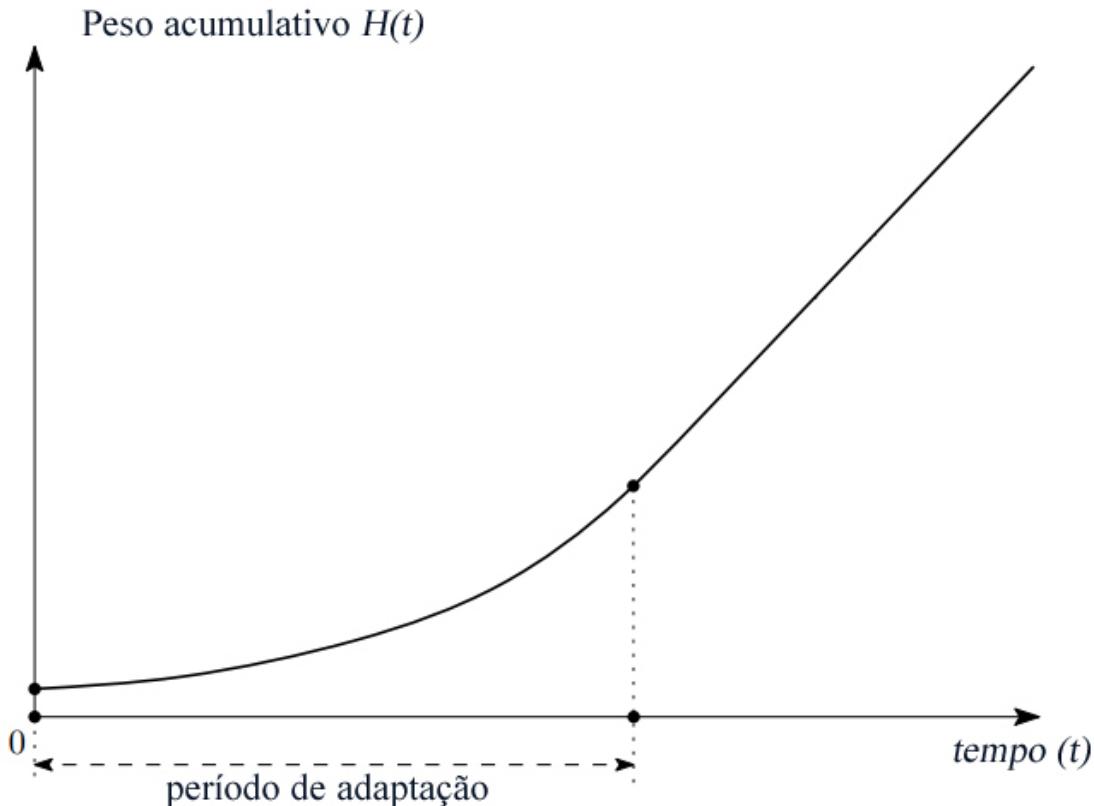
Dependendo do grau de importância de uma transação, pode-se entender que será aceita como válida, quando seu ramo no Tangle for escolhido em “97%” (por exemplo) das vezes pelo algoritmo de seleção de pontas, ou seja, 97% seria o grau de confiança. Em outras palavras, quando quase todas as “*tips*” participarem daquela parte da cadeia. Uma maneira de estudar a adoção de uma transação pela rede, é justamente por meio de uma análise do peso acumulado. Tendo em vista que em determinado momento este deve crescer linearmente, para uma rede que possua um crescimento homogêneo. Popov (2016), estudou esse comportamento, obtendo o peso acumulado de uma transação $H(t)$ em função do tempo médio entre a criação e revelação de uma transação para rede (h) e o passar do tempo (t).

$$H(t) \approx 2\exp(0.352t/h) \quad (1)$$

A Figura 4, apresenta o gráfico para a expressão (1), que indica o comportamento típico do peso acumulado de uma transação. Ela expressa o “tempo de adaptação” de uma transação, visto que ao alcançar um crescimento linear indica que as novas “*tips*” estão indiretamente ligadas a ele, tendo com isso alta probabilidade de certeza que a transação não será abandonada.

É interessante compreender que após um período de adoção, a transação não será abandonada, e podemos confiar que aquela transação é válida e será válida sempre. Na verdade, o percentual exato depende da maturidade da rede e do peso acumulado. O grau de confiança que se necessita dependerá de cada situação. Como um exemplo, micro transações podem exigir 50% de confiança, enquanto a troca de uma grande quantidade de *tokens* podem exigir mais do que 99%. Popov (2016) sugere o algoritmo MCMC para seleção de pontas baseado no fato de que o Tangle principal teria mais poder de *hashing* acumulado (maior peso) do que possíveis atacantes.

Figura 4 – Peso acumulativo x tempo. Em regime de alta carga



Fonte – (POPOV, 2016))

2.2.2 Coordenador

No atual e próximo estágio de desenvolvimento da tecnologia (IOTA 1.0 e IOTA 1.5), a IOTA conta com um Coordenador centralizado para fornecer segurança, dado o risco de atores desonestos que procuram atacar a rede. O consenso na IOTA, atualmente exige que uma transação confirmada seja referenciada (direta ou indiretamente) por uma transação emitida pelo Coordenador (em inglês, Coordinator) (IOTA, C. T., 2019), que é emitido a cada 10 segundos; todas as transações aprovadas por ele são consideradas como tendo uma confiança de 100%, imediatamente (GAL, 2018). O coordenador acaba por facilitar também as verificações de gastos duplos pelas “tips”, tendo em vista que a quantidade de verificações são limitadas até encontrar um marco do coordenador.

A utilização do coordenador na rede IOTA permite maior segurança, perdendo em termos de descentralização. O que não é bem visto enquanto uma criptomoeda, pois, a princípio, permite que a Fundação IOTA escolha quais transações recebem prioridade, congele fundos, ignore transações e é um ponto de ataque central, se o Coordenador parar de funcionar, as confirmações na rede parariam (HANDY, 2017).

Dois artigos fundamentam as premissas de como será retirado o “Coordenador” da rede, eles são intitulados: “*The coordicide*” (IOTA, C. T., 2019); e “*Fast Probabilistic Consensus within Byzantine Infrastructures*” (POPOV; BUCHANAN, 2019), ambos apresentados em maio de 2019. Neles os autores detalham novos esquemas de segurança para rede com a ausência do coordenador e prometem, transações mais rápidas, *time-stamps* confiáveis, ordenadas e um novo algoritmo para controle de taxa, que em teoria, evita que invasores sobrecarreguem a rede. Em caso de sucesso, é importante ressaltar que todas as informações deste trabalho continuam valendo. Foram previstos novos componentes, mas as características fundamentais existentes do Tangle permanecem.

2.2.3 Wallet

Na rede IOTA, uma semente (em inglês, seed) atua como uma senha que concede acesso à carteira (*wallet*) do usuário ou dispositivo. A semente deve ser gerada aleatoriamente e consiste em 81 trytes. Além disso, no ecossistema IOTA, existem os conceitos de “chave privada (*private key*)” e “pública”(*public key*). As chaves privadas são calculadas com *hash* da semente concatenada com o índice de endereço, onde o índice pode ser qualquer número inteiro positivo (IOTA, S., 2019). Chaves públicas são endereços e são calculadas com *hash* em suas chaves privadas associadas. Um endereço contém tokens e pode ser usado como entrada (o *token* é gasto) ou como saída para uma transação (o endereço recebe um *token*). Os fundos de todos os endereços (chaves públicas) são somados para calcular o saldo da conta de um usuário (SHAFEEQ *et al.*, 2019).

O protocolo IOTA usa o *Winternitz One-Time Signature (WOTS)*, uma assinatura criptográfica baseada em *Hash* (SHAFEEQ *et al.*, 2019) que é bastante promissora e resistente a computadores quânticos (BUCHMANN; DING, 2008). Como o protocolo IOTA usa WOTS, a segurança de um endereço específico, diminui à medida que aumenta o número de vezes que ele é usado (SHAFEEQ *et al.*, 2019). Se o usuário muitas vezes reutiliza um endereço (a mesma chave pública), é fácil para outras pessoas analisar os gastos de uma pessoa. Portanto, uma análise de dados de uma transação pode identificar o histórico e o saldo da transação, como o que acontece com o Bitcoin e outras criptomoedas (SARFRAZ *et al.*, 2019). É preferível usar um novo endereço (chave pública) para receber pagamentos. A IOTA possui um serviço de mixagem dedicado para melhorar o anonimato (SARFRAZ *et al.*, 2019).

Esse problema ocorre porque cada vez que os *tokens* são enviados de um endereço, o emissor deve aprovar a movimentação de *tokens* do seu endereço. Isso é alcançado usando uma chave privada exclusiva na transação. No entanto, toda vez que a assinatura é criada, ela revela 50% da chave privada associada ao endereço que liberou os *tokens* (SHAFEEQ *et al.*, 2019). Se o usuário reutilizar um endereço para

assinar várias transações de saída, isso resultará na exposição de uma grande fração da chave privada correspondente, o que facilita para um adversário forjar a assinatura para roubar fundos.

O atual protocolo da IOTA reduz os problemas de reuso de endereços, usando bibliotecas que examinam transações no Tangle em busca de endereços já utilizados. Se um endereço já tiver sido usado, ele não poderá receber *tokens*. No entanto, existem os *snapshots* (capturas instantâneas), que removem o histórico de transações. Portanto, um endereço gasto pode receber *tokens* após um instantâneo, porque o histórico de transações é limpo e os endereços que não contêm mais saldo são esquecidos, tornando impossível verificar transações antigas. (SHAFEEQ *et al.*, 2019).

2.2.4 Light Node e FullNode

Existem dois tipos de nós no protocolo IOTA, o *FullNode* (nó completo) e o *Light node* (nó leve). O *FullNode* é completamente independente, portanto, precisa de vizinhos para participar da rede para sincronizar o Tangle. O *Light Node* possibilita a conexão com um *FullNode* remoto (seja próprio *FullNode* ou fornecido publicamente), a fim de obter o estado mais recente da rede, buscando principalmente validações das duas transações necessárias para emitir uma transação (IOTA, F., 2020).

Na última etapa do processo de envio de transações para o Tangle, os dados do pacote que contém a transação são enviados para a rede. Se um light node for usado, ele será conectado a um *FullNode* e enviará o pacote da transação. Após o verificado e validado com êxito o pacote de transações, a transação é encaminhada para outros nós e o pacote de transações é propagado por toda a rede.

Qualquer pessoa que planeje desenvolver aplicativos de longo prazo para o Tangle deve levar em consideração operar um *FullNode*. Operar um *FullNode* oferece um ponto de entrada seguro no Tangle sob seu próprio controle. A operação do nó completo contribui para a estabilidade e a eficiência geral da rede IOTA, especialmente se as transações forem geradas ativamente por meio dele. Operar um *FullNode* fornece informações valiosas sobre a funcionalidade, desempenho e estabilidade do Tangle. Os fornecedores públicos de *Fullnodes* frequentemente estão sobrecarregados com solicitações de *Light Node* (IOTA, F., 2020).

Um *FullNode*, é basicamente um servidor conectado à internet no qual uma instância executa a biblioteca oficial (IRI) da IOTA. Segundo a Fundação IOTA, um *FullNode* deve preferencialmente ser operado em uma instância de servidor dedicada com os seguintes requisitos mínimos: 4Gb RAM, 2 Core, 100Gb SSD/HDD. Em servidor com IP fixo para comunicar-se com seus vizinhos. Um guia completo para instalação de um *Full node* pode ser encontrado nos endereços:

- <https://iri-playbook.readthedocs.io/en/master/>;
- <https://www.iota.partners/>;

- <https://docs.iota.org/docs/node-software/0.1/iri/references/iri-configuration-options>.

2.2.5 Snapshot

Como uma grande quantidade de dados estão sendo trocados, a rede cresce rapidamente, especialmente por permitir transações de valor zero, com a transferência apenas de dados, por esse motivo a implementação do Tangle inclui o '*snapshot*'. Ao realizar um '*Snapshot*' restam apenas os balanços, todo o restante é apagado. O '*snapshot*' é uma captura instantânea é semelhante à remoção do Blockchain, exceto que o '*snapshot*' tem a vantagem significativa de agrupar várias transferências para o mesmo endereço em um registro, o que leva a um requisito de armazenamento menor (SØNSTEBØ, 2017). No passado, a Fundação IOTA fazia “*Global Snapshots*” em intervalos irregulares. Hoje, existem instantâneos locais que substituem os globais. Os instantâneos locais do Tangle são obtidos independentemente por *Fullnodes*, manuais ou totalmente automáticos.

2.2.6 Permanode

Existem certas aplicações que necessitam manter dados brutos completos, por exemplo, uma auditoria transparente exigirá essa capacidade. Este é o papel de *Permanodes*. Um '*Permanode*' armazena todo o histórico e dados do Tangle de forma permanente e segura (SØNSTEBØ, 2017). Outra alternativa seria manter um *Full-Node*, ou *LigthNode* sem “*snapshutting*” sobre domínio da pessoa ou organização que precisa daqueles dados. O permanode está em desenvolvimento, mas consiste basicamente em um banco de dados com características específicas.

2.2.7 Masked Authenticated Messaging

A rede IOTA permite o envio de transações sem a troca de *tokens*, portanto um endereço pode ser utilizado para guardar dados de medição. As transações são públicas. Como impedir que um invasor falsifique dados de medição ou interfira com *spams*? Seria possível controlar o acesso desses dados por outros usuários? O ‘Mensagens autenticadas mascaradas’ (em inglês, *Masked Authenticated Messaging - MAM*) foi desenvolvido para resolver esse tipo de questão.

O MAM atua como um protocolo de comunicação de dados, criptografando e autenticando fluxos de dados, ele é um módulo baseado no protocolo IOTA que fornece funções para enviar e ler fluxos de mensagens usando o Tangle. A criptografia das mensagens é conhecida como “criptografia pós-quântica”, acredita-se que os algoritmos criptográficos pós-quânticos sejam seguros contra um ataque por um computador quântico suficientemente forte (BROGAN *et al.*, 2018). A criptografia e o sistema de

autenticação visam garantir que as mensagens não foram alteradas e realmente vêm de um remetente específico.

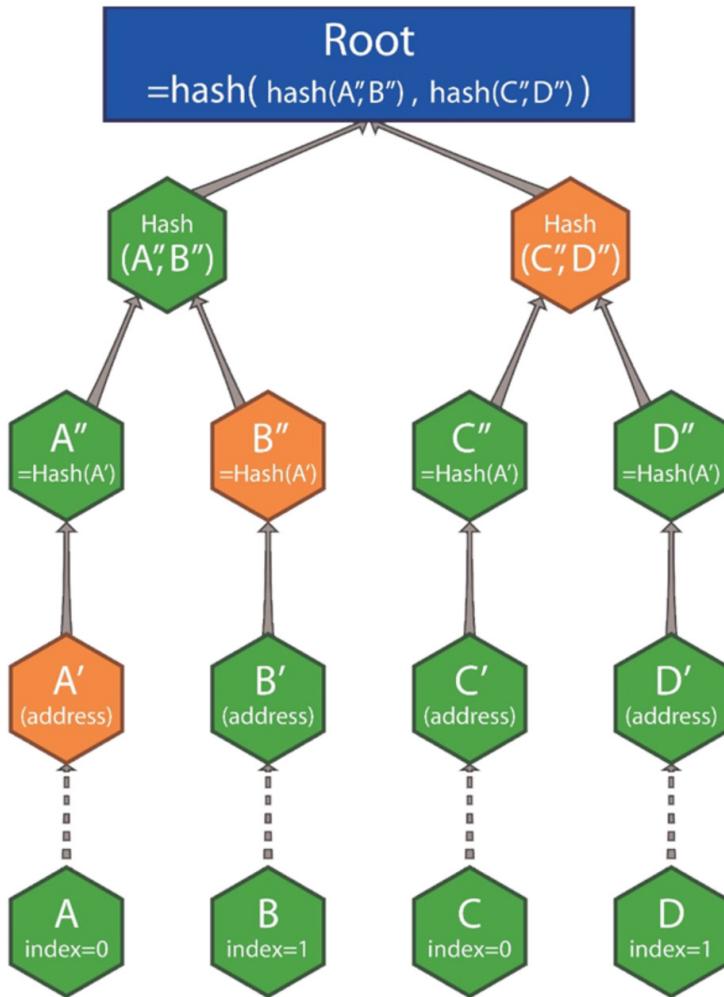
Com o MAM, um fluxo de mensagens vinculadas é criado a partir de mensagens individuais, enviando cada mensagem individual para um novo endereço na forma de transações no Tangle. Cada mensagem é vinculada à mensagem subsequente (HANDY, 2017), dada a transação n , tem-se o ponteiro para a transação $n + 1$. No entanto, eles não têm conhecimento da localização da transação $n - 1$. Portanto, eles não podem ler nenhuma mensagem em um fluxo de dados antes de seu ponto de entrada. Isso permite o sigilo antecipado, que é a noção de apenas poder ler transações futuras (BROGAN *et al.*, 2018).

O MAM usa o esquema de assinatura Merkle (*Merkle signature scheme — MSS*). Este esquema é baseado na (*Merkle Hash Tree - MHT*) combinada com as assinaturas de Uso Único (On time signature — OTS) (BROGAN *et al.*, 2018). O esquema de assinatura Merkle (MSS) é usado porque supõe-se que resista a ataques quânticos de computador e por causa de seus curtos tempos de geração e verificação de assinaturas, além de suas fortes garantias de segurança. O MSS vem com uma prova padrão de modelo de segurança e supera o RSA em muitos aspectos em relação aos tempos de execução (HÜLSING, 2013). O MSS permite que um método use uma chave de verificação pública para verificar vários OTS. Cada mensagem (A, B, C, D na Figura 6) é assinada com um esquema OTS e é uma folha de MHT, apresentada como A, B, C, D, na Figura 6. Aplicando as funções *hash* para encurtar os endereços, a raiz da árvore Merkle pode ser obtida (ZHENG *et al.*, 2019). Cada árvore pode produzir o mesmo número de mensagens que o número de folhas do MHT. Cada folha também contém o endereço da próxima árvore, ou seja, um ponteiro para a próxima mensagem (Direção futura do canal) (ZHENG *et al.*, 2019) (MEDIUM, 2018).

Em essência, funciona como um rádio, onde apenas aqueles com a frequência certa podem ouvir, no MAM, apenas aqueles com os IDs de canal certos obtêm acesso aos dados. (SØNSTEBØ, 2017). O MAM possui três modos de operação diferentes, público, privado e restrito. No modo público, a raiz de uma mensagem é igual ao seu endereço, quem descobrir a raiz pode receber as mensagens. No modo privado, o endereço é o *hash* da raiz. Não é suficiente para saber o endereço. No modo restrito, a carga útil de cada mensagem é adicionalmente criptografada e só pode ser descriptografada com uma *key*. A qualquer momento pode ser gerada uma nova *key* pelo emissor, que pode novamente propagar para os usuários que são autorizados (HANDY, 2017).

É importante enfatizar que as mensagens enviadas ao MAM são transações típicas, com valor zero, ou seja, fazem parte do Tangle, como outras transações. A diferença é como as mensagens são vinculadas entre si no Tangle. Essas mensagens fazem parte da razão distribuída e contribuem para a segurança da rede, aumentando

Figura 5 – Exemplo de uma *Merkle Hash Tree* — MHT) com 4 folhas.



Fonte – (SILVANO, W. F.; MARCELINO, 2020))

o poder total de *hash* e se beneficiando das propriedades de integridade dos dados da rede, enquanto outras transações continuam a referenciá-las indiretamente (HANDY, 2017) (MARINO *et al.*, 2019).

2.2.8 Bibliotecas e ferramentas

A Fundação IOTA e a comunidade envolvida fornecem várias ferramentas e bibliotecas para permitir o desenvolvimento de aplicações com o Tangle. A seguir são descritas as principais ferramentas e bibliotecas que fazem parte do contexto deste trabalho.

2.2.8.1 Mainnet, Devnet e Spamnet

A rede oficial de nós completos da IOTA é conhecida como Mainnet. Além da Mainnet, a *IOTA Foundation* também opera o chamado Devnet (também conhecido como Testnet). O Devnet é uma cópia tecnologicamente idêntica ao Tangle do Mainnet, ele é usado para desenvolver e testar aplicativos em um ambiente fora da produção. O Spamnet é destinado a testar aplicativos que enviam spam à rede.

2.2.8.2 IOTA Tangle Explorer

O IOTA Tangle Explorer é um sistema web, ele faz acompanhamento do estado atual do Tangle, incluindo rastreamento das transações por endereço, *bundle* e tag da transação. Também é possível verificar quais transações foram aprovadas e quais os dados ou mensagens estão contidas em uma transação. Existem dois ambientes do Tangle explorer.

- Ambiente de teste: <https://comnet.thetangle.org>;
- Ambiente principal: <https://thetangle.org>.

2.2.8.3 IOTA Reference Implementation

O IRI (implementação de referência IOTA. Ou em inglês, *IOTA Reference Implementation*) é um software Java de código aberto que é executado no IOTA Mainnet e no Devnet. Este software define o protocolo IOTA atual, que permite que os nós: a) validem transações; b) armazenem transações válidas no *ledger*; c) permitir que os clientes interajam com eles por meio de uma API HTTP (ROGOZINSKI, 2020).

- Biblioteca IRI: <https://github.com/IOTAledger/iri>

2.2.8.4 IOTA client

Cada interação com o Tangle ocorre através de um *Full node*. Por meio da API do *Full node* ou da API do IRI. A API é uma interface HTTP JSON-REST. Ele é endereçado por meio de solicitações HTTP POST, e retorna dados no formato JSON.(LAUMAIR, 2020),

No contexto desse trabalho, a API do IRI também é chamada de “IOTA client”. Para facilitar o trabalho com a API, a *IOTA Foundation* fornece várias bibliotecas para diferentes linguagens de programação. Além das funções normais como criar transações; assinar transações; gerar endereços; e interagir com um nó IRI; a biblioteca também oferece funções secundárias, para manipular assinaturas ou converter ASCII para Trytes e vice-versa (LAUMAIR, 2020). A documentação da referência pode ser encontrada nos seguintes endereços:

- Biblioteca javascript: <https://github.com/IOTAledger/IOTA.js>

- Documentação da API: <https://docs.iota.org/docs/node-software/0.1/iri/references/api-reference>

2.2.8.5 MAM client

O MAM não faz parte do protocolo IOTA , é uma função adicional realizada na forma de um módulo IXI (*IOTA eXtensible Interface*). A funcionalidade real do MAM foi programada no Rust e compilada no WebAssembly. Para poder usar o MAM em Javascript, a Biblioteca JS do Cliente MAM deve estar integrada (JANES, 2019). O código fonte desta biblioteca, incluindo a documentação, pode ser encontrado no endereço:

- <https://github.com/IOTAledger/mam.client.js/>

2.3 CONSIDERAÇÕES FINAIS SOBRE AS CARACTERÍSTICAS DA IOTA

O autor dessa dissertação, com seu orientador, publicou um trabalho de revisão de literatura sobre IOTA (SILVANO, W. F.; MARCELINO, 2020) , nele constam (entre outras coisas) características gerais da IOTA e arquiteturas geral dos sistemas que utilizam IOTA. Esses pontos são destacados a seguir.

IOTA é uma criptomoeda pública semi-descentralizada, capaz de realizar altas taxas de transação, uma vez que as transações ocorrem em paralelo. IOTA não requer consenso imediato, o custo para confirmar e anexar uma transação é zero, pois todos os usuários da rede podem participar do mecanismo de consenso (não existem mineradores). É possível compartilhar e trocar dados e pagamentos sem qualquer taxa, com imutabilidade garantida (SILVANO, W. F.; MARCELINO, 2020).

A atual definição de consenso de IOTA exige que uma transação confirmada seja referenciada (direta ou indiretamente) por uma transação assinada por um computador central; todas as transações aprovadas por ele são consideradas como 100% confiáveis (GAL, 2018). No entanto, ao contrário das transações de valor, as transações de valor zero não requerem confirmação e são transmitidas entre os nós da rede imediatamente após serem emitidas. Como resultado, a camada de dados IOTA é completamente descentralizada e a existência do Coordenador não é afetada.

Ao optar por usar o *Winternitz One-Time Signature (WOTS)* como um protocolo de esquema de assinatura, o IOTA fornece velocidade e forte resistência a ataques de um possível computador quântico. Com o módulo MAM, também é possível compartilhar fluxos de dados, que podem ser criptografados ou não. Embora pequeno, o menor pacote necessário para enviar dados é grande o suficiente para uma transação com as tecnologias LPWAN. Tecnologias que usam DAG como IOTA não suportam contratos inteligentes e têm grande dificuldade em serem completamente descentralizadas. No momento da redação deste texto, essas tecnologias precisam de um ponto central, como o 'Coordenador'. Tecnologias que usam DAG como IOTA não suportam contra-

tos inteligentes e têm grande dificuldade em serem completamente descentralizadas (SILVANO, W. F.; MARCELINO, 2020).

A fraqueza técnica mais investigada é a impossibilidade de reutilizar um endereço devido ao esquema de assinatura WOTS. A segurança de um endereço específico (possibilidade de apropriação de fundos) diminui com o número de vezes que é usado para enviar fundos aumenta. Isso facilita para um adversário forjar a assinatura para roubar fundos, pois cada vez que os *tokens* são enviados, ele revela 50% da chave privada associada. O protocolo IOTA atual atenua os problemas de reutilização de endereço usando uma biblioteca que impede que transações com endereços já utilizados possam ser usados novamente. No entanto, esse protocolo pode não ser capaz de verificar quais endereços já foram usados depois de um *snapshot*. Isso ocorre porque a captura instantânea remove o histórico de transações necessário para verificar se um endereço já foi usado (SILVANO, W. F.; MARCELINO, 2020).

Outra preocupação é garantir que a rede esteja saudável. Com base nos documentos investigados na pesquisa de Silvano e Marcelino (2020), mesmo em cenários em que o atacante emite quase metade das transações, não é suficiente prejudicar a rede de maneira significativa. Haverá um momento em que as transações não serão abandonadas, ou seja, que é segura, e que ela estará permanentemente na rede (SILVANO, W. F.; MARCELINO, 2020).

Sobre as arquiteturas dos projetos que utilizam IOTA/Tangle, pode-se identificar de três diferentes abordagens (Figura 6):

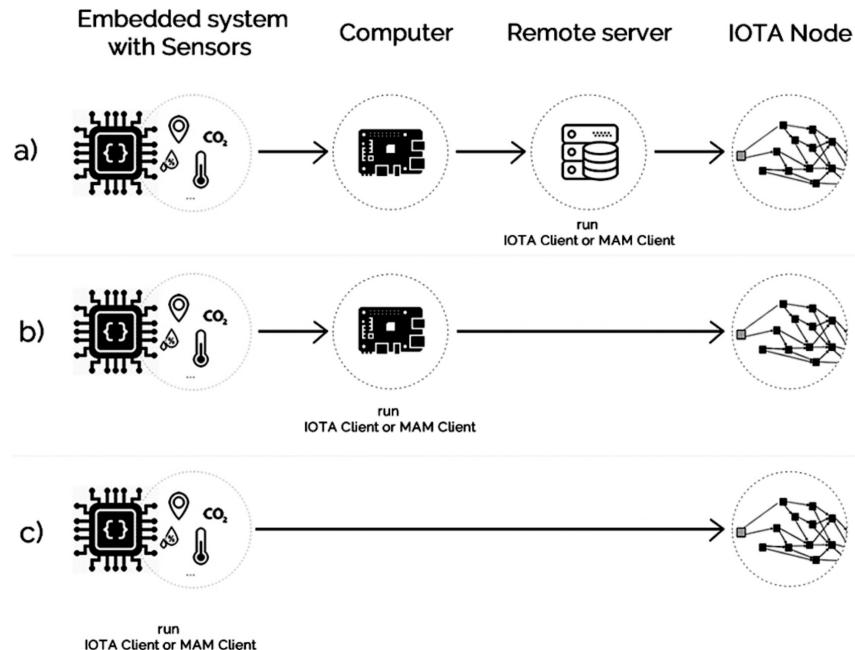
a) Um sistema embarcado conectado aos sensores envia os dados para um computador (telefone celular, computador de placa única ou computador) através de alguma conexão (LoRaWAN, Sigfox, Zigbee, Bluetooth de baixa energia, sem fio). O computador tem a função de enviar dados (não o pacote inteiro) para um servidor remoto (que executa um cliente IOTA ou cliente MAM). O servidor remoto continua a construir o pacote e transmiti-lo para o nó IOTA (nó Light ou Full) (SILVANO, W. F.; MARCELINO, 2020).

b) Um sistema embarcado conectado aos sensores lê os dados e os envia para um computador (telefone celular, servidor remoto, computador de placa única) através de algum tipo de conexão. O computador executando um cliente IOTA ou cliente MAM, continua a gerar o pacote e o transmite para o nó IOTA (SILVANO, W. F.; MARCELINO, 2020).

c) Um sistema embarcado (executando um cliente IOTA ou cliente MAM) conectado aos dados dos sensores lê e constrói o pacote, e o transmite para o nó IOTA (SILVANO, W. F.; MARCELINO, 2020).

A arquitetura do item a) é melhor quando necessário um alto pré-processamento de dados antes da criação da transação e/ou há muitos sensores geograficamente próximos, e o objetivo é minimizar o número de computadores (ou computador de placa

Figura 6 – Arquiteturas de rede possíveis para publicar dados de sensores no Tangle



Fonte – (SILVANO, W. F.; MARCELINO, 2020)

única) necessários. A principal desvantagem é a centralização identificada na figura do servidor remoto. A arquitetura (b) elimina um ponto de falha, em comparação com o anterior, consequentemente é mais seguro. Ele ainda tem uma desvantagem específica da centralização, mas pode ser minimizado usando protocolos de comunicação seguros e criptografados. A Arquitetura (c) é ideal porque os dados coletados são enviados diretamente para a rede IOTA, favorecem a descentralização da rede e têm menos pontos de falha. O desafio da arquitetura c) é ter um sistema embarcado capaz de executar um cliente IOTA (ou cliente MAM) e criar e enviar objetos mínimos necessários para uma transação IOTA, de cada grupo de sensores. No entanto, esse tipo de dispositivo costuma ter baixo poder computacional e baixa largura de banda disponível (SILVANO, W. F.; MARCELINO, 2020).

3 REDE LPWAN SIGFOX

A Sigfox é uma operadora de rede que construiu uma solução de conectividade baseada em LPWAN, assim como LoraWan e *Narrow Band Internet of Things (NB-IoT)*. As ideias centrais por trás das redes LPWAN incluem: diminuir a quantidade e taxa de transferência de dados que podem ser enviados para rede, em prol de maior área de cobertura por antena, menor consumo de energia por dispositivo e menores custos quando comparado com tecnologias de rede celular como 2G, 3G, 4G e LTE (GADDAM; RAI, 2018) (GOMEZ *et al.*, 2020). Para conseguir isso, as tecnologias LPWAN utilizam uma pequena faixa do espectro eletromagnético das ondas de rádio, essa tecnologia é conhecida como UNB (do inglês, *Ultra Narrowband — UNB*).

As ondas de rádio do espectro eletromagnético, de forma geral, são leiloadas. Para que uma empresa tenha o direito de utilizar determinada faixa do espectro eletromagnético ela deve pagar uma quantia em dinheiro, que é diferente em cada país que opera. Os leilões ocorrem para dar segurança jurídica e tecnológica para as empresas, evitando, por exemplo, possíveis interferências por outros sistemas.

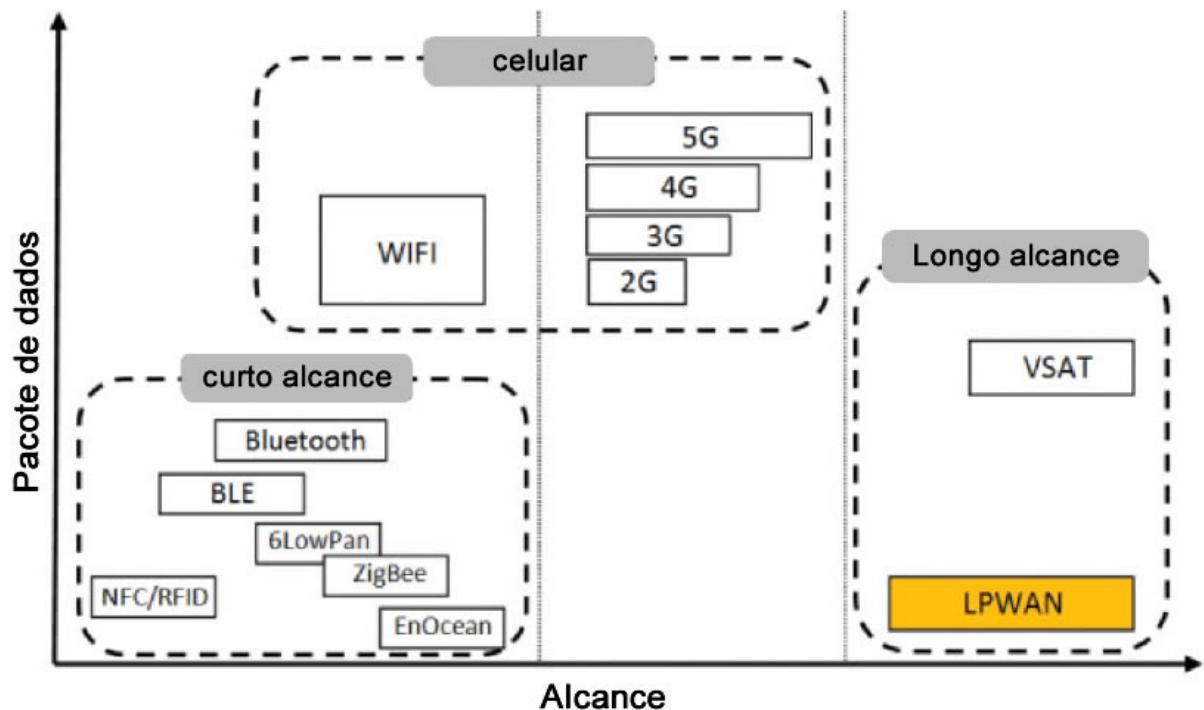
Para compreender as consequências das diferentes escolhas das distintas redes LPWAN, na seção a seguir são apresentadas as características gerais das redes Sigfox, NB-IoT e LoraWan, nas subseções seguintes, cada uma dessas tecnologias são apresentadas. O ecossistema por trás da tecnologia Sigfox é abordado na Seção 3.2.

3.1 CONTEXTUALIZAÇÃO: TECNOLOGIAS LPWAN

As aplicações das redes LPWAN estão principalmente relacionadas a sistemas IoT, como medição de dados de sensores. As implicações práticas dos sistemas LPWAN incluem dispositivos conectados em rede, alta vida útil de bateria, alta cobertura de conectividade e custo de hardware e rede baixos quando comparado com redes celulares (GADDAM; RAI, 2018) (MACIEL, 2020). As redes LPWAN também são robustas, a interferência de sinal e os dados podem ser enviados a longas distâncias de sua antena mais próxima (MEKKI *et al.*, 2018). Um dispositivo capaz de enviar dados para uma rede LPWAN pode custar menos que 2 Euros e uma conexão de um ano custa menos de 1 Euro por dispositivo por ano. As características mencionadas fazem desta tecnologia ser a melhor escolha para um projeto IoT que precise transmitir poucos dados (MEKKI *et al.*, 2018). A Figura 7 apresenta os diferentes tipos de conectividade de acordo com o tamanho do pacote de dados e seu alcance, observa-se que as tecnologias LPWAN estão no quadrante inferior direito do gráfico, inferindo assim o baixo pacote de dados e alta área de cobertura, como já mencionado.

Apesar das similaridades, as redes NB-IOT, LoraWan e Sigfox possuem algumas características diferentes, como podem ser observadas na Figura 8; por exemplo, a Sigfox possui maior cobertura e alcance e está praticamente empatada em termos de

Figura 7 – Taxa de dados vs alcance

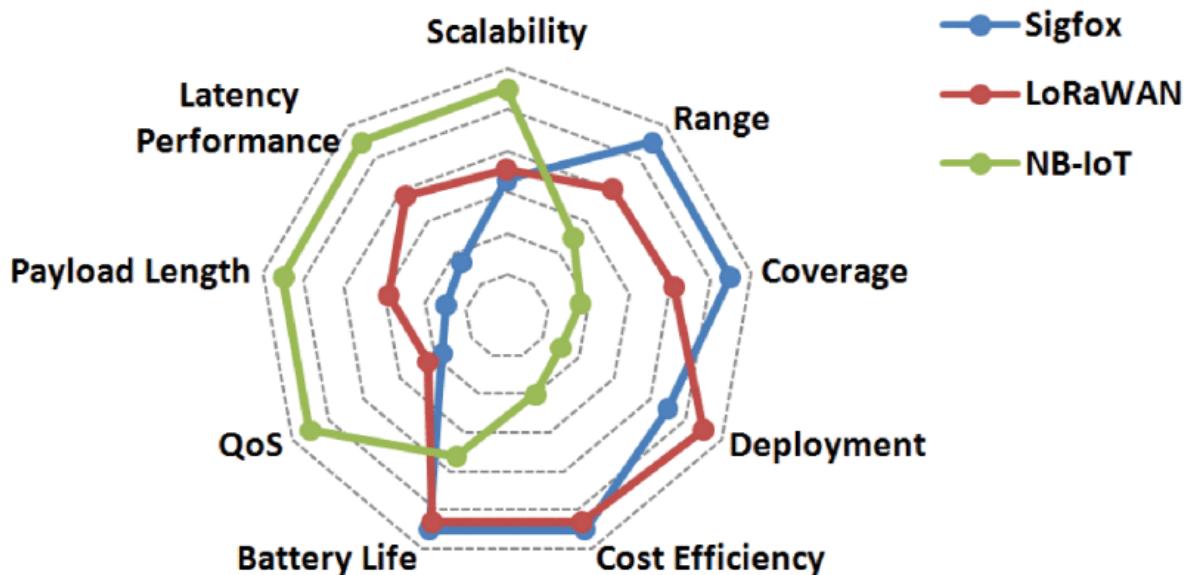


Fonte – (MEKKI *et al.*, 2018). Tradução do autor

baixo custo e alta vida útil da bateria. Já a NB-IoT permite maior pacote de dados, maior taxa de transmissão e latência menor. Portanto a escolha da tecnologia LPWAN adequada para cada projeto pode variar de acordo com o caso de uso. A necessidade de decisões rápidas e precisas, como é o caso do mercado de medição elétrica, exige baixa latência e alta qualidade de serviço (do inglês, *Quality of Service - QoS*). A rastreabilidade de produtos em grandes regiões exige a necessidade de conectar vários dispositivos, com alta eficiência energética, em uma grande área de cobertura, a custos baixos (MEKKI *et al.*, 2018).

Em virtude dos dispositivos da LPWAN terem baixa capacidade de processamento e pouca taxa para envio de bits, essa tecnologia ainda não suporta o IPv6, como por exemplo, a LoRaWAN que possui um pacote de dados máximo de aproximadamente 256 bytes, e o IPv6 que precisaria de 1600 bytes para funcionar corretamente (AL-KASHOASH; KEMP, 2016). As LPWANs rapidamente atraíram o interesse da indústria, academia e das organizações de desenvolvimento de padrões, já são previstos 4 bilhões de dispositivos conectados a redes LPWAN até 2025 (GOMEZ *et al.*, 2020)

Figura 8 – Comparação das características: Sigfox, LoRaWAN e NB-IoT



Fonte – (MEKKI *et al.*, 2018)

3.1.1 NB-IoT

A NB-IoT é uma tecnologia de banda estreita UNB, para comunicar dispositivos IoT. A tecnologia foi criada para co-existir com a GSM (*Global System for Mobile Communication*) e com LTE (*Long Term Evolution*, também chamada de 4G), em 2016. A NB-IoT é baseada na LTE, no entanto, existem algumas diferenças. A NB-IoT possui menos funcionalidades, mas melhora nos requisitos da IoT, por exemplo, no LTE é comum que as antenas enviem mensagens de *broadcast*, uma espécie de método de transferência de mensagem para todos os receptores simultaneamente, e isso consome energia, tanto da antena como de todos os receptores. Na NB-IoT, é raro ser enviada esse tipo de mensagem e quando é enviada, é muito menor, reduzindo o custo energético (MEKKI *et al.*, 2018).

A taxa máxima de *uplink* da NB-IoT é de 200 kbps e de *downlink* 20 kbps, as mensagens possuem tamanho máximo de 1600 bytes. Estima-se que a NB-IoT consiga conectar mais de 50 mil dispositivos em um canal, com uma latência de 10 segundos no pior dos casos. Uma bateria pode durar até 10 anos enviando 200 bytes por dia. (MEKKI *et al.*, 2018)

A tecnologia tem como uma de suas principais vantagens a similaridade com a LTE; os mesmos dispositivos que conseguem se comunicar com LTE podem usar a rede NB-IOT, o que facilita muito sua adoção (SINHA *et al.*, 2017).

A NB-IoT opera nas faixas de frequência licenciadas (700 MHz, 800 MHz e 900 MHz) com uma largura de banda de 200.000 Hz (MEKKI *et al.*, 2018). Ao utilizar

uma faixa licenciada, a NB-IoT possui diversos diferenciais, como altos índices de QoS quando comparado com LoraWan e Sigfox, no entanto, os leilões de faixas de frequência normalmente saem por mais de 500 milhões de dólares por MHz, tornando a tecnologia mais cara que as outras duas citadas (SINHA *et al.*, 2017).

3.1.2 LoRaWAN

A camada física da LoRaWAN se chama LoRa (do inglês, *Long Range*), que é uma técnica de modulação de banda proprietária (AL-KASHOASH; KEMP; 2017). A LoRa utiliza as bandas ISM que são frequências reservadas para indústria, ciência e medicina, não licenciadas. Na Europa a LoraWan opera em 868.000 Hz, nas Américas 915.000 Hz e na Ásia 433.000 Hz, que são as distintas faixas não licenciadas por região(MEKKI *et al.*, 2018).

A comunicação bidirecional é feita através de uma modulação que envia um sinal de banda estreita (UNB) por uma largura de banda de canal mais ampla, resultando em um canal com menos ruídos, menos interferências e com menos chance de estar congestionado (MEKKI *et al.*, 2018). A modulação utilizada também faz com que o sinal seja resistente ao efeito Doppler, fazendo com que dispositivos tenham uma alta performance ao se comunicar com objetos em movimento (MIKHAYLOV *et al.*, 2016).

Outra vantagem da LoRa é que a modulação tem seis fatores de dispersão ortogonais, que resulta em diferentes taxas de dados, isso possibilita que vários sinais possam ser enviados ao mesmo tempo, no mesmo canal, sem perder qualidade da comunicação (MIKHAYLOV *et al.*, 2016).

A taxa de dados da LoRa está entre 300 bps e 50 kbps dependendo do canal que for utilizado (MEKKI *et al.*, 2018). Cada mensagem pode ter até 243 bytes de tamanho útil, uma mensagem enviada por um dispositivo é recebida por todas as estações base que estão em seu alcance, isso cria uma redundância que acaba melhorando a porcentagem de mensagens recebidas com sucesso ao custo do preço de desenvolvimento, pois seria necessária a instalação de várias antenas em regiões próximas. Essa redundância possibilita também a localização dos dispositivos com a técnica de localização baseada na diferença de hora de chegada das mensagens(MEKKI *et al.*, 2018).

As redes LoRaWAN podem ser públicas ou privadas, as redes privadas são proprietárias, ou seja, apenas indivíduos escolhidos podem utilizá-las. Já as redes públicas podem ser vistas como serviços que uma empresa de telefonia móvel pode prestar aos seus clientes (MEKKI *et al.*, 2018).

A segurança nas redes LoRaWAN são protegidas por duas chaves, onde cada uma tem o tamanho de 128 bits. A primeira é uma chave de sessão que prova a integridade entre o usuário e a rede, como por exemplo, verificar a integridade da mensagem. A segunda chave entrega confiabilidade entre os dispositivos e a rede, ela

é utilizada para criptografar e descriptografar as mensagens com o algoritmo AES-128 (AL-KASHOASH; KEMP, 2016).

A rede LoRaWAN é dividida em três classes, classe A, B e C que são apresentadas a seguir:

- Classe A: dispositivos tem comunicação bidirecional com as estações base, eles enviam suas mensagens quando necessário e podem receber mensagens da estação base em no máximo duas janelas. Por causa dessa comunicação especial, essa classe consome menos energia;

- Classe B: dispositivos podem abrir mais do que duas janelas de recebimento, para abrir mais janelas, é necessário um sinal da estação base, isso faz com que a estação base saiba quando o dispositivo estará disponível para recebimento;

- Classe C: dispositivos estão quase sempre com suas janelas de recebimento abertas, e só fecham a janela de recebimento para envio de mensagens, entre as três classes esta é a que consome mais energia e possui menor latência (MEKKI *et al.*, 2018).

3.2 ECOSSISTEMA SIGFOX

Sigfox é uma tecnologia de rede LPWAN, criada pela empresa de mesmo nome, fundada em 2009 (GOMEZ *et al.*, 2020). Não é apenas uma tecnologia IoT, mas também um operador de rede que fornece uma solução completa, que abrange desde a coleta de dados de dispositivos sob cobertura até a transferência desses dados para o sistema de informação do cliente (SIGFOX, S., 2020). O modelo de negócios é baseado no faturamento da conectividade fornecida aos dispositivos. Desde 2009, Sigfox teve um crescimento rápido e, em julho de 2020, está disponível em 70 países, com uma área de cobertura estimada em 5 milhões de quilômetros quadrados (GOMEZ *et al.*, 2020) (**sigfoxm2miot2018**). Atualmente, cada estação base atinge uma área de 3 a 10 km em ambientes urbanos e de 30 a 50 km em áreas rurais, oferecendo serviços diferentes para até 1 milhão de dispositivos (CENTENARO *et al.*, 2016).

A tecnologia foi desenvolvida em prol de uma solução barata, confiável e de baixa potência para conectar sensores e dispositivos. Parte importante de sua solução está diretamente relacionado a faixa do espectro de rádio que opera (SIGFOX, 2020b). Assim como a LoRaWAN, a Sigfox utiliza as bandas ISM não licenciadas para operar, 868 MHz na Europa, 915 MHz nas Américas, e 433 MHz na Ásia (MEKKI *et al.*, 2018).

3.2.1 Número de mensagens por dia

Por utilizar a banda ISM pública a Sigfox, cumpre as regras de compartilhamento ("ciclo de serviço") dos países no qual opera. Esses regulamentos existem para manter essas bandas disponíveis para todos. Por exemplo, na Europa, o regulamento permite

que dispositivos nessas frequências enviem mensagens 1% do tempo por hora (o que significa 36 segundos). Para estar em conformidade com os regulamentos em vigor, os dispositivos Sigfox podem enviar apenas um número definido de mensagens por dia (SIGFOX, 2020b). O número de mensagens por dia permitido na rede Sigfox é uma aplicação direta do regulamento ETSI europeu:

- Existem 3.600 segundos em uma hora.
- 1% de 3.600 é de 36 segundos, portanto, um dispositivo pode emitir por 36 segundos por hora.
- Uma mensagem Sigfox leva 6 segundos para enviar para dispositivos RC1.

Portanto, um dispositivo pode enviar no máximo 6 mensagens por hora ($36/6$), o que significa um total de 144 mensagens por dia ($24*6$). A Sigfox mantém 4 mensagens para uso do protocolo, o que permite 140 mensagens por dia para o seu dispositivo.

3.2.2 Dispositivos Sigfox

Antes de um dispositivo Sigfox ser registrado na rede, ele deve passar por um processo de certificação definido pelas especificações oficiais da Sigfox. Esse processo serve para garantir a compatibilidade e a qualidade do serviço. Nestes testes de certificação, o protocolo da camada de enlace e o desempenho da radiação de Rádio Frequência são avaliados, dando origem a uma classificação baseada na potência da transmissão (SIGFOX, 2020b). Quando o processo de certificação é aprovado, é fornecido um certificado oficial, que posteriormente será necessário para o registro de qualquer outro dispositivo do mesmo modelo. Além disso, todo dispositivo que consegue se comunicar com a rede SigFox tem uma chave salva dentro do dispositivo pelo fabricante, essa chave não pode ser trocada (AL-KASHOASH; KEMP, 2016). O 'Device-ID' é um identificador de 32 bits globalmente exclusivo que é gravado na memória do dispositivo e não muda durante a vida útil do dispositivo. O PAC (do inglês, *Porting Authorization Code*) prova a propriedade do dispositivo e muda sempre que o dispositivo é registrado ou transferido (RUBIO-APARICIO *et al.*, 2019).

Todos os dispositivos têm um modem da SigFox para fazer comunicação unidirecional e bidirecional. Na primeira, o dispositivo envia a mensagem e não tem nenhum retorno, sendo assim, uma mensagem não verificada. Já na mensagem bidirecional, logo após o envio da mensagem o dispositivo abre uma janela de recebimento de uma mensagem *downlink*, que pode conter dados úteis ou não. Na SigFox, essa é a única forma de confirmar uma mensagem enviada, não existe retorno para mensagens perdidas durante a transmissão (GOMEZ *et al.*, 2020).

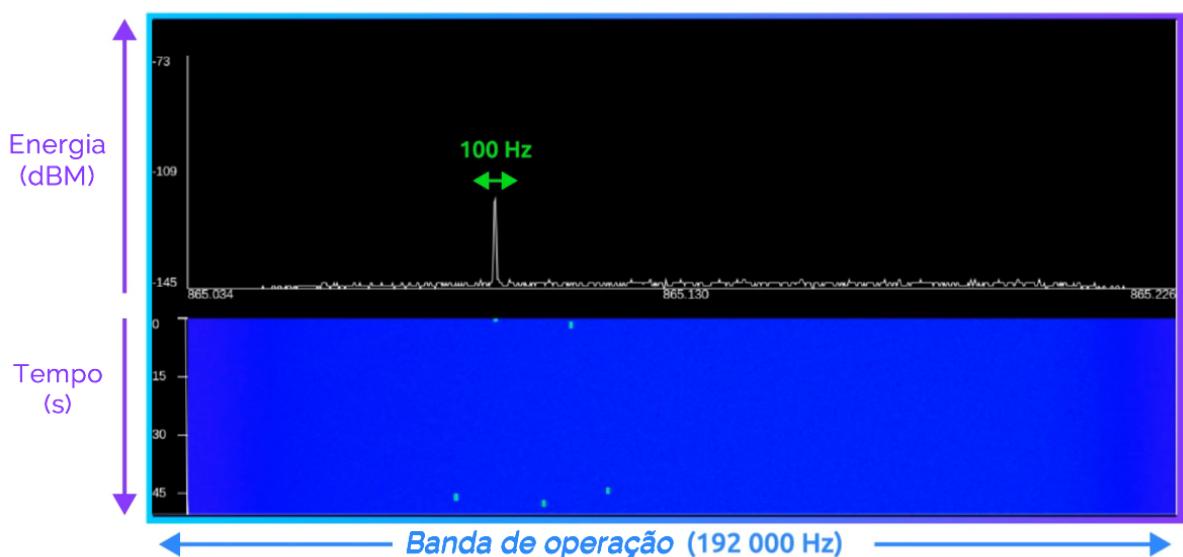
3.2.3 Protocolo de transmissão das informações

Para transmissão de informações, na camada física do protocolo é utilizada uma tecnologia de rádio frequência conhecida por *UNB - Ultra Narrow Band* (larga

de banda muito estreita), com uma largura de canal de 100 Hz, modulação DBPSK - Differential Binary Phase Shift Keying (Chaveamento Diferencial de Fase Binária) e taxa de bits de 100 bps (DO *et al.*, 2014).. A modulação utilizada pela Sigfox é do tipo de mudança de fase, oferecendo a maior imunidade ao ruído, com diferença de fase máxima de 180° (LAURIDSEN *et al.*, 2017).

A modulação DBPSK para *uplink* de mensagens dos dispositivos, permite um hertz de banda de operação para transmitir um bit por segundo. Se considerarmos que a transmissão DBPSK emite 100 Hz, isso significa que um único sinal ocupa uma parte fina do espectro da banda de operação (Figura 9). A modulação DBPSK é chave para a alta sensibilidade das estações base, pois existe uma diferença muito grande entre o que é ruído e o que não é. (SIGFOX, S., 2020)

Figura 9 – Modulação de sinal de rádio frequência - Sigfox

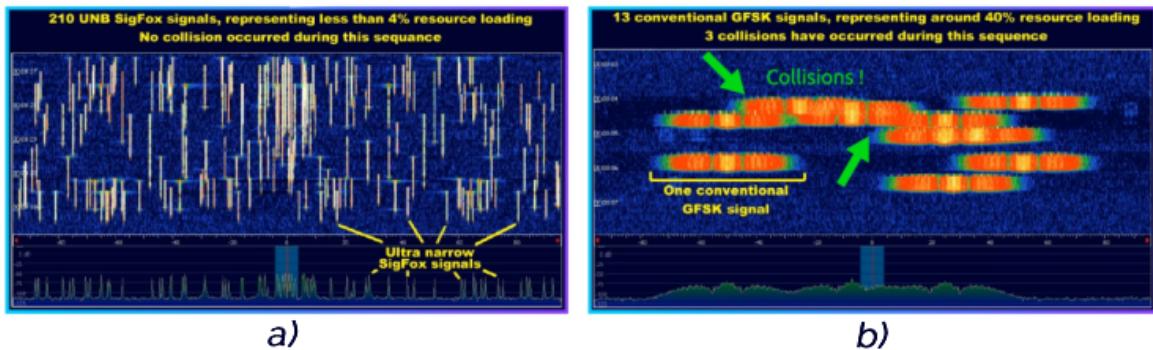


Fonte – (SIGFOX, S., 2020)

O sistema Sigfox foi desenvolvido para fornecer a máxima simplicidade de projeto dos dispositivos transceptores, com base nas condições de ruído e interferência em uma largura de canal UNB que garante um nível relativamente alto da densidade espectral do sinal e ruído reduzido (STANIEC, s.d.). Uma análise espectral de sinais de UNB emitida por dispositivos Sigfox (Figura 9a) e emitida por uma rede 3G (Figura 9b) ajuda a entender a grande diferença entre as tecnologias. Na Figura 9a) observa-se 210 mensagens Sigfox cobrindo 4% da banda de operação, na Figura 9b) 13 sinais de Wi-fi típicos, cobrem 40% da banda de 200 000 Hz. As frequências utilizadas pela Sigfox são selecionadas a partir de uma faixa contínua (largura total de 192 kHz), em vez de um conjunto discreto predefinido de canais. Esse recurso permite o uso de

transmissores de qualidade mais fraca nos terminais. O recurso implica em redução de custos dos dispositivos de transmissão e recepção (STANIEC, s.d.).

Figura 10 – Comparação de sinais Sigfox x 3G

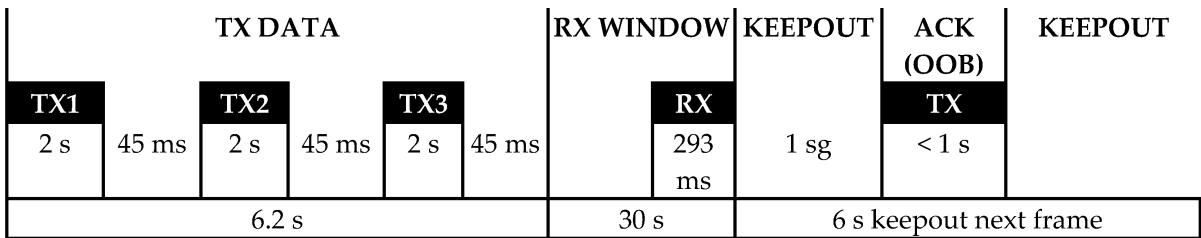


Fonte – (SIGFOX, S., 2020)

É possível obter conexões sem fio de longo alcance de até 163,3dB de perda total, com 14 dBm de potência de transmissão, usando uma antena com ganho de 2,15 dBm, um receptor de estação base com sensibilidade de -142 dBm e uma antena de recepção de 5,15 dBm (SIGFOX, 2020a). Na Figura 11, pode-se observar que cada período de transmissão de um dispositivo dura cerca de 2s é repetido 3 vezes em diferentes frequências, a fim de aumentar as possibilidades de recepção pela rede. As estações base mantêm a recepção em um segmento de 192 kHz em torno da frequência central e os dispositivos podem transmitir em qualquer frequência dentro desse segmento (SIGFOX, 2020a). Se uma resposta for solicitada, uma janela de recepção de 25 s é aberta e uma confirmação de recepção é gerada posteriormente para a transmissão da rede até o dispositivo. A modulação *GFSK (Gaussian Frequency Shift)* é usada a uma velocidade de 600 bps e um canal é escolhido de acordo com o canal usado para upload no segmento de *downlink* de 200 kHz e na frequência central (LAURIDSEN *et al.*, 2017). Portanto, é uma comunicação bidirecional, mas assimétrica, que é sempre iniciada pelo dispositivo e só é produzida uma comunicação de download se solicitada por esse dispositivo. O número de mensagens de upload por dispositivo na rede é limitado a 140 por dia (como já mencionado) e o número de mensagens de download é limitado a 4.

Até 12 bytes (96 bits) de dados podem ser de carga útil, ou seja, uma mensagem definida pelo usuário. A sobrecarga de dados no protocolo não inclui nenhuma sinalização com a rede e as mensagens também não são confirmadas. O usuário é livre para distribuir as informações desejadas dentro dos 12 bytes de carga útil, uma vez que estes serão armazenados e chegarão aos servidores do cliente como estão (LAURIDSEN *et al.*, 2017).

Figura 11 – Cronologia de uma comunicação Sigfox

Fonte – (MEKKI *et al.*, 2018)

3.2.4 Segurança

Em relação à segurança, o emissor é autenticado por meio do identificador do dispositivo e a autenticação da mensagem é realizada por meio do seu número de sequência. Como uma negociação com a rede. No momento do envio de mensagens, não é necessário que o dispositivo transmita a mensagem sem aguardar uma resposta, portanto, tentar interferir com o receptor do dispositivo não evita a comunicação. Na conexão de rádio frequência não há criptografia das mensagens, se necessário, esta tarefa é atribuída à camada de aplicativo *OSI (Open System Interconnection)*. Neste caso, um 'túnel VPN' é estabelecido entre as estações base e os servidores Sigfox e o protocolo HTTPS seguro pode ser usado para se comunicar com a infraestrutura do usuário (LAURIDSEN *et al.*, 2017).

3.2.5 Arquitetura de rede

A topologia da rede Sigfox é do tipo estrela, conectando vários objetos à mesma estação base e todas as estações base aos servidores Sigfox. A estação base funciona como um coletor de dados recebidos em relação a determinado endereço IP. A detecção de elementos duplicados e a autenticação são gerenciadas pelo servidor de rede, não pelas estações base. Cada zona é geralmente coberta por 3 estações base no que é chamado de 'diversidade espacial'. Essa diversidade espacial aumenta a confiabilidade da recepção de mensagens, por meio de 3 estações base em 3 locais diferentes, cobrindo cada objeto(LAURIDSEN *et al.*, 2017).

As estações base são antenas Sigfox locais, que recebem mensagens de dispositivos emissores e as encaminham para a nuvem Sigfox. Eles são implantados em campo pelos Operadores Sigfox locais. São compostos de três elementos principais: Uma antena, para receber mensagens pelo ar, geralmente implantada em pontos altos ou torres; um amplificador de baixo ruído, para amplificar o sinal e filtrar o ruído; e um ponto de acesso, que interpreta as mensagens Sigfox e as envia para a 'Sigfox Cloud'. Uma vez conectados, eles se tornam parte da rede pública e passam a ouvir todas as

mensagens Sigfox enviadas por dispositivos nas proximidades (SIGFOX, 2020b).

Como pode ser observado na Figura 11, a arquitetura Sigfox conta com vários dispositivos transmitindo mensagens para a rede, a partir do envio de sinais de rádio frequência dentro da área de cobertura das estações base. Cada estação base é conectada a 'Sigfox Cloud'. As estações bases detectam as mensagens, modulam e reportam as mensagens para a 'Sigfox Cloud'. A partir da 'Sigfox Cloud' as mensagens podem ser enviadas para uma plataforma do cliente (SIGFOX, S., 2020).

Figura 12 – Arquitetura de rede Sigfox



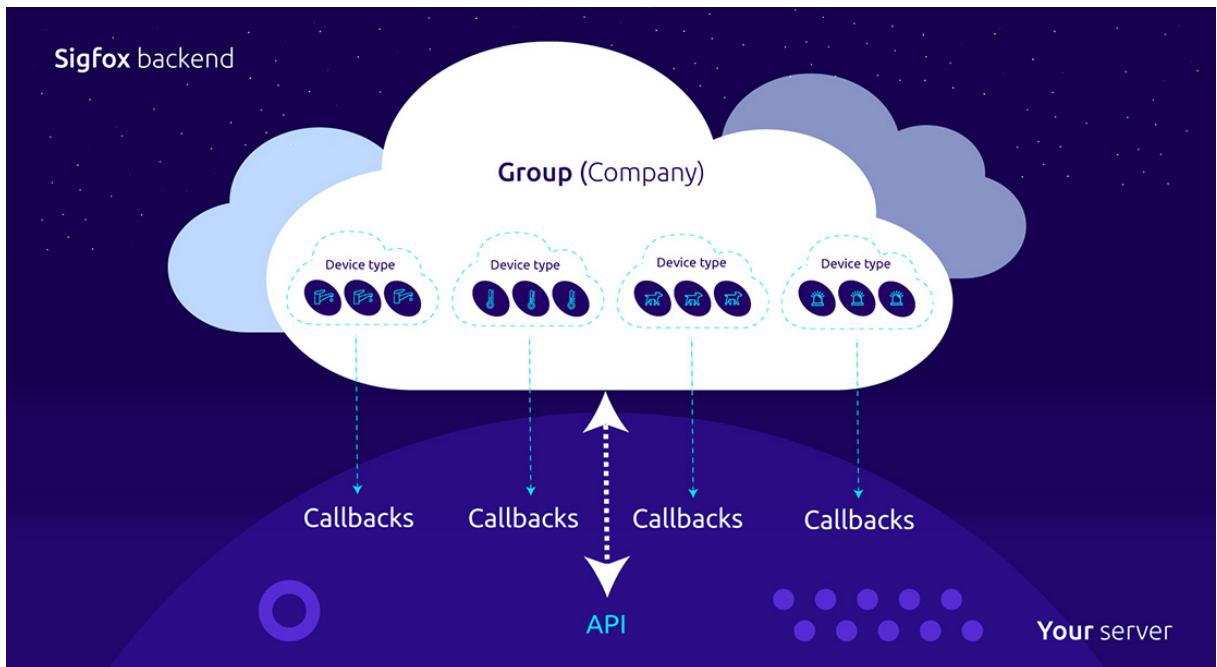
Fonte – (SIGFOX, S., 2020)

3.2.6 Backend Sigfox

O 'Sigfox Cloud' é o *hub* central onde as mensagens e informações dos dispositivos são armazenadas. É necessário integrar 'Sigfox Cloud' para recuperar, usar os dados e administrar os dispositivos (SIGFOX, 2020b). Integrar significa criar um link entre o 'Sigfox Cloud' e a plataforma cliente. Para isso, dois métodos estão disponíveis: A API de *callback* e a API *REST*. Cada um deles serve a um propósito de comunicação entre o Sigfox Cloud e um servidor. Em resumo, os callbacks de chamada são usados para recuperar as mensagens dos dispositivos, e a API *REST* é usada para administrar os dispositivos e criar serviços relacionados, como uma plataforma do cliente.

Todas as mensagens do 'Sigfox cloud' são centralizadas no *back-end* da SigFox, onde o desenvolvedor já tem uma interface para trabalhar. O *back-end* também é responsável por filtrar as mensagens replicadas dos dispositivos. Todas as mensagens centralizadas na *Cloud* são salvadas em dois banco de dados, como backup (SIGFOX, S., 2020).

Figura 13 – Tipos de chamadas - Sigfox



Fonte – (SIGFOX, 2020b)

3.2.6.1 Callbacks

As consultas de *callback* de chamada são solicitações HTTP, que são mensagens de notificação (somente de mão única) e estão vinculadas a um tipo de dispositivo. Um servidor só pode obter dados através de retornos *callback*, não pode gerenciar dispositivos. Quando o 'Sigfox Cloud' recebe uma mensagem de um dispositivo emissor, ele gera instantaneamente uma mensagem de retorno de chamada e a envia para os servidores da plataforma. Dessa forma, não é necessário verificar regularmente a existência de novos dados, o sistema envia qualquer novo conteúdo automaticamente (SIGFOX, 2020b).

3.2.6.2 API Rest

As consultas da API REST são solicitações HTTP bidirecionais e funcionam no nível do grupo, um servidor pode solicitar e receber dados do 'Sigfox Cloud' por meio da API. A API REST Sigfox segue uma política de "uso justo", "você pode fazer solicitações desde que siga os limites de taxa da API e concorde em nunca usar mais recursos do que o exigido nominalmente pelo seu aplicativo". A API REST permite o registro e gerenciamento dos dispositivos na 'Sigfox Cloud', incluindo seus ciclos de vida de assinatura feita. Dessa forma, não é necessário se conectar ao site da Sigfox *Back-end* para executar operações recorrentes, como declaração de retorno

de chamada, gerenciamento de dispositivos, etc. A API REST permite manipular os dispositivos registrados diretamente de um servidor cliente (SIGFOX, 2020b).

4 ESTADO DA ARTE

Este capítulo é dedicado a explorar as produções científicas relacionadas a este trabalho, a utilização do *ledger* distribuído da IOTA e rede LPWAN Sigfox no monitoramento e rastreamento na cadeia de suprimentos. Isso é realizado por meio de uma revisão sistemática de literatura, a fim de compreender qual o atual estado da arte, buscando com isso, identificar as lacunas de pesquisa e enfatizar as contribuições científicas deste trabalho.

A Revisão sistemáticas da literatura é definida como uma técnica de investigação científica, essa investigação é realizada sobre um tema central, no qual utiliza de procedimentos e critérios bem definidos para buscar resultados de produções científicas (COOK *et al.*, 1997). A revisão sistemática de literatura também permite ao pesquisador, reunir, avaliar criticamente e conduzir uma síntese dos resultados de múltiplos estudos primários (CORDEIRO *et al.*, 2007).

Na Seção 4.1, é apresentada a metodologia para realização dessa pesquisa. Na Seção 4.2 são apresentados os resultados da pesquisa. A Seção 4.3 consiste na análise descritiva dos trabalhos selecionados.

4.1 METODOLOGIA DA PESQUISA BIBLIOGRÁFICA

Essa sessão descreve a metodologia de pesquisa, incluindo descrição das bases de dados, palavras-chave e como foram filtrados os resultados da busca.

4.1.1 Bases de dados

Foram exploradas três bases de dados acadêmicas: IEEE Xplore, Web of Science e Scopus. O acesso a estas bases foi realizado diretamente por meio das plataformas citadas.

A biblioteca digital IEEE Xplore é um recurso poderoso para a descoberta e acesso a conteúdo científico e técnico publicado pelo IEEE (Instituto de Engenheiros Elétricos e Eletrônicos) e seus parceiros de publicação. Nela pode-se encontrar mais de 195 periódicos, 1.400 processos de conferências, 5.100 padrões técnicos e aproximadamente 2.000 livros (XPLORE, 2018).

A Web of Science é uma base de dados para pesquisa, na qual permite ao usuário acessar uma variedade de trabalhos de pesquisa de classe mundial vinculada a um núcleo de periódicos rigorosamente selecionado e descobrir novas informações com exclusividade por meio de conexões de metadados e citações meticulosamente capturadas (SCIENCE, 2018).

A Scopus é base de dados de resumos e citações, ela abrange cerca de 36.377 títulos de 11.678 editores, dos quais 34.346 são revisados por pares periódicos de

nível superior. Nesta base, pode-se encontrar trabalhos das áreas de ciências da vida, ciências sociais, ciências físicas e ciências da saúde (SCOPUS, 2018).

4.1.2 Palavras-chave

Em consulta prévia, identificou-se que não existem trabalhos que relacionem “IOTA”, “Sigfox” e “cadeia de suprimentos (*supply chain*)”, tendo isso em vista, optou-se por realizar o processo sistemático da pesquisa, realizando buscas a partir da concatenação de pares e trios de palavras, que são definidas nessa sessão. Contou-se também com a utilização do caractere curinga (*) buscando incluir sinônimos da palavra, e como consequência a inclusão de falsos negativos.

Em uma análise exploratória inicial, identificou-se que os termos em inglês *track* e *monitor* relacionam-se com o sentido de acompanhamento, tratado nesse trabalho. Já a tradução literal do termo Cadeia de suprimentos, “*supply chain*”, é padronizado e facilmente identificado nos trabalhos. O termo mais utilizado para referir-se a *Ledger* distribuídos, não é DLT, e sim Blockchain, inclusive o Tangle da IOTA é frequentemente considerado um tipo de Blockchain. Por considerar que as tecnologias utilizadas neste trabalho são muito novas, IOTA (2015) e Sigfox (2009), buscamos todos os resultados relacionados a essas tecnologias. IOTA é um termo utilizado em muitos contextos científicos, e deve ser combinado com “Tangle”, para que os resultados sejam condizentes com o *ledger* distribuído.

A sequência de buscas com seus descritores é apresentadas a seguir:

- Etapa 1: (supply chain AND monitor*) OR (supply chain AND track*);
- Etapa 2: (supply chain AND monitor* AND blockchain) AND (supply chain AND track* AND blockchain);
- Etapa 3: IOTA AND Tangle;
- Etapa 4: Sigfox;

4.1.3 Filtro de qualidade

Visando identificar trabalhos de qualidade, porém não filtrar demasiadamente, optou-se por selecionar resultados baseado no indicador “H index” de cada periódico. O H5-index refere-se ao maior número h, de modo que h artigos publicados possuam pelo menos h citações cada, nos últimos cinco anos (MESTER, 2016). O índice H foi estudado pela comunidade científica e considerado relevante porque é simples de medir e considera a quantidade e o impacto das publicações. Um periódico não pode ter um alto índice h sem publicar um número considerável de artigos. Os periódicos que possuem fluxo contínuo de artigos com muitas citações são beneficiados por essa métrica (MESTER, 2016).

No contexto desse trabalho são identificados artigos publicados em periódicos com H5-index maior que 20, de acordo com métricas do Google Scholar, ou seja, o número de artigos publicados na revista, nos últimos cinco anos, que possuem pelo menos 20 artigos com 20 citações. Esse critério visa garantir que os artigos analisados passaram por um cuidadoso processo de seleção.

4.1.4 Análise exploratória

Apesar do cuidado com palavras chaves e critérios de seleção dos artigos, uma análise exploratória se faz necessária. A análise visa identificar possíveis documentos inconsistentes com a temática proposta e principalmente, agrupar artigos por tipo de abordagem, buscando coletar dados a respeito dos objetos e tipo de pesquisa realizados até o presente momento. Essa é uma análise manual, que ocorre em três fases: leitura dos artigos selecionados (1); identificação das principais temáticas (2); categorização dos artigos (3).

4.2 RESULTADOS DE PESQUISA

4.2.1 Etapa 1: Monitoramento na cadeia de suprimentos

Para o levantamento das produções relacionadas ao monitoramento na cadeia de suprimento, foi inserido os descritores “supply chain” AND “monitor” e “supply chain” AND “track” (Etapa 1), observando um total de 5831 resultados, sendo 955 na IEEE Xplore, 1269 no Web of Science e 3607 na Scopus. A evolução das produções pode ser observada na Figura 14, separadas por base de dados.

É possível observar na Figura 14 que o tema teve sua primeira publicação em 1988, posteriormente foi abordado apenas em 1994. O ano com maior número de produções foi 2020, com 610 trabalhos, contudo ressalta-se que a pesquisa ocorreu em 5/07/2020, portanto, existe um longo período para o surgimento de novas publicações em 2020. Nota-se uma inclinação maior nas curvas nos anos de 2016 e 2017, dando indícios de novos interesses na área.

4.2.2 Etapa 2 - Blockchain e monitoramento na cadeia de suprimentos

Ao adicionar o termo “Blockchain” aos descritores (Etapa 2), foi possível adequar melhor os resultados às temáticas deste trabalho. Encontrou-se 263 resultados, sendo 56 na IEEE Xplore, 70 no Web of Science e 137 na Scopus. Os resultados podem ser observados na Figura 15.

Observa-se que o termo Blockchain, surge apenas em 2017 relacionada a monitoramento na cadeia de suprimentos, com 16 resultados. No ano de 2019 a temática já possuía 163 resultados. Podemos dizer, observando os dados da Figura 14 e Figura 15,

Figura 14 – Etapa 1: Pesquisas relacionadas a monitoramento na cadeia de suprimentos

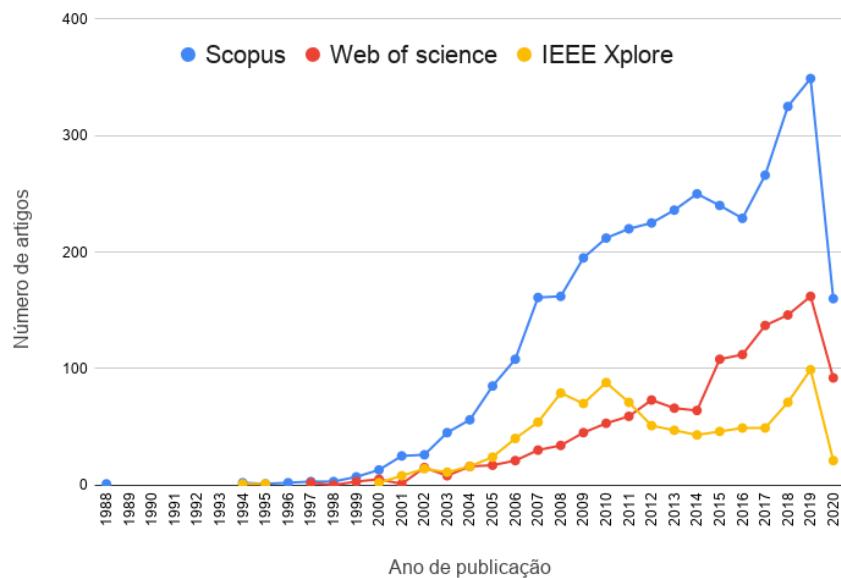
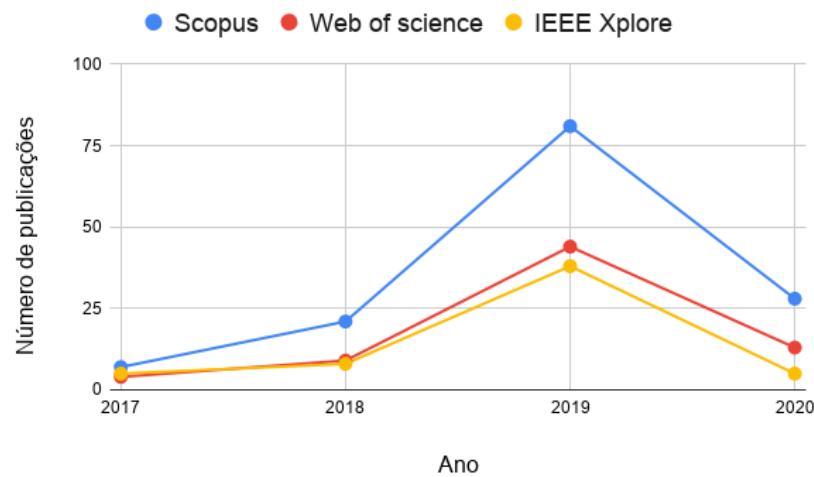


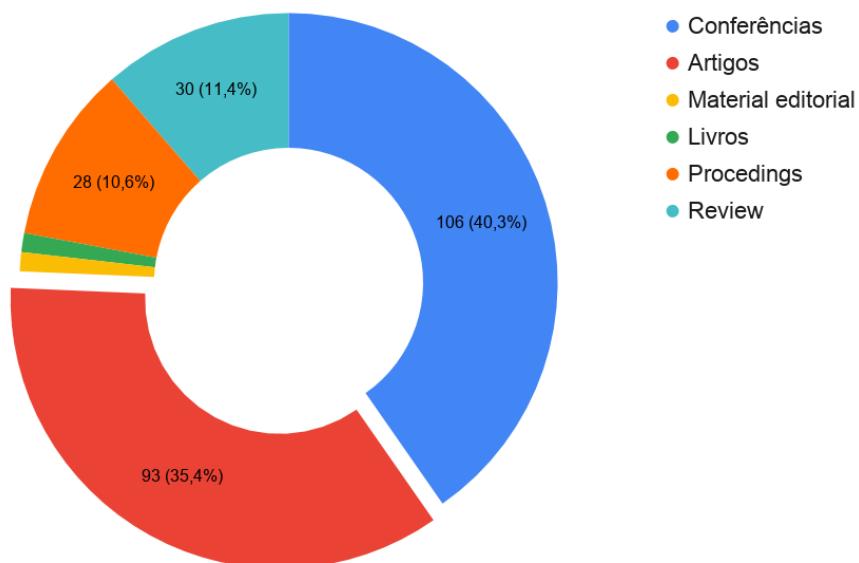
Figura 15 – Etapa 2: Pesquisas relacionadas a Blockchain no monitoramento na cadeia de suprimentos



que parte dos novos interesses pelo monitoramento na cadeia de suprimentos, surgem junto com o surgimento da Blockchain nessas pesquisas. Como exemplo, o IEEE Xplore possuía 49 resultados em 2017, e passou para 99 em 2019 (Figura 14), sendo que 38 destes resultados estão relacionados a Blockchain (Figura 15), representando 38% do total de 2019. Pode-se afirmar, portanto, que há um crescente interesse em pesquisas que relacionem o monitoramento na cadeia de suprimentos com Blockchain, e que esta temática já ocupa parte substancial da pesquisa.

Os trabalhos podem ser divididos em 6 tipos de documentos: *reviews*, *procedings*, livros, material editorial, conferências e artigos, conforme apresentado na Figura 16. Artigos e conferências são os documentos com maior quantidade de resultados, totalizando 75,7% dos resultados, 35,4% artigos e 40,3% conferências.

Figura 16 – Etapa 2: Tipos de documentos



Buscando otimizar a qualidade da análise, optou-se por selecionar apenas os 93 artigos para uma avaliação mais criteriosa. Ao utilizar o filtro de qualidade, definido na Seção 4.1.3 identificou-se 51 artigos com H5-Index > 20. Utilizando o software EndNote, foi possível identificar 17 resultados repetidos, restando 34 artigos.

Identificou-se o Qualis de cada periódico no qual o artigo foi aceito, visando validar a qualidade da seleção. Uma análise exploratória dos artigos permitiu identificar as abordagens das publicações. Identificou-se três grupos de publicações: entrevistas, revisão de literatura, propostas de solução e outros. Estes artigos são apresentados na Tabela 1 com seus respectivos títulos, periódico, H5-index, Qualis e tipo de abordagem.

Tabela 1 – Artigos

Id	Artigo	Periódico	H5-index	Qualis	Abordagem
1	Estimating Service Quality in Industrial Internet-of-Things Monitoring Applications With Blockchain	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	solução
2	A Survey on Using Blockchain in Trade Supply Chain Solutions	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	revisão
3	A Blockchain-Based Approach for the Creation of Digital Twins	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	outro
4	Blockchain-Based Solution for the Traceability of Spare Parts in Manufacturing	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	solução
5	Blockchain Applications – Usage in Different Domains	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	solução
6	Blockchain-Based Soybean Traceability in Agricultural Supply Chain	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	revisão
7	Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	outro
8	When Intrusion Detection Meets Blockchain Technology: A Review	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	revisão
9	Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism	IEEE Access	119	B3 (CC), B1(E3), A2(E4)	solução
10	Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain	IEEE Internet of Things Journal	93	B2 (CC), B2 (E4)	solução
11	Supply chain re-engineering using Blockchain technology: A case of smart contract based tracking process	Technological Forecasting and Social Change	87	A1(ADM), A1(PU), A1(E3), B2(CC)	revisão
12	A Study on the Transparent Price Tracing System in Supply Chain Management Based on Blockchain	Sustainability	78	A2(E1), A2(ARQ), A2(GEO), B1(IT)	outro
13	The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	International Journal of Production Research	77	A(ADM), A1(CC), A1(CAGR), A2(CA), B1(E2), A2(E3), B1(E4), B1(IT), B2(MT), B1 (MD)	revisão
14	A blockchain-based approach for a multi-echelon sustainable supply chain	International Journal of Production Research	77	A1 (CC), A1 (ADM), A2 (CA), B1(E2), A2 (E3), B1 (E4), B2 (MT), B1 (MED)	solução
15	Blockchain-based life cycle assessment: An implementation framework and system architecture	Resources Conservation and Recycling	76	A1 (ADM), B1(CAL), A1(CA), A1(E1), A1(E2), A2(E3), A1(IT)	revisão
16	Blockchain in Energy Efficiency: Potential Applications and Benefits	ENERGIES	69	B2(FSC), B2(BIOD), B1(BIOT), B3(CC), B1(CA), A2(CA), B1(EC), A1(E2), B1(E3), B1(E4), A2(IT), B1(ZOO)	revisão

Fonte – O autor. *3 Qualis de maior impacto.

Tabela 2 – Artigos (continuação)

Artigo	Artigo	Periódico	H5-index	Qualis	Abordagem
17	Smart contract-based approach for efficient shipment management	Computers & Industrial Engineering	64	A1 (CC); A1(ADM); A1(E2); A2(IT)	solução
18	Blockchains in operations and supply chains: A model and reference implementation	Industrial Engineering	64	A1 (ADM), A1 (CC), A2(CAGR), B1 (ECM), A2(E1), A1 (E2), A2(E3), B1(E4), A2(IT), B1 (MT)	solução
19	Building trust and equity in marine conservation and fisheries supply chain management with Blockchain	Marine Policy	55	B1(BIOD), B1(BIOT), A1(RI), A2(CA), B1(CB), B1(EC), B3(ES), A2(GEO), A1(GEO), A1(HIS), A2(IT), A2(MV), B1 (NT), A2(SCo), A2 (SOC)	revisão
20	Real-time supply chain—A Blockchain architecture for project deliveries	Robotics and Computer-Integrated Manufacturing	50	A2(CC), A2(E3), A2(GEO)	solução
21	Adaptable Blockchain-Based Systems: A Case Study for Product Traceability	IEEE Software	44	B1 (IT), A1(CC), B3 (BIOT)	revisão
22	Safe farming as a service of blockchain-based supply chain management for improved transparency	Cluster Computing	43	B1 (CC), B1 (E1)	outro
23	Exploring Research in Blockchain for Healthcare and a Roadmap for the Future	IEEE Transactions on Emerging Topics in Computing	41	B2(CC), B2 (E4)	revisão
24	Blockchain in logistics industry: in fizz customer trust or not	Journal of Enterprise Information Management	38	–	revisão
25	Blockchain's roles in strengthening cybersecurity and protecting privacy	Telecommunications Policy	37	A2(EC), B1(E3), B1(IT), B3(CC)	revisão
26	Ensuring transparency and traceability of food local products: A Blockchain application to a Smart Tourism Region	Concurrency and Computation: Practice and Experience	36	A2 (CC), B2(IT)	solução
27	Thai Agriculture Products Traceability System using Blockchain and Internet of Things	International Journal of Advanced Computer Science and Applications	35	—	outro

Fonte – O autor. *3 Qualis de maior impacto.

Tabela 3 – Artigos (continuação)

Id	Artigo	Periodico	H5-index	Qualis	Abordagem
28	Shifting trust in construction supply chains through Blockchain technology	Engineering, Construction and Architectural Management	30	B5(CC), B1 (E1)	entrevista
29	Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management	Future Internet	27	—	revisão
30	Anti-BIUFF: towards counterfeit mitigation in IC supply chains using Blockchain and PUF	International Journal of Information Security	26	B1(CC), B2(MT)	B2(E4), outro
31	Can Blockchain Strengthen the Internet of Things?	IT Professional	26	A2(E4)	revisão
32	Blockchain in Additive Manufacturing and its Impact on Supply Chains	Journal of Business Logistics	26	—	entrevista
33	The Struggle is Real: Insights from a Supply Chain Blockchain Case	Journal of Business Logistics	26	—	revisão
34	Distributed Ledger Technology as a Tool for Environmental Sustainability in the Shipping Industry	Journal of Marine Science and Engineering	23	—	revisão

Fonte – O autor. *3 Qualis de maior impacto.

Os artigos que possuem algum tipo de solução a respeito da Blockchain no monitoramento da cadeia de suprimentos, representam 29,4% dos tipos publicações apresentados na tabela Tabela 1, totalizando 10 artigos. Tendo em vista que objetivo desta dissertação está relacionado ao desenvolvimento e avaliação de uma solução baseada em *ledger* distribuído para cadeia de suprimentos, optou-se por aprofundar a análise desses artigos.

Uma nova análise exploratória buscou identificar o tipo de acompanhamento que cada uma das soluções propõem a área de aplicação, tipo de *ledger* distribuído e o modo de acesso da Blockchain. Essas informações são apresentadas na Tabela 4.

Tabela 4 – Soluções - Blockchain no monitoramento da cadeia de suprimentos

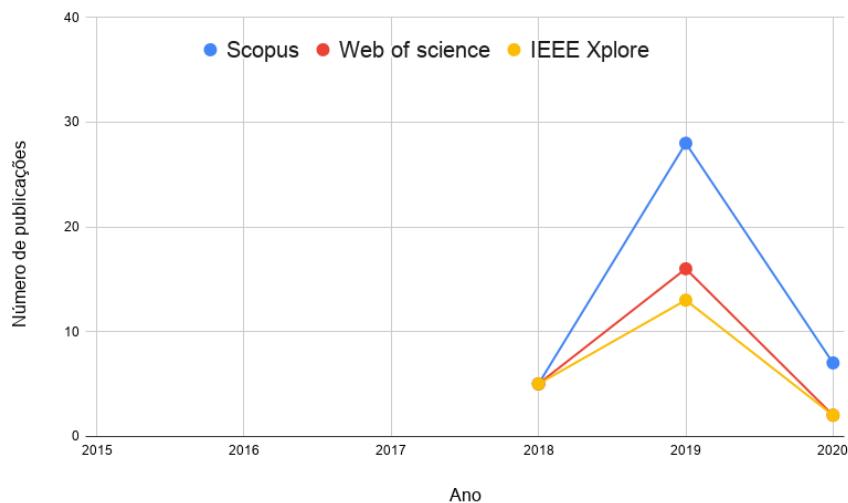
id	Artigo	Monitoramento	Aplicação	blockchain
1	Estimating Service Quality in Industrial Internet-of-Things Monitoring Applications With Blockchain (MAITI <i>et al.</i> , 2019)	contínuo	genérico	BigchainDB
4	Blockchain-Based Solution for the Traceability of Spare Parts in Manufacturing (HASAN, H. R. <i>et al.</i> , 2020)	durante a custódia	Peças de reposição	Ethereum
6	Blockchain-Based Soybean Traceability in Agricultural Supply Chain (SALAH <i>et al.</i> , 2019)	contínuo	Soja	Ethereum
9	Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism (TSANG <i>et al.</i> , 2019)	contínuo	Alimentos perecíveis	não definido
10	Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain (MONDAL <i>et al.</i> , 2019)	durante a custódia	genérico	não definido
14	A blockchain-based approach for a multi-echelon sustainable supply chain (MANUPATI <i>et al.</i> , 2020)	não específico	créditos de carbono	não definido
17	Smart contract-based approach for efficient shipment management (HASAN, H. <i>et al.</i> , 2019)	contínuo	vacinas	Ethereum
18	Blockchains in operations and supply chains: A model and reference implementation (HELO; HAO, 2019)	durante a custódia	genérico	Ethereum
20	Real-time supply chain—A Blockchain architecture for project deliveries (HELO; SHAMSUZZOHA, 2020)	contínuo	genérico	Ethereum
26	Ensuring transparency and traceability of food local products: A Blockchain application to a Smart Tourism Region (BARALLA <i>et al.</i> , 2020)	contínuo	Alimentos perecíveis	Ethereum

4.2.3 Etapa 4 - IOTA

Conforme descrito na etapa 4 da Seção 4.1, utilizou-se o descriptor “IOTA” AND “Tangle”, resultando em 83 resultados, sendo 20 na IEEE Xplore, 23 no Web of Science e 40 na Scopus. A evolução temporal das publicações pode ser observada na Figura 17. As publicações sobre IOTA nas bases de dados supracitadas aparecem apenas em

2018, o que tem sentido tendo em vista que o IOTA/Tangle foi idealizada em 2015 e lançada em 2016.

Figura 17 – Etapa 4: Pesquisas relacionadas ao ledger distribuído da IOTA/Tangle



Apenas 28 dos 83 resultados encontrados são artigos. Buscando identificar quais desses artigos foram encontrados em mais de uma base de dados, identificou-se 14 resultados repetidos, utilizando o software EndNote. Portanto, foram encontrados 15 artigos únicos. Utilizando o filtro de qualidade, definido na Seção 4.1.3, outros 2 artigos foram descartados. Uma análise exploratória dos artigos permitiu identificar as abordagens de cada publicação. Foram identificados três grupos de publicações: revisão de literatura, propostas de solução e outro. Dentre as soluções, identificou-se também o setor de aplicação. Estes artigos são apresentados na Tabela 1 com seus respectivos títulos, periódico, H5-index, Qualis, tipo de publicação e setor de aplicação.

Nenhum dos artigos possui relação com IOTA na cadeia de suprimentos, esse fato pode ser observado na Figura 18 e na Tabela 5. A ausência de resultados, indicou a necessidade de uma busca mais abrangente. Conferências, livros e material editorial também foram verificados, no entanto, também não foram encontrados resultados válidos. Sendo assim, pode-se dizer, que nenhum resultado sobre IOTA aplicada a cadeia de suprimento foi publicado e pode ser acessado na IEEE, Scopus ou Web of Science.

Figura 18 – IOTA - Abordagem e tipos de aplicação dos artigos

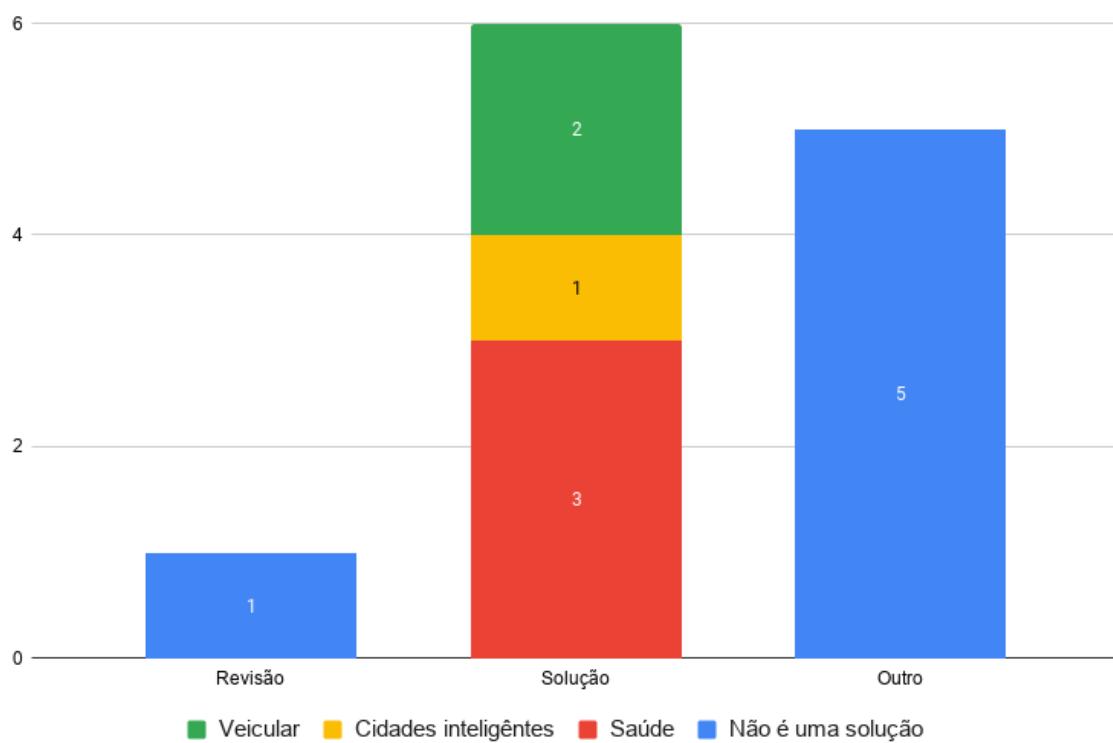


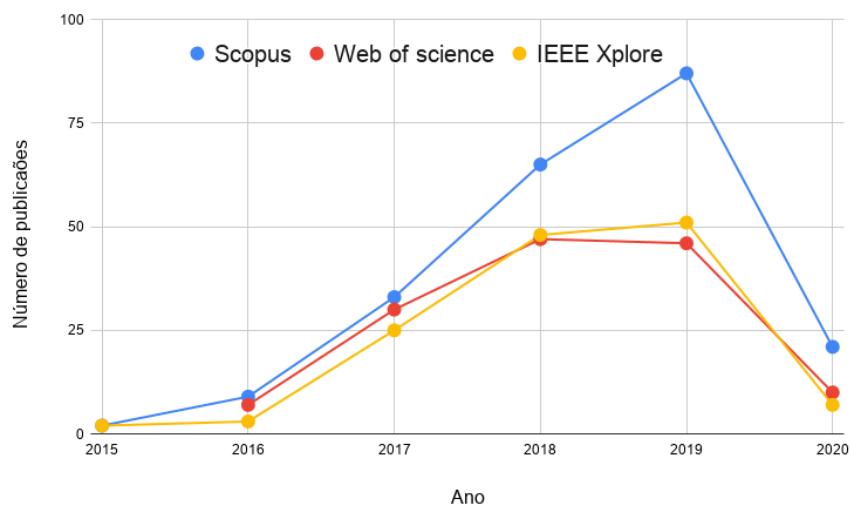
Tabela 5 – Artigos - IOTA

Artigo	Periódico	H5-index	Qualis	Abordagem	Aplicação
Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance	IEEE Access	119	A2(E4); B1(E3); B3 (CC)	solução	Cidades Inte- ligentes
A Distributed Framework for Energy Trading between UAVs and Charging Stations for Critical Applications	IEEE Transactions on Vehicular Technology	104	A1(CC); A1(E4)	solução	veicular
A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management	Sensors	104	A1(CC); A1(E4); A2(IT); A2(AU);	solucao	saúde
Indoor Air-Quality Data-Monitoring System: Long-Term Monitoring Benefits	Sensors	104	A1(CC); A1(E4); A2(IT);	solução	saúde
On the stability of unverified transactions in a DAG-based Distributed Ledger	IEEE Transactions on Automatic Control	100	A1(CC); A1(E3); A1(IT)	outro	N/A
Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies	Journal of Medical Internet Research	96	A1(CC); A1(MD1); A1(MD2);	solução	saúde
IOTA Tangle: A cryptocurrency to communicate Internet-of-Things data	Future Generation Computer Systems	86	A1(E3) A2(CC); A2(IT);	revisão	N/A
Blockchain IoT for Smart Electric Vehicles Battery Management	Sustainability	78	A2(E1); A2(AU); B1(IT)	solução	veicular
A Scalable IoT Protocol via an Efficient DAG-based Distributed Ledger Consensus	Sustainability	78	A2(E1); A2(AU); B1(IT)	outro	N/A
Equilibria in the tangle	Computers & Industrial Engineering	64	A1(CC); A1(E2); A1(ADM); A2(IT)	outro	N/A
Prototype for dual digital traceability of metrology data using X.509 and IOTA	CIRP Annals	49	A1(E3)	outro	N/A
Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach	IEEE Transactions on Engineering Management	26	A2(CC); B1(E3)	outro	N/A

4.2.4 Etapa 5 - Sigfox

O descritor “Sigfox” resultou em 493 resultados, sendo 136 na IEEE Xplore, 140 no Web of Science e 217 na Scopus. Os resultados podem ser observados na Figura 19.

Figura 19 – Etapa 5: Pesquisas relacionadas à rede LPWAN Sigfox



A atualidade da pesquisa sobre “Sigfox”, pode ser constatada na Figura 19. Os primeiros resultados aparecem apenas em 2015, o que poderia ser imaginado, pois a Sigfox foi criada apenas em 2009. Pode-se dizer também, que o volume de publicações vem aumentando. No ano de 2019 foram encontrados 184 resultados.

Os artigos representam 143 dos 493 resultados. Utilizando o software Endnote, foram encontrados 29 resultados repetidos, restando 114 artigos. Buscou-se identificar por meio de uma análise exploratória nos títulos e resumo desses artigos, aqueles que estão relacionados ao monitoramento ou rastreamento utilizando Sigfox, foram localizados 4 resultados únicos. O mesmo foi feito para Sigfox na cadeia de suprimentos, sendo recuperado 1 resultado. Ademais, utilizando o filtro de qualidade definido na Seção 4.1.3, 1 artigo foi excluído da análise. Os artigos selecionados podem ser visualizados na Tabela 6.

Tabela 6 – Artigos - Sigfox

Artigo	Periodico	H5-index	Qualis	Aplicação
A low-cost IOT-based system to monitor the location of a whole herd	Sensors	104	A1(CC); A1(E4); A2(IT)	Monitoramento
Proposal for the design of monitoring and operating irrigation networks based on IoT, cloud computing and free hardware technologies	Sensors	104	A1(CC); A1(E4); A2(IT)	Monitoramento
An alternative wearable tracking system based on a low-power wide-area network	Sensors	104	A1(CC); A1(E4); A2(IT)	Monitoramento
Localization in Low Power Wide Area Networks Using Wi-Fi Fingerprints	Applied sciences	53	B1(CAgra); B2(CB 1); B3(CB2)	Cadeia de suprimentos

4.3 ANÁLISE DESCRIPTIVA

A busca por produções bibliográficas que se aproximem das propostas da dissertação resultou em 21 trabalhos encontrados: 10 propostas de soluções no uso Blockchain para monitoramento na cadeia de suprimentos; 6 resultados que utilizam IOTA como uma solução de protocolo distribuído para comunicação de dados; e 4 trabalhos relacionados ao uso da Sigfox no monitoramento de sensores ou aplicada a cadeia de suprimentos.

Nenhum dos trabalhos encontrados, possui interface entre todas as temáticas envolvidas nessa dissertação. Ainda não existem artigos que busquem utilizar IOTA na cadeia de suprimentos e apenas 1 artigo aplica Sigfox a cadeia de suprimentos. Não há qualquer menção sobre o potencial uso de IOTA e Sigfox em conjunto.

Outro fator importante a ser observado trata-se do aceite das pesquisas nos periódicos. Pode-se dizer, que de acordo com o Qualis dos periódicos, as principais temáticas deste trabalho são das áreas de computação, interdisciplinar e engenharias. Pode-se afirmar também que os temas são de interesse da comunidade científica e vêm sendo aceitos em periódicos de alto impacto. As revistas com maior quantidade de publicações são: Sensors (2 artigos sobre IOTA; 3 artigos sobre Sigfox) e IEEE Access (4 - artigos sobre Blockchain no monitoramento da cadeia de suprimentos; 1 artigo sobre IOTA).

4.3.1 IOTA/Tangle

Pesquisadores do setor de saúde buscam na tecnologia IOTA a possibilidade de compartilhar dados de pacientes da maneira menos invasiva possível e de forma barata

e segura, permitindo que essas pessoas possam inclusive revogar o compartilhamento de seus dados. A ausência de custos para transações, integridade dos dados e o protocolo MAM são vistos como garantidores de segurança, privacidade e baixo custo. Os dados dos pacientes podem ser obtidos de dispositivos vestíveis ou outros sensores (JIANG *et al.*, 2019) (SUN *et al.*, 2019) (ZHENG *et al.*, 2019).

A pesquisa de aplicações automotivas são motivadas pela baixa segurança dos sistemas atualmente implantados em automóveis e pela possibilidade de comércio seguro e confiável de energia em estações de recarga de energia para carros elétricos (HASSIJA *et al.*, 2020) (FLOREA, Bogdan Cristian; TARALUNGA, 2020).

O uso de *tokens* IOTA é proposto como uma forma de estimular o comportamento humano através do depósito e resgate de *token*. O *token* é usado para garantia de bom comportamento (FERRARO *et al.*, 2018). Assim a IOTA não é apenas uma criptomoeda, é também um protocolo de comunicação distribuída, que trabalha com algoritmos de consenso em uma rede distribuída, essa evidência fica mais clara ao analisar as aplicações dessa tecnologia.

4.3.2 Sigfox

Três dos quatro trabalhos selecionados que utilizam Sigfox, relacionam suas escolhas como uma solução economicamente barata, e com ampla área de cobertura (MAROTO-MOLINA *et al.*, 2019) (FERNÁNDEZ-AHUMADA *et al.*, 2019) (FERNÁNDEZ-GARCIA; GIL, 2017). Alguns autores propõe uma solução alternativa de rastreamento de dispositivos, para sistemas que usam Sigfox buscando redução de consumo energético (JANSSEN *et al.*, 2017).

Outros autores utilizam Sigfox para monitoramento de rebanho, segundo os pesquisadores, atualmente soluções de rastreamento de animais baseadas em sistemas de posicionamento global (GPS) estão disponíveis comercialmente, no entanto, os dispositivos existentes têm várias restrições, principalmente relacionadas à transmissão de dados sem fio e ao custo financeiro, que inviabiliza a monitoração de todos os animais em um rebanho. Sendo assim, o principal objetivo deste trabalho foi desenvolver uma solução de baixo custo para permitir o monitoramento de um rebanho inteiro. Foi desenvolvido um sistema baseado em IoT, que exige que alguns animais do rebanho estejam equipados com GPS conectados a uma rede Sigfox e o restante com *tags Bluetooth* de baixo custo (MAROTO-MOLINA *et al.*, 2019).

Ahumada et al. (2019) apresenta uma solução de baixo custo para irrigação automática baseada em nuvem. Os autores projetam uma rede de nós baseada em um microcontrolador Lora e conexão de rede Sigfox. Pois, segundo os autores, a automação de processos de irrigação no campo, encontrou várias dificuldades, incluindo a falta de redes de comunicação e as grandes distâncias para os pontos de fornecimento de energia elétrica. A implementação recente de redes de comunicação sem

fio LPWAN (Sigfox, LoraWan e NB-IoT) e o mercado de controladores eletrônicos com baixo consumo de energia, possibilitou novas perspectivas para automação de redes de irrigação agrícola, que são exploradas nesse trabalho (FERNÁNDEZ-AHUMADA *et al.*, 2019).

O trabalho de Garcia et al. (2017) apresenta um sistema alternativo de rastreamento vestível baseado em Sigfox. Um receptor GPS foi integrado a um substrato têxtil e as coordenadas de latitude e longitude foram enviadas para a nuvem por meio da rede Sigfox. Para enviar as coordenadas pelo protocolo Sigfox, foi utilizado um algoritmo de codificação específico que foi projetado, simulado e testado em uma antena UHF personalizada em tecido jeans. Um servidor remoto específico foi desenvolvido para decodificar as coordenadas de latitude e longitude. Depois de decodificadas as coordenadas, o servidor remoto envia essas informações ao visualizador de dados de código aberto SENTILO para mostrar a localização do nó do sensor em um mapa. A funcionalidade deste sistema foi demonstrada experimentalmente. Os resultados garantem a utilidade e a usabilidade do sistema de rastreamento proposto para o desenvolvimento de nós sensores e apontam que pode ser uma alternativa de baixo custo a outros produtos comerciais baseados em redes de celular.

Outro artigo sugere que o gerenciamento da cadeia de suprimentos exige atualizações regulares da localização dos ativos, que podem ser ativadas por redes LPWAN, como a Sigfox. Embora seja possível localizar um dispositivo simplesmente com seus sinais de comunicação, a precisão é prejudicada com Sigfox devido à ampla área de cobertura de uma antena. Por outro lado, a instalação de um elemento de localização de satélite no dispositivo aumenta muito seu consumo de energia. Os autores investigam o uso de informações sobre pontos de acesso *Wi-Fi* próximos, como forma de localizar o ativo pela rede Sigfox, sem a necessidade de conexão com essas redes *Wi-Fi*. O artigo relata o erro de localização que pode ser alcançado por esse tipo de localização externa. Usando uma combinação de dois bancos de dados, pode-se localizar um dispositivo com erro médio de 39 m. Isso mostra que a precisão da localização desse método é promissora (JANSSEN *et al.*, 2017).

4.3.3 Blockchain no monitoramento e rastreamento da cadeia de suprimentos

De forma geral, os artigos que mais se aproximam da temática da dissertação foram encontrados na etapa 2 da pesquisa. Os artigos de monitoramento ou rastreamento de dados de produtos da cadeia de suprimentos utilizando Blockchain. As temáticas podem ser divididas em duas partes, aquelas que fazem acompanhamento enquanto a carga está parada sobre a custódia ou durante o seu transporte, a segunda opção está mais diretamente relacionada a proposição aqui levantada.

4.3.3.1 Monitoramento durante a custódia

Dentre os tipos de monitoramento apresentados na Tabela 4, três propõem monitoramento do produto apenas quando ele está sob nova custódia. Os autores apresentam três diferentes possibilidades desse acompanhamento.

Alguns autores propõem uma arquitetura que se concentra principalmente nas atividades de entrega de pacotes. A principal funcionalidade do sistema consiste na entrada de transações na rede Ethereum, utilizando um sistema. Esse sistema permite incluir em um bloco do Blockchain, informações do pacote, inspeção de qualidade, informações do operador, informações de localização e um carimbo de data/hora. O bloco registrado passa a fazer parte de uma série de blocos relacionados ao produto (HELO; HAO, 2019).

A solução de Hasan et al. (2020) busca armazenar detalhes das peças de reposição e cotações dos fornecedores. Os contratos inteligentes da **Ethereum** são utilizados para registrar todas as informações de comunicação entre as entidades participantes. Por este motivo os autores modelam contratos inteligentes para cada etapa necessária para sua execução. No entanto, segundo os autores, a solução descentralizada proposta é genérica e, portanto, pode ser implementada em uma infraestrutura pública ou privada de Blockchain (HASAN, H. R. et al., 2020).

Outros autores propõem um tipo de mecanismo de consenso, o *proof-of-object(PoO) based authentication protocol*. Similar ao PoW, no PoO quem estiver em posse do objeto físico pode reivindicar sua posse por meio de uma prova criptográfica, adquirida por meio de uma etiqueta de RFID acoplada ao objeto. Depois que um nó reivindica o objeto por meio do PoO, outros nós participantes verificam a autenticidade da declaração. O novo bloco é adicionado assim que for alcançado um consenso sobre a autenticidade do bloco (MONDAL et al., 2019)

4.3.3.2 Monitoramento não definido

Um sistema que faz acompanhamento das emissões de carbono por meio de contrato inteligente foi proposto por Manupati et al. (2019). Ele executa um contrato inteligente quando identifica que as emissões passam de um determinado marco. Os autores modelam matematicamente equações para o cálculo das emissões de carbono. O cálculo é baseado no local (estoque, transporte e fabricação) e tempo de espera, transporte ou fabricação. Buscando remodelar a logística visando menos emissões (MANUPATI et al., 2020).

4.3.3.3 Monitoramento contínuo

Seis artigos apresentados na Tabela 4, projetam o monitoramento contínuo dos produtos. Quatro desses artigos estão relacionados ao monitoramento de produtos que

se deterioram na ausência de controle e/ou no passar do tempo; e dois artigos propõem uma solução abrangente para cadeia de suprimentos. A seguir, são apresentados de forma sintética os artigos, as principais escolhas e implicações relativas ao uso da Blockchain.

Um sistema baseado em nuvem para acompanhamento em tempo real das cadeias de logística e suprimentos foi proposto por Helo e Shamsuzzoha (2019). Os autores definem alguns problemas de logística e apresentam, de forma abrangente, uma possível solução. Para esses autores o sistema deve ser formado pela combinação de RFID, IoT e tecnologia Blockchain em uma visualização integrada em “tempo real”. As etiquetas de RFID (do inglês, *Radio Frequency Identification*) e sensores IoT fornecem dados em tempo real, enquanto a tecnologia Blockchain é usada para fornecer uma cadeia de transações imutáveis. O único teste feito pelos autores é a criação de blocos na rede Kovan (rede de teste pública), que simula a situação de uma Blockchain baseada em Ethereum privada. Os autores concluem que o tempo de processamento para geração e verificação dos blocos existentes podem levar entre 15 e 30 s, dependendo da situação da rede. Esses números de desempenho mostram que o Blockchain não resolve a necessidade de consultas rápidas de dados. Para acesso rápido, é necessário usar um armazenamento local para clientes, o que requer capacidade de 500 MB, dependendo do histórico de transações valiosas (HELO; SHAMSUZZOHA, 2020).

Maiti, Kang e Haedy (2019) estudam e modelam um sistema de rastreamento baseado no Blockchain, onde um microcontrolador é usado para rastrear o status de sensores. Se eles não estiverem dentro de um intervalo especificado, um conjunto de penalidades é aplicado. O sistema proposto permite que os dispositivos IoT enviem dados para o Blockchain por meio de contratos inteligentes. Depois que os dados são inseridos na Blockchain, um sistema pode procurar dados para correlacionar com outros dispositivos similares. Dessa forma, uma penalidade pode ser calculada ao longo do tempo, caso o sistema não se comporte adequadamente. Conectividade: os autores ressaltam que o mecanismo de comunicação podem ser *Wi-fi/Ethernet* com conexão direta à Internet, LPWAN como LoRa ou conexão celular. Nos dois últimos, os dados são enviados para um *gateway* da Internet. Os dados são finalmente transmitidos para um conjunto de servidores executando o blockchain. Os dispositivos IoT podem ter problemas com o monitoramento do sensor e a transmissão de dados se eles forem alimentados por bateria ou colocados em áreas de cobertura de comunicação baixa, ou intermitente. A escolha da Blockchain: O Ethereum é a escolha básica do Blockchain, mas exige que os usuários paguem para armazenar as informações no Ethereum principal. Como se trata de um livro contábil, é necessário criar códigos de cadeia para verificar e manter a propriedade dos dispositivos. Assim, o *BigchainDB* (privada) é usado para esta implementação. O uso de uma Blockchain privada é utilizado, pois

permite que o sistema funcione rapidamente. No caso de um ataque no estilo DDoS, as solicitações de transação podem ser distribuídas corretamente e o serviço pode ser mantido normalmente. De acordo com os autores, as Blockchains privadas como banco de dados podem suportar o gerenciamento de dados da IoT facilmente (MAITI *et al.*, 2019).

As abordagens de (SALAH *et al.*, 2019) utiliza o Blockchain Ethereum com seus contratos inteligentes para realizar transações comerciais de acompanhamento e rastreabilidade da soja em toda a cadeia de suprimentos agrícola. A solução proposta se concentra na utilização de contratos inteligentes para governar e controlar todas as interações e transações entre todos os participantes envolvidos no ecossistema da cadeia de suprimentos. A solução também possibilita o acompanhamento com dispositivos IoT, no entanto, não são exploradas as deficiências e detalhamento dessa questão. Os autores apenas comentam que até o momento, a tecnologia Blockchain ainda enfrenta os principais desafios relacionados à escalabilidade, governança, registro de identidade, privacidade, normas e regulamentos.

Os autores Baralla et al. (2020) projetaram e desenvolveram um sistema de rastreamento para cadeia de suprimentos agroalimentar, buscando garantir a integridade e a rastreabilidade dos alimentos, durante todas as fases da cadeia de distribuição. O sistema utiliza Blockchain da Ethereum permissionada suportada por uma camada de controle de acesso adicional e por um banco de dados externo. A camada de controle de acesso permite supervisionar a leitura e gravação de dados por partes licenciadas interessadas, ou seja, atores regularmente credenciados para executar um trabalho específico. O modo público da Ethereum garante maior transparência. O banco de dados externo também contém dados confidenciais e uma grande quantidade de dados, provenientes de dispositivos IoT, que são grandes demais para serem armazenados na Blockchain, tendo em vista que o registro de dados em uma Blockchain não permissionada tem um custo diretamente proporcional ao tamanho dos dados. A integridade dos dados armazenados no banco de dados é aprimorada registrando o código de *hash* do recurso e a URL que aponta para esse recurso, na Blockchain. Os dados detectados pelos sensores, como temperatura ou umidade, são gravados periodicamente em um arquivo de *log* vinculado ao lote. Durante o transporte, além dos dados anteriores, podem existir registros provenientes de dispositivos GPS que confirmam o movimento do lote entre dois locais diferentes. Todos os dados registrados durante o transporte são armazenados nos respectivos arquivos de *log* assim que o lote é entregue. O registro dos dados na Blockchain ocorre sempre que o lote sofrer uma mudança de estado ou se sofrer uma variação muito grande. Sempre que for necessário armazenar dados na Blockchain, uma nova instância de estrutura de dados correspondente é criada pelo contrato inteligente associado. Se a nova instância for uma informação atualizada de um lote, será adicionado um link para a anterior(BARALLA *et al.*, 2020). Não há

menções sobre conectividade dos dispositivos IoT ou em que momento os *logs* são verificados.

Hasan et al. (2019) propõe uma solução para o gerenciamento eficiente da cadeia de suprimentos, que envolve o envio de itens por contêineres inteligentes. A solução proposta utiliza os recursos de contratos inteligentes no Blockchain Ethereum para governar e gerenciar as interações entre o remetente e o destinatário. Um contrato inteligente que une as entidades da cadeia de suprimentos, é criado e iniciado pelo remetente. O contrato inteligente rege automaticamente as regras pelas quais o destinatário deve depositar o pagamento antes do envio e, se o envio chegar ao destino sem violações, o pagamento será emitido ao remetente. Por outro lado, se ocorrerem violações aos critérios de remessa, a remessa será abortada e um reembolso será emitido para o destinatário. Além disso, os autores preveem regras específicas para retirar a carga e outros tipos de multas. A conectividade dos sensores dentro do contêiner ocorre por 4G ou 5G para a transmissão periódica dos dados a um servidor MQTT e para a comunicação com a rede Blockchain Ethereum. Alertas e notificações automáticos são enviados ao remetente e ao destinatário quando determinadas condições não são atendidas ou ocorrem violações durante o transporte. As violações são determinadas por um mecanismo baseado em regras executadas por uma Raspberry Pi, dentro do container e enviados para a Blockchain. O não cumprimento dessas regras é considerado uma violação. As leituras do sensor são monitoradas pelo contêiner habilitado para IoT e sempre que houver variações, o contêiner de remessa inicia a chamada para determinadas funções dentro do contrato inteligente e, em seguida, os eventos dessas violações são transmitidos a todas as partes interessadas, incluindo o remetente e o destinatário. Qualquer transação na cadeia custa uma certa quantidade de Ether ou criptomoeda. A taxa de transação de todas as funções é calculada como “gas” na Blockchain Ethereum, mas o custo é pago em “Ether”. Por outro lado, o preço do “gas” fornece o custo em Ether para uma unidade de gas, que recebe a unidade “Gwei”. Portanto, uma quantidade maior de Gwei incentivaria os mineradores e elevaria a prioridade da transação. Por isso, é importante estudar e examinar o código para possíveis maneiras de diminuir o custo e torná-lo mais eficiente (HASAN, H. et al., 2019).

Tsang et al. (2019) propõem uma arquitetura para rastreabilidade de produtos perecíveis. São premissas dos autores, a incompatibilidade de sistemas Blockchain com alta carga de dados e dificuldades inerentes de Blockchain em forjar blocos computacionalmente baratos e confiáveis. A proposta conta com um novo tipo de mecanismo de consenso, diferente de Blockchains tradicionais, os autores propõem o *proof of supply chain share (PoSCS)*, desenvolvido para selecionar validadores de maneira probabilística para forjar e validar os blocos no Blockchain. Seu algoritmo de consenso considera o tempo de trânsito do produto, análise das partes interessadas e o volume

de remessas nas cadeias de suprimentos, em vez de poder computacional e riqueza. Além disso, os autores propõem uma solução híbrida para integrar tecnologias de IoT, computação em nuvem e Blockchain. As interações de IoT em tempo real seriam gerenciadas em um banco de dados em nuvem, em vez de armazenar todos os dados no Blockchain. O modelo reduz a carga computacional pré-processando os dados dos dispositivos IoT em um banco de dados em nuvem, enquanto os IDs de associação dos dados são gerados para armazenamento nos blocos no final do ciclo. Essas escolhas buscam utilizar blocos de dados leves que podem ser operados no Blockchain para melhorar a adaptabilidade e flexibilidade do sistema (TSANG *et al.*, 2019).

4.3.4 Diferenciais do trabalho proposto

Na literatura encontram-se trabalhos que propõe o monitoramento ativo de dados para cadeia de suprimentos utilizando sistemas distribuídos baseados em Blockchain públicos, no entanto esses sistemas são economicamente custosos, exemplo disso é o sistema implementado por Baralla et al. (2020) em que as taxas de registro na Blockchain da Ethereum variaram entre \$ 0,122 (0,00083 ETH) e \$ 0,244 (0,00166 ETH), com tempo médio de confirmação das transações de 63s e 25s respectivamente. Os dados foram simulados em dezembro de 2019, com uma ferramenta oferecida pelo ethgasstation.info. Registrar uma carga mínima de dados na Blockchain da Ethereum nos dias de hoje (26/08/2020) custa taxas médias entre \$ 0,52 (0,001344 ETH) e \$ 0,71 (0,001848 ETH), com tempo de confirmação das transações de 56s (4 blocos) e 28s (2 blocos), respectivamente. Esse exemplo torna evidente que sistemas Blockchain públicos não são adequados para armazenamento de fluxos de dados. Os custos de armazenagem de dados podem ficar caros quando se trata de registros advindos de sensores. Por outro lado, sistemas baseados em Blockchain privados como Hiperledger e BigchainDB não são completamente transparentes, pois nem todos os interessados podem acessar e participar da rede Blockchain. Além disso, em relação a conectividade de sensores, frequentemente usa-se rede celular, no entanto, o design da tecnologia implica em planos de conectividade custosos quando comparados com redes LPWAN. Por esses motivos, uma arquitetura que combine conectividade Sigfox com IOTA é inédita e permite, potencialmente registrar fluxos de dados advindos de sensores utilizando conectividade Sigfox na rede segura, imutável e pública da IOTA.

5 METODOLOGIA DA PESQUISA

Este capítulo apresenta os procedimentos adotados para o desenvolvimento do protótipo. A Figura 20 exemplifica as etapas que serão seguidas, buscando apresentar o desenvolvimento do protótipo.

Figura 20 – Etapas da pesquisa tecnológica



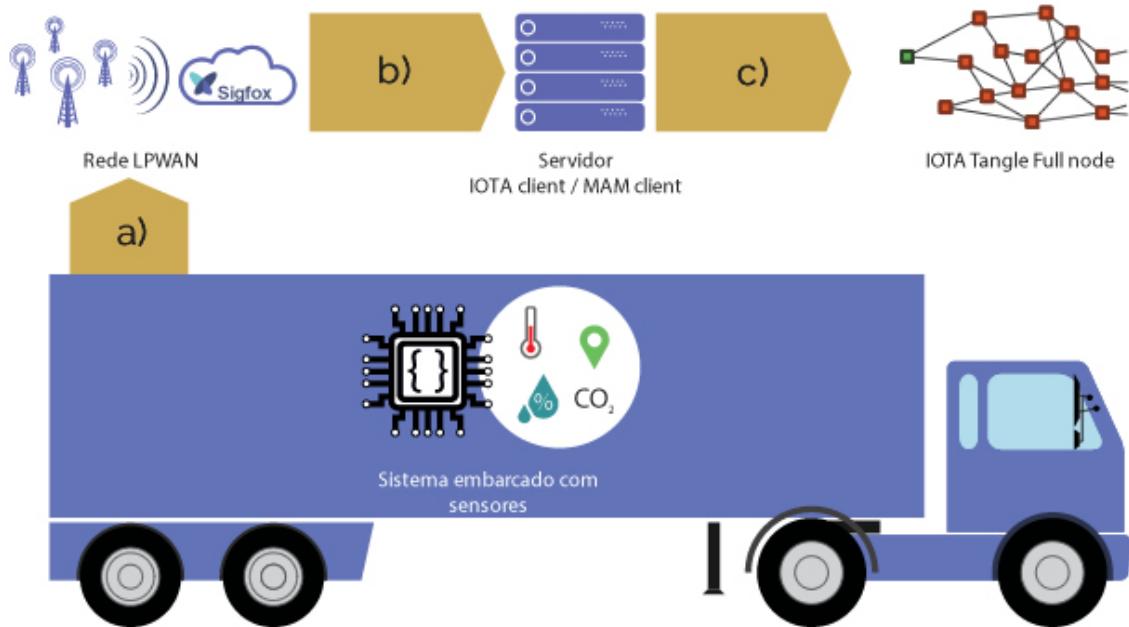
A pesquisa experimental também conta com experimentações, e detalhamento do ambiente de pesquisa, que será apresentado no capítulo seguinte.

5.1 ARQUITETURA DO ECOSISTEMA

Após o completo entendimento das tecnologias IOTA e Sigfox, foi possível modelar a arquitetura capaz de suplantar o desenvolvimento e testes do protótipo. O modelo proposto consiste em um sistema embarcado, em movimento, capaz de realizar medições e enviá-las via rede Sigfox para armazenamento na rede distribuída da IOTA. Porém, dadas as características das tecnologias, faz-se necessária a utilização de um servidor intermediário, capaz de gerar e enviar pacotes IOTA para um *Fullnode* da rede (SILVANO, W. F. et al., 2020). A Figura 21 sintetiza o esquema proposto para capturar os dados de entrada e inseri-los no Tangle.

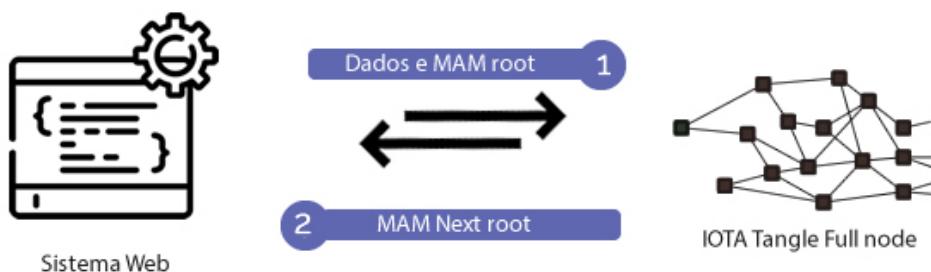
Esquematicamente pode-se separar a função do servidor em três: receber dados da Sigfox; criar pacotes e inserir dados no Tangle; apresentar dados ao usuário. Para inserir dados no Tangle, utilizou-se a biblioteca MAM pois permite trabalhar melhor com fluxos de dados na rede. Para abrir um canal MAM é necessário primeiramente criar um canal único para as mensagens, este será a raiz da árvore Merkel apresentada na Seção 2.2.7, a partir dela cada nova mensagem inserida na rede será armazenada em uma nova mensagem na rede IOTA e fará parte do fluxo de mensagens. Portanto é importante guardar a raiz (root) da árvore Merkel inicial (nome do canal MAM) para visualização dos dados completos. É igualmente importante guardar o “next root” para inserção dos próximos dados. A Figura 22 apresenta a primeira etapa de inserção dos dados no MAM, em a) os dados são do dispositivo sensor via rede Sigfox, em b) passam por um servidor que cria o pacote IOTA, em c) os dados são enviados para um *Fullnode* IOTA.

Figura 21 – Arquitetura proposta



Fonte – O autor

Figura 22 – Inserção de dados utilizando MAM



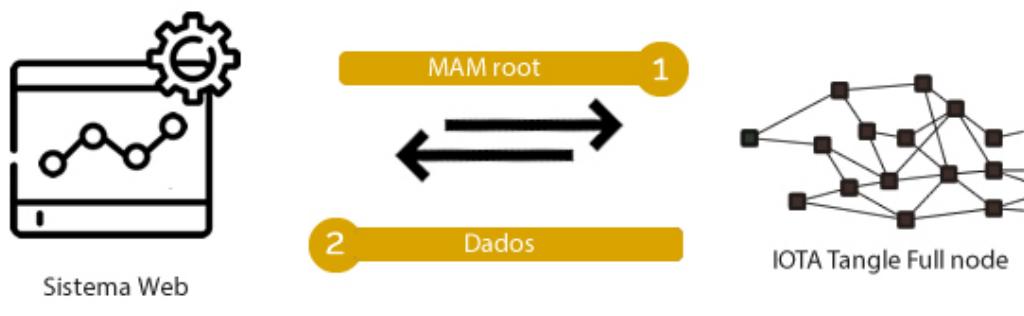
Fonte – O autor

As mensagens/dados subsequentes serão inseridos igualmente ao serem apresentados na Figura 22, porém será necessário capturar o “next root” armazenado no banco de dados.

Para visualização, os dados são recebidos diretamente do Tangle, nenhum dado é armazenado no banco de dados. Portanto, sempre que um usuário quiser visualizar os dados, uma requisição de acesso ao canal MAM é feita com o MAM root, retornando os dados armazenados no canal MAM (Figura 23).

Para fins de execução do projeto, os dados em a) passam anteriormente pelo

Figura 23 – Visualização dos dados



Fonte – O autor

servidor da empresa Ayga (Figura 24 a1) e complementação da Here (Figura 24 a2), descrita a posteriori.

Para fins de idealização do projeto, a arquitetura apresentada na Figura 24 não precisa ocorrer se quisermos um sistema com o menor número possível de pontos de falhas. Esse fato, no entanto, facilitou o desenvolvimento dessa pesquisa. O entendimento do ecossistema necessário, ajudou também a identificar quais tecnologias e desenvolvimentos necessários para execução deste protótipo.

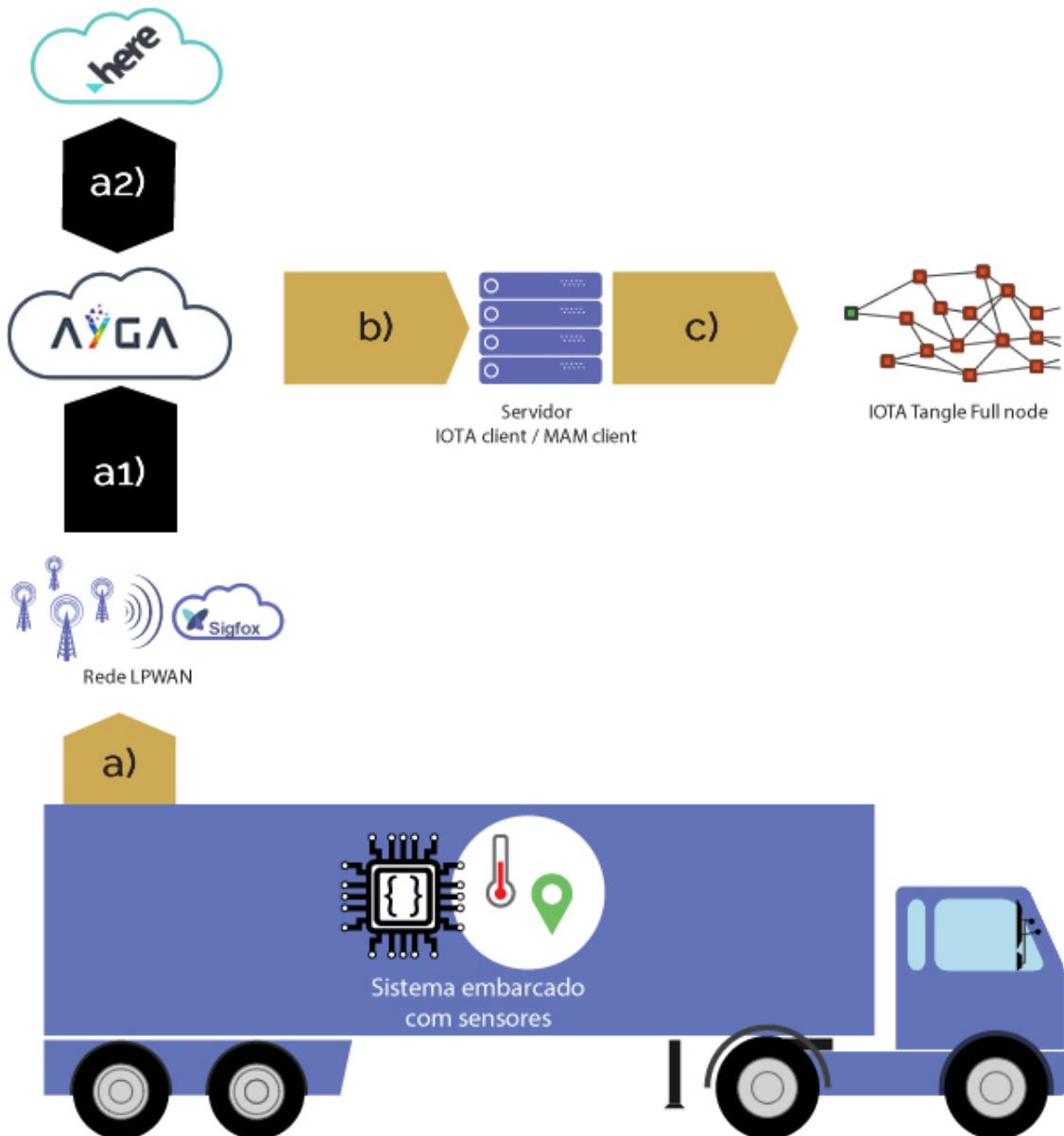
5.2 TECNOLOGIAS ENVOLVIDAS

Além de Utilizar IOTA e Sigfox, para execução dessa dissertação utilizaram-se outras tecnologias, tais como o dispositivo de Hardware, responsável pela medição dos dados, sistema de apoio para obtenção de geolocalização (API da empresa Here) e outras tecnologias relacionadas ao desenvolvimento de um sistema Web.

5.2.1 Sistema Embocado

A escolha do hardware é fundamental para viabilizar a implantação de um projeto IoT, em especial o proposto por essa dissertação. O principal objetivo na escolha do hardware foi manter as qualidades centrais das outras duas tecnologias utilizadas (IOTA e Sigfox), que são o baixo custo e baixo consumo de energia, de modo a facilitar a coleta de dados ambientais e possibilitar a geolocalização do dispositivo. No entanto, percebeu-se um problema fundamental na obtenção de geolocalização, esse tipo de dispositivo costuma demandar uso excessivo de energia. Nesse sentido, não basta acoplar um GPS a um dispositivo Sigfox. Por outro lado, foi encontrado na literatura um candidato promissor para obtenção de geolocalização, a utilização de *MAC Address*(do inglês, *Media Access Control*) de redes *Wi-fi*, muitas vezes chamada

Figura 24 – Arquitetura da dissertação



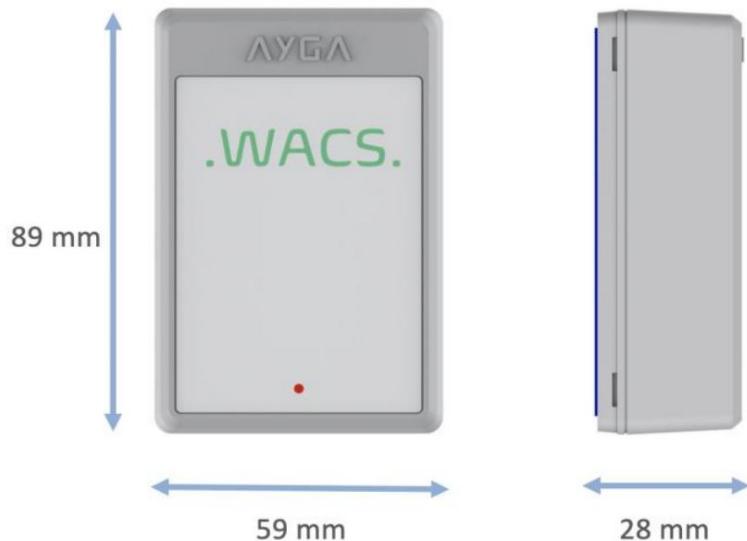
Fonte – O autor

de “tringulação de sinais de rede Wi-fi” (LYMBEROPoulos *et al.*, 2015) (LEMIC *et al.*, 2015) (BAHL; PADMANABHAN, 2000) (CHINTALAPUDI *et al.*, 2010) (LEMIC *et al.*, 2016)(SALLOUHA *et al.*, 2017) (SONG *et al.*, 2017) (PECORARO *et al.*, 2018) (AERNOOTS *et al.*, 2018). Dessa maneira, buscou-se por um dispositivo de hardware que pudesse fornecer antena Wi-fi para captura de *MAC address*, sensores e módulo Sigfox.

5.2.1.1 AYGA WACS-2

Encontraram-se as soluções pretendidas em um hardware protótipo desenvolvido pela empresa Ayga. A empresa forneceu um dispositivo que utiliza Sigfox como protocolo de comunicação de rede e possui módulo para identificação de rede Wi-fi, além de outros sensores. Esse dispositivo recebe o nome de WACS 2 (Figura 25). As principais características do dispositivo relacionadas a este trabalho são apresentadas na Tabela 7.

Figura 25 – WACS 2



Fonte – Ayga (2020)

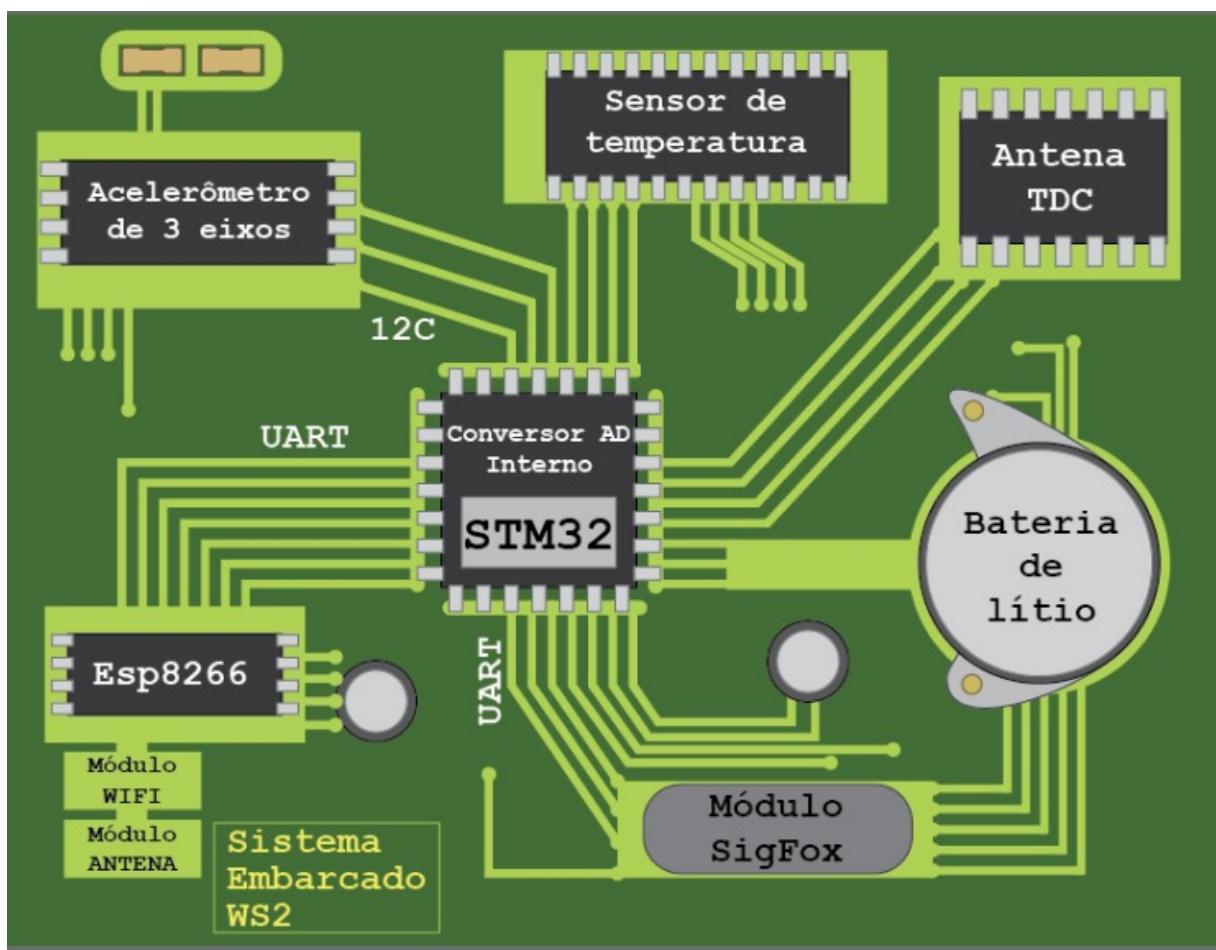
A arquitetura da placa é representada na Figura 26, apresentada na Figura 27, e descrita a seguir.

A placa do dispositivo tem como microcontrolador o STM32 que funciona como “cérebro” do sistema embarcado. Esse microcontrolador opera com tensão entre 1.8 e 3.6V, tendo um *clock* operacionalizado por um cristal que varia entre 4 a 26MHz. Com três ADC internos, 140 pinos I/O, duas entradas UARTs (7.5Mbit/s), quatro entradas

Tabela 7 – Ayga Wacs 2

Característica	Descrição
Módulo Wi-fi	Obtenção de MACs de ponto de acesso Wi-Fi de 2,4 GHz
Sensor de temperatura	Faixa de medição: -20 a 60 ° C; Resolução: 0,1 ° C; Precisão: 1%
Sensor de movimento	Aceleração máxima: +- 16 g; Taxa máxima de atualização: 200 Hz
Temperatura de operação	-20 a 65 ° C
Dimensões	59 x 89 x 28 mm

Figura 26 – WACS 2: ilustração dos componentes

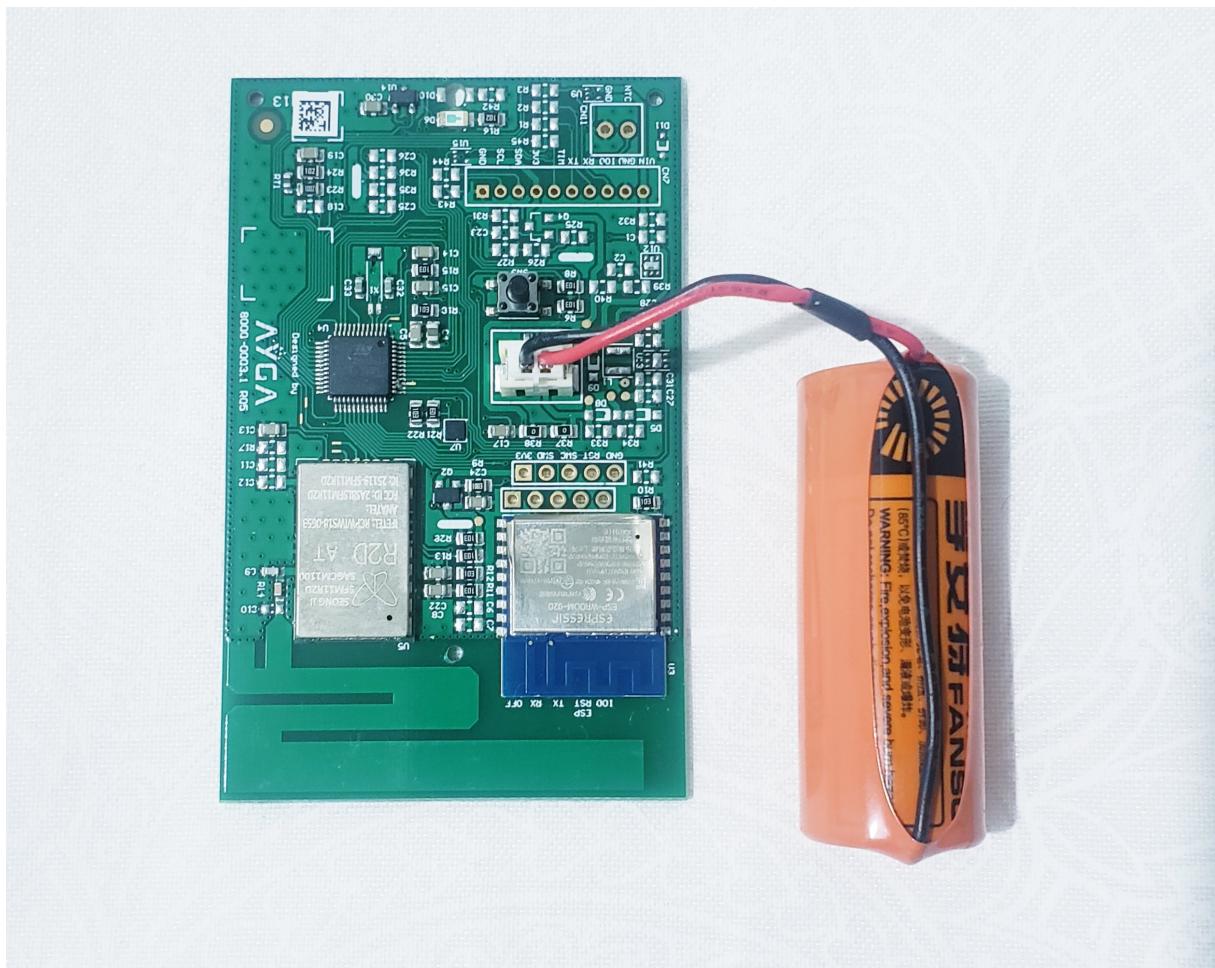


Fonte – O autor

UARTs e duas entradas USB 2.0. Processador Arm Cortex-M3 com barramento de 32 bits e arquitetura RISC.

Conectado ao conversor AD interno do STM32 existe um Sensor de Temperatura NTC passivo de alta precisão. Este sensor consegue converter a temperatura ambiente em uma tensão linear com uma precisão de 0,1°C. Esta tensão por sua vez, é convertida em um sinal digital pelo conversor AD para ser utilizado em outros lugares

Figura 27 – WACS 2: foto real



Fonte – O autor

do sistema embarcado.

O módulo e antena *Wi-fi* é acoplado em um ESP8266, compatíveis com o protocolo 802.11 b/g/n da IEEE, podendo ler sinais da faixa dos 2.4GHz (velocidade de até 71 Mbps). O ESP8266 escaneia por roteadores de *Wi-fi* próximos e escolhe uma quantidade de sinais específicos. O sistema interno da Ayga, acoplado ao dispositivo é responsável por selecionar os melhores sinais. A avaliação de quais sinais é feita com as seguintes variáveis: Intensidade do sinal (os mais próximos ao dispositivo tem maior intensidade), exclusão de sinais com nomes de rede de celular e/ou, acesso remoto mobile. Fazendo essa avaliação é obtido os *MACs* das redes.

O último componente do sistema embarcado é a antena Sigfox. Esse componente é responsável por converter os sinais digitais em ondas eletromagnéticas, e vice-versa. A antena foi desenvolvida do zero, podendo se comunicar com a rede Sigfox no Brasil. A antena utilizada é omnidirecional. Então o sinal é enviado em 360º a partir da antena, ou seja, tendo a antena como centro, o sinal é enviado em todas as

direções. Outra característica importante da antena é a sua topologia. Nesse projeto é utilizado uma topologia F invertido. Essa topologia consiste em uma antena monopolo (um condutor reto em forma de haste), mas ao invés de ser perpendicular ao plano de aterramento, ela é paralela.

O sistema embarcado recebe energia por uma bateria de lítio de 3,5 v.

5.2.2 API Here - Geolocalização

A obtenção dos *MAC Address*, obtidos com a antena *Wi-fi* do dispositivo WS2 não é capaz de fornecer a localização, isso é conseguido utilizando um banco de dados contendo *MAC address* e localização do roteador (latitude e longitude). Isso poderia ser mapeado manualmente, ou ainda utilizar um serviço de terceiro. Para execução do projeto, optou-se por utilizar a API da empresa Here, que por conseguinte utiliza dados mapeados pelos Google e outras bibliotecas.

Além de fotos e informações 3D, os “carros do google” (Figura 28) também são usados para capturar informações que estão soltas no ar, especificamente nomes de redes *Wi-fi* e seus respectivos endereços MAC (GOOGLE, 2010).

Figura 28 – Carro Google



Fonte – Aleksey Baranenko

A empresa Here fornece um serviço para obter a estimativa de localização com base em *MAC address*, por meio de uma comunicação HTTPS usando POST. Tanto a solicitação quanto a resposta são formatadas como JSON, e o tipo de conteúdo de ambas é application/json (HERE, 2021).

5.2.3 Sistema Web

O desenvolvimento do sistema web, envolve uma série de tecnologias e/ou linguagens de programação.

5.2.3.1 MongoDB

Optou-se por utilizar o MongoDB para guardar informações do usuário, como contas (nome, senha, entre outros) e informações sobre distribuidores e suas viagens.

Esse é o banco de dados do MERN, sigla em inglês que engloba diferentes tecnologias que compõe o *back-end* de uma aplicação web, MongoDB (M), Express (E), *framework* de *back-end* (F), React (R), NodeJS (N). Sendo um banco de dados não relacional, ele é mais rápido que bancos de dados relacionais, mas não consegue manter a integridade do mesmo jeito que seu concorrente. Por não ter relações, esse tipo de banco acaba escalando verticalmente, sendo ideal para aplicações IoT (PORTER *et al.*, 2019). As tabelas e linhas do SQL (do inglês, *Structured Query Language*) são substituídos por coleções e documentos no NoSQL (NGUYEN; LEE, S.-W., 2018).

A funcionalidade que é mais utilizada do MongoDB é a possibilidade de guardar dados dinâmicos em documentos do tipo BSON. Documentos que são da mesma coleção podem ter diferentes campos e pares chave-valor, enquanto que esses dados podem ser mudados sem nenhum tipo de restrição. Isso faz com que não sejam necessários dados estritamente estruturados, que é obrigatório em banco de dados relacionais, essa possibilidade aumenta a velocidade das operações realizadas no banco (NGUYEN; LEE, S.-W., 2018).

5.2.3.2 React

React é o componente de *front-end* da MERN. Desenvolvido e mantido pelo Facebook. Uma das grandes vantagens do React sob os seus concorrentes é a facilidade de aprender a utilizar a ferramenta (PORTER *et al.*, 2019).

O React funciona com componentes, em que cada pedaço da interface do usuário é desenvolvido como um componente individual que pode ser reutilizado em outra parte da interface ou até em outro projeto. O React, por ser desenvolvido em Javascript, herda da sua linguagem o poder de atualizar dados dinamicamente na página sem precisar recarregar (NGUYEN; LEE, S.-W., 2018).

5.2.3.3 Node

O Node é uma ferramenta de *back-end*, o qual é um servidor assíncrono escrito em Javascript baseado na tecnologia Google V8. Por utilizar o Javascript, o Node é executado em apenas um processo, mas isso, apesar de causar problemas de velocidade, reduz os *bugs* (PORTER *et al.*, 2019).

Toda vez que uma nova operação de entrada/saída é necessária, em vez de ser aberta uma nova *thread* ou processo, o Node irá deixar a tarefa em espera, realizando outras tarefas enquanto espera a resposta desta (PORTER *et al.*, 2019).

5.2.3.4 Express

O Express é um *framework* para o Node que é responsável pelas rotas da aplicação. Isso é possível pois o Express é construído em cima das requisições HTTP (PORTER *et al.*, 2019). O Express é chamado de *middleware* nas aplicações web. Esse *middleware* faz o gerenciamento de *cookies*, sessões, logins, parâmetros de URLs, *headers* das requisições e entre outras funcionalidades relacionadas às rotas (PORTER *et al.*, 2019).

Esse *framework* herda todas as propriedades do Node, como escalabilidade, facilidade, flexibilidade entre outras. Express é o *framework* mais famoso do Node (PORTER *et al.*, 2019). TJ Holowaychuk lançou o Express em 2010, mas hoje essa ferramenta é mantida pela Node Foundation e por desenvolvedores que contribuem para o código *open source* (PORTER *et al.*, 2019).

5.3 DESENVOLVIMENTO DA PROVA DE CONCEITO

O desenvolvimento dessa prova de conceito foi dividido em quatro etapas: (1) responsável pela aquisição de sinais do sistema embarcado, (2) responsável pelo envio dos dados ao Tangle, (3) gestão de usuários e viagem (*back-end*), (4) apresentação dos dados para o usuário (*back-end + front-end*) (Figura 24).

A prova de conceito foi hospedada no Heroku (<https://www.heroku.com/>), pois oferece este serviço de forma gratuita para aplicações NodeJS, contém IP público necessário para receber dados advindos de APIs da AYGA e IOTA. A prova de conceito também foi disponibilizada no Github: <https://github.com/wellingtonufsc/mestradoPPGTIC>.

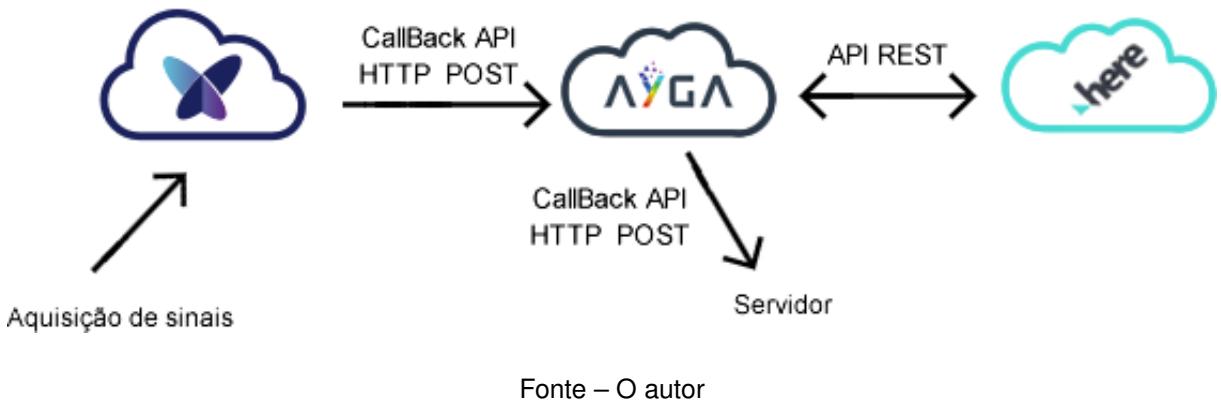
As etapas de desenvolvimento, configurações, e delineamento técnico são exploradas a seguir.

5.3.1 Aquisição de sinais

Para fins de execução desse projeto, optou-se pela aquisição de *MAC address* por meio do módulo e antena *Wi-fi* e dados de temperatura com WACS 2(WS2), conforme descrito na Seção 5.2.1.1. Após a compactação, os dados são inseridos em um pacote especial no módulo SigFox do WS2 e convertidos em ondas eletromagnéticas (antena), as quais são enviadas em uma frequência de aproximadamente 902 MHz e recebidos por uma base station SigFox. A Base Station transforma essas ondas de rádio em pacotes de dados para serem enviados via internet. Depois de convertido e verificadas as falhas, o pacote é enviado a SigFox Cloud pela internet. A nuvem Sigfox

envia os dados via HTTP POST para o servidor da empresa AYGA, e por fim, os dados são enviados à próxima etapa via HTTP POST para nosso servidor (Figura 29).

Figura 29 – Comunicação de dados



Fonte – O autor

Configurou-se a Nuvem da SigFox para o envio dos pacotes, utilizando a opção “*CallBack API*”. O *CallBack API* é um meio de comunicação unidirecional, ela encaminha as mensagens de forma automática. Assim que chegam à nuvem Sigfox os dados são enviados para uma *url*, que deve ser configurada para receber requisições HTTP. No caso dessa dissertação, configurou-se um endereço da Ayga.

Na Nuvem da Ayga, é possível configurar algumas variáveis de leitura do hardware WACS 2. Por exemplo, pode-se configurar quais sensores serão utilizados, o período e/ou o modo de leitura dos sensores.

A partir da Ayga, os MACs são enviados para a API da empresa Here, onde são feitas comparações e aproximações para descobrir a latitude e longitude do dispositivo. No entanto, dada a quantidade de dados que podem ser enviadas por um dispositivo Sigfox (12 bytes), isso acaba sendo um limitante. É possível enviar apenas 2 *MAC address* por mensagem.

Ressalta-se que a estimativa pode ser aprimorada utilizando RSSI (*Received Signal Strength Indicator*, ou em português, Indicador de Força do Sinal Recebido), no entanto, dada a quantidade limitada de dados por mensagem Sigfox e as características do projeto proposto, optou-se por não utilizar.

A Ayga encaminha os pacotes contendo o identificador do sistema embarcado, os dados de temperatura, localização (latitude e longitude) e *timestamp* da leitura. O pacote é enviado via *Callback* para o servidor responsável pela inserção desses dados no Tangle.

5.3.2 Envio dos dados ao IOTA/Tangle

Assim que os dados chegam ao servidor, um *back-end* escrito em NodeJS e Express, é responsável por criar e enviar o pacote de dados para o Tangle da forma

como chegaram. Para criar o pacote utilizou-se a biblioteca IOTA (Seção 2.2.8.4) e MAM client (Seção 2.2.8.5).

Os dados recebidos chegam em formato Json (Figura 30), onde se pode identificar o dispositivo de origem (*deviceUUID*), o tipo de sinal *temperature* (temperatura) ou *positionDOTS* (posição), além dos valores medidos.

Cada dispositivo é responsável por realizar medições de um único sistema de transporte, por exemplo, o baú de um caminhão, que é identificado com *deviceUUID*. Dessa maneira, cada placa identifica a “viagem” que foi realizada pelo sistema de transporte que contém determinado *deviceUUID*. À medida que o tempo passa, o dispositivo realiza novas medidas de temperaturas e localização.

Pelos motivos apresentados, o *back-end* realiza uma verificação do UUID, e os envia para o Tangle sem qualquer modificação. Ao chegar no servidor, os dados são encaminhados por uma rota do Express (Figura 31), essa rota repassa os dados para a função “attachToTangle”, que é responsável por enviar os dados ao Tangle.

A função “attachToTangle”, apresentada na Figura 32, recebe os dados e o “estado da IOTA”. O “estado da IOTA” representa as informações de um canal IOTA MAM, como, por exemplo, o “root do canal”. Se existir um estado, é necessário utilizá-lo, pois a viagem já foi iniciada, e são necessárias que todas essas informações fiquem no mesmo canal para que possam ser lidas mais tarde. Caso não seja passado um estado, quer dizer que é uma nova viagem, então é necessário inicializar um estado (*Mam.init()*). As informações de cada viagem sempre estão no respectivo canal. Em seguida os dados são convertidos para trytes (*asciiToTrytes()*) e criada uma mensagem IOTA (*Mam.create()*).

O estado da IOTA é salvo e em seguida os dados são enviados ao Tangle, passando como parâmetros o endereço da mensagem, o payload (conteúdo), o nível de segurança e a quantidade mínima de *proof-of-work* a ser realizada. Por fim, são retornadas as informações de confirmação (ou não) e o root da mensagem MAM, conforme apresentado Seção 2.2.7.

O código responsável pelo envio dos dados ao Tangle foi disponibilizado no Github e pode ser encontrado em:

<https://github.com/wellingtonufsc/mestradoPPGTIC/tree/master/servidorIOTA>

5.3.2.1 Backend da plataforma Web

O *back-end* tem a função de gerenciar usuários e receber e guardar os dados do canal MAM. Esses dados são armazenados em um serviço MongoDB e rodam em nodeJs.

Foram criadas três coleções dentro do MongoDB (Figura 33): a coleção “Configurations” não é obrigatória, serve apenas para armazenar duas variáveis do Tangle, o modo (“mam mode”) e o provedor (“mam provider”) que são configurados para guardar

Figura 30 – Dados de temperatura e localização recebidos da AYGA em formato Json

```
{  
    "deviceUUID": "00000074",  
    "signals": [  
        {  
            "UUID": "temperature",  
            "logs": [  
                {  
                    "date": "2021-04-10T08:58:25.000Z",  
                    "value": 25.6  
                },  
                {  
                    "date": "2021-04-10T09:08:20.000Z",  
                    "value": 15.6  
                },  
                {  
                    "date": "2021-04-10T09:18:45.000Z",  
                    "value": 12.6  
                }  
            ]  
        }  
    ]  
},  
{  
    "deviceUUID": "00000074",  
    "signals": [  
        {  
            "UUID": "positionDOTS",  
            "logs": [  
                {  
                    "date": "2021-04-10T08:48:31.000Z",  
                    "value": {  
                        "lat": -27.5752035,  
                        "lng": -48.61474951,  
                        "radius": 90  
                    }  
                },  
                {  
                    "date": "2021-04-10T08:58:21.000Z",  
                    "value": {  
                        "lat": -27.5952035,  
                        "lng": -48.31474951,  
                        "radius": 35  
                    }  
                },  
                {  
                    "date": "2021-04-10T09:08:58.000Z",  
                    "value": {  
                        "lat": -27.071245,  
                        "lng": -48.7141241,  
                        "radius": 8  
                    }  
                }  
            ]  
        }  
    ]  
}
```

Fonte – O autor

o ambiente de teste ou produção que é usado. A segunda tabela “users” guarda as informações das contas dos usuários do sistema, como o nome, e-mail, senha e tipo

Figura 31 – Encaminhamento para attachToTangle

```
info = await attachToTangle(body);
```

Fonte – O autor

Figura 32 – Função attachToTangle

```
119  async function attachToTangle(jsonData, mam_state = null) {
120    let config = await loadConfiguration();
121    let mamState;
122
123    if(!mam_state) {
124      mamState = Mam.init(config.mam_provider);
125      mamState = Mam.changeMode(mamState, config.mam_mode);
126    } else {
127      mamState = mam_state;
128    }
129
130    const trytes = asciiToTrytes(JSON.stringify(jsonData));
131    const message = Mam.create(mamState, trytes);
132
133    mamState = message.state;
134
135    let transactions = await Mam.attach(message.payload, message.address, 3, 14);
136
137    let info = {};
138    info.state = mamState;
139    info.root = message.root;
140
141    if (transactions.length == 0) {
142      throw new Error('erro ao salvar a transação no Tangle');
143    }
144
145    return info;
146  };

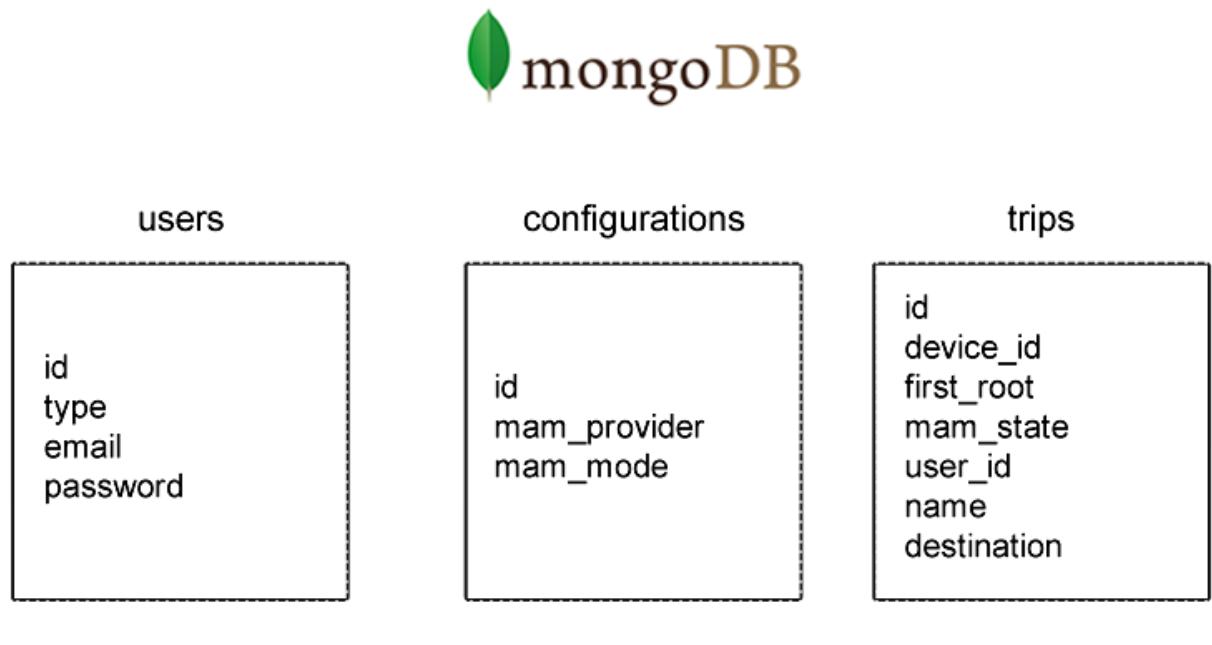
```

Fonte – O autor

(type). Os usuários podem ser “Distribuidores” ou “Consumidores”. A terceira coleção, “trips”, armazena as informações das viagens.

A terceira coleção merece mais atenção, dentro dela constam dois campos importantes: o “device id” e o “mam state”, com essas duas informações é possível vincular os sistemas embarcados com o estado da IOTA, que contém o canal, a segurança e o “first root” (id do canal MAM). Por fim, há os campos “user id”, “name” e “destination”, o primeiro representa o usuário que registrou a viagem, o segundo é só um campo para dar nome à viagem e o terceiro se refere ao trajeto.

Figura 33 – MongoDB - Coleções criadas



Fonte – O autor

O *back-end* da aplicação foi disponibilizado no Github e pode ser encontrado em:

<https://github.com/wellingtonufsc/mestradoPPGTIC/tree/master/appIOTA>

5.3.2.2 Front-end da plataforma Web

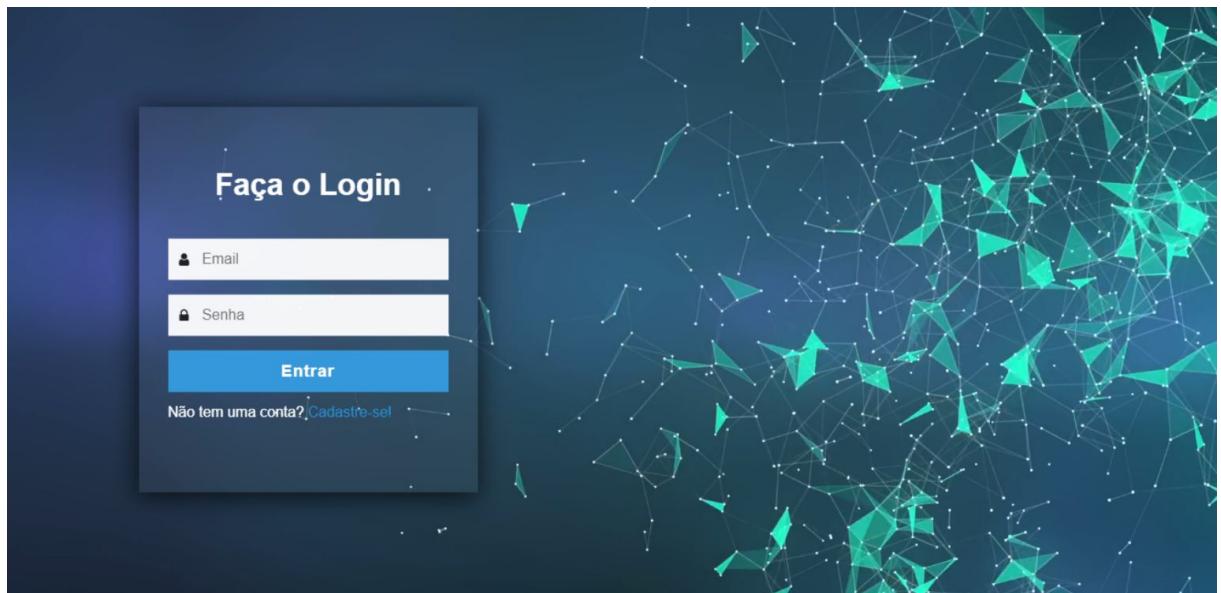
O *front-end* fornece ao usuário a possibilidade de registrar viagens, visualizar dados e *link* de verificação dos dados em *Fullnodes IOTA*. Essa parte do código foi escrita em React devido à facilidade de lidar com rotas de APIs e rápida aprendizagem, além de HTML e CSS, o que possibilitou criar layouts responsivos.

O sistema Web possui em sua interface inicial uma tela de login e senha (Figura 34), com a possibilidade de criar uma conta. Durante a criação de contas, é possível escolher entre dois tipos, distribuidor ou consumidor, a diferença entre as contas está na possibilidade de registrar uma nova viagem e/ou dispositivo, o distribuidor possui essa função nativa, enquanto o “consumidor” pode apenas visualizar os dados das viagens cadastradas por distribuidores.

Após o login, o usuário visualiza um *Dashboard*, que contém poucas informações além de um menu lateral (Figura 35), caba ressaltar que esse *layout* pode ser incrementado, no entanto, essa é apenas uma prova de conceito.

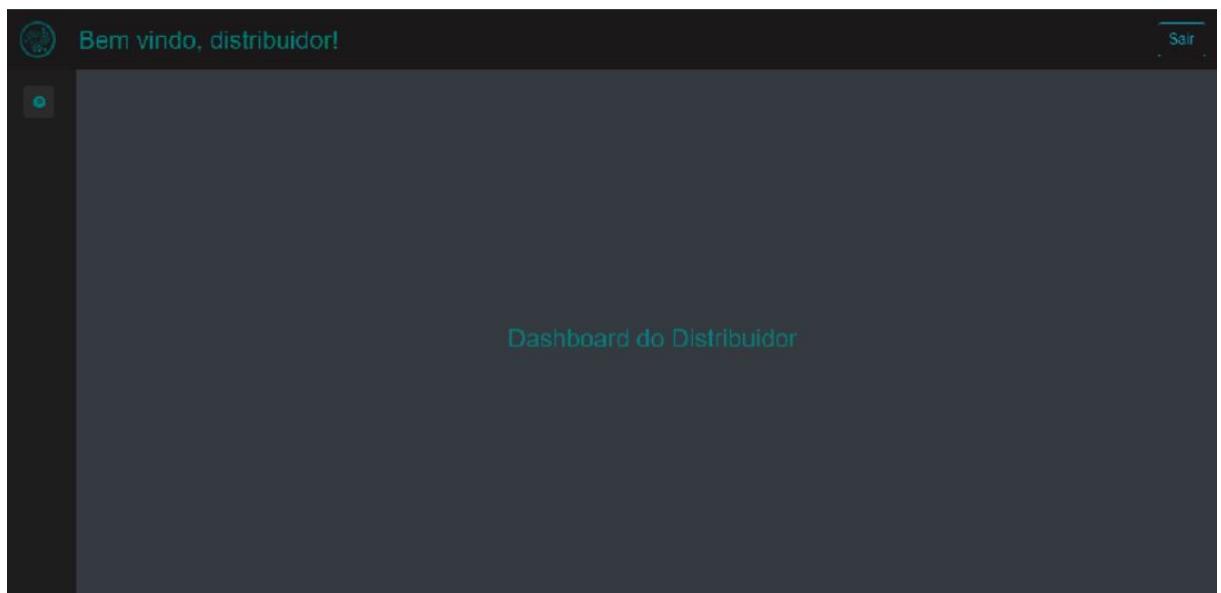
O menu permite ao usuário navegar entre as viagens cadastradas e/ou cadastrar uma nova viagem, no caso do distribuidor. A Figura 36) ilustra a tela de cadastro de

Figura 34 – Tela inicial - Login



Fonte – O autor

Figura 35 – Dashboard após o login



Fonte – O autor

viagem. Para cadastrar uma viagem é necessário inserir o ID da placa, o nome da viagem (normalmente o produto que está sendo transportado) e o trajeto da viagem.

Caso o distribuidor A, tenha interesse em registrar uma viagem que irá sair de Araranguá/SC para Florianópolis, transportando vacinas. Ele poderá registrar o nome

Figura 36 – Cadastro de viagem



Fonte – O autor

do produto como “Vacinas”, e o Trajeto como “Araranguá/SC → Florianópolis/SC”. Após o cadastro, as informações ficam disponibilizadas para os consumidores, ou seja, os clientes interessados em acompanhar o trajeto. O sistema retornará erro caso o distribuidor insira um identificador da placa que não existe, ou caso ainda não tenha sido identificada quaisquer tentativas de envio de dados.

Ao acessar a página de visualização de alguma viagem, é possível ver de forma gráfica os dados de temperatura e localização. Esses dados são obtidos diretamente do Tangle por meio de uma requisição para um *Fullnode* IOTA. A requisição do *front-end* é apresentada na Figura 37.

O código para requisitar dados do canal MAM apresentado na Figura 37, é iniciado por uma instância do MAM, utilizando o `Mam.init()`, depois é utilizado o método `fetch()`, com o id do canal (first root), que permitirá identificar todas as mensagens do canal. Seguindo o código apresentado na Figura 37, as mensagens são convertidas de trytes para bytes e apresentadas no *front-end* em formato gráfico.

A página de visualização da viagem é apresentada na Figura 38 e Figura 39, respectivamente temperatura e localização. Os dados de temperatura são apresentados em um gráfico temporal, onde o eixo x representa o tempo e o eixo y o valor de temperatura registrado. A localização é apresentada em pontos de um mapa, o primeiro ponto registrado para a viagem é identificado em vermelho e o último em verde.

Para manter a visualização dos dados atualizando constantemente, o id do canal é utilizado pelo *front-end* em um *listener* (ouvinte, em português), dessa forma

Figura 37 – Requisição de dados de um canal MAM para um IOTA Fullnode

```
Mam.init(config.mam_provider);

async function addListenerMam() {
    const result = await Mam.fetch(product.first_root, config.mam_mode);

    let msgs = [];

    if (result && result.messages) {
        result.messages.forEach(message => {
            const msg = JSON.parse(trytesToAscii(message));
            msgs.push(msg);
        });
    }

    setMessage(Object.assign({}, msgs));
}

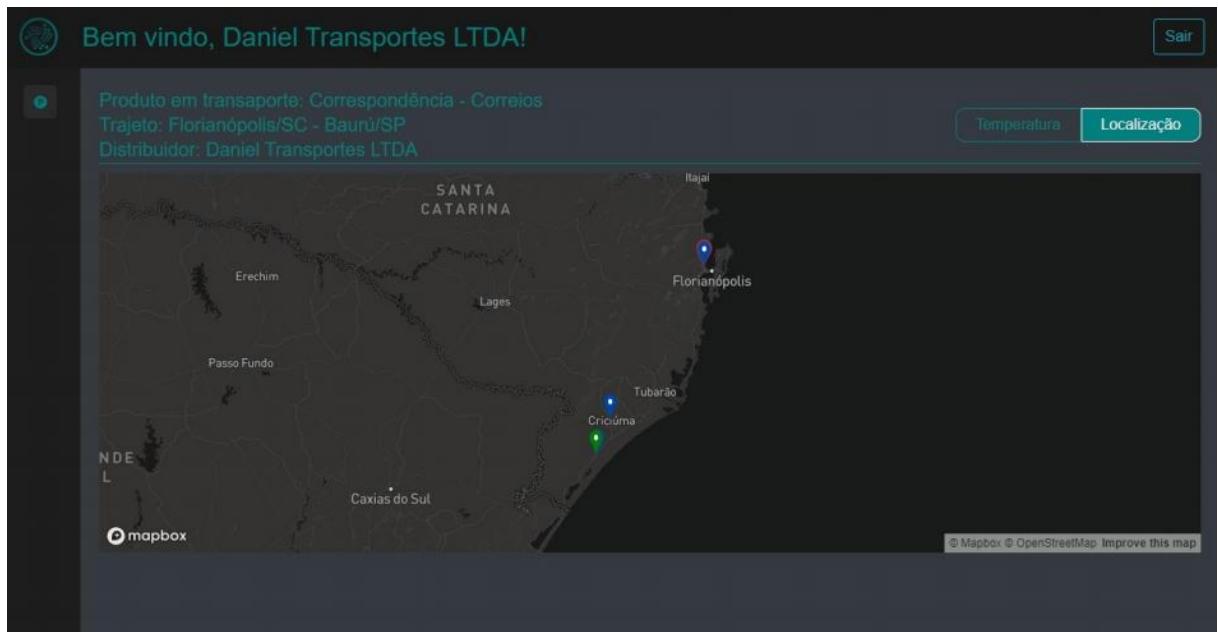
addListenerMam();
interval = setInterval(addListenerMam, 30000);
```

Fonte – O autor

Figura 38 – Visualização da viagem: temperatura das cargas



Figura 39 – Visualização da viagem: localização das cargas



Fonte – O autor

os dados são disponibilizados para o usuário, em forma gráfica assim que publicados no Tangle.

Além disso a partir do front-end é possível validar as medidas obtidas. Foi adicionada a visualização de dados o botão “comprove”, ele permite verificar rapidamente os dados em um *Fullnode* público da IOTA, com uma interface amigável conhecido como MAM explorer.

O front-end da aplicação foi disponibilizado no Github e pode ser encontrado em:

<https://github.com/wellingtonufsc/mestradoPPGTIC/tree/master/appiotafront>

6 DELINEAMENTO EXPERIMENTAL

Dadas as justificativas para a escolha do dispositivo de hardware proposto, LPWAN e tecnologia de registro distribuído, verifica-se a necessidade de realizar testes que contribuam para um melhor entendimento das potencialidades e limitações do ecossistema proposto.

6.0.1 Precisão da geolocalização com MAC address de redes Wi-fi

Pretende-se avaliar a viabilidade da obtenção de localização utilizando *MAC address* de redes *Wi-fi* com o dispositivo Ayga WS-2 e API da Here.

6.0.1.1 Ambiente de pesquisa

Segundo testes e resultados apresentados por Borges (2019), a única antena Sigfox instalada em Araranguá — Santa Catarina — Brasil, está localizada na Universidade Federal de Santa Catarina, na Unidade do bairro Mato Alto, e devido ao modo como foi instalada, possui área de cobertura de pelo menos 3 km (BORGES *et al.*, 2019). Por este motivo, parte dos testes estáticos com o dispositivo ocorrem nesse espaço delimitado, conforme Figura 40. Assim, os dados de geolocalização são de lugares conhecidos, e com cobertura de rede garantida em perímetro urbano, ou seja, com muitas redes *Wi-fi*.

Todos os testes com o dispositivo são realizados dentro de um automóvel, com o dispositivo Ayga WS-2 fixo no painel.

6.0.1.2 Coleta de dados

Vinte medições são realizadas durante duzentos minutos, ou seja, uma mensagem a cada dez minutos, em 20 locais diferentes, dentro da área de cobertura apresentada na Seção 6.0.1.1.

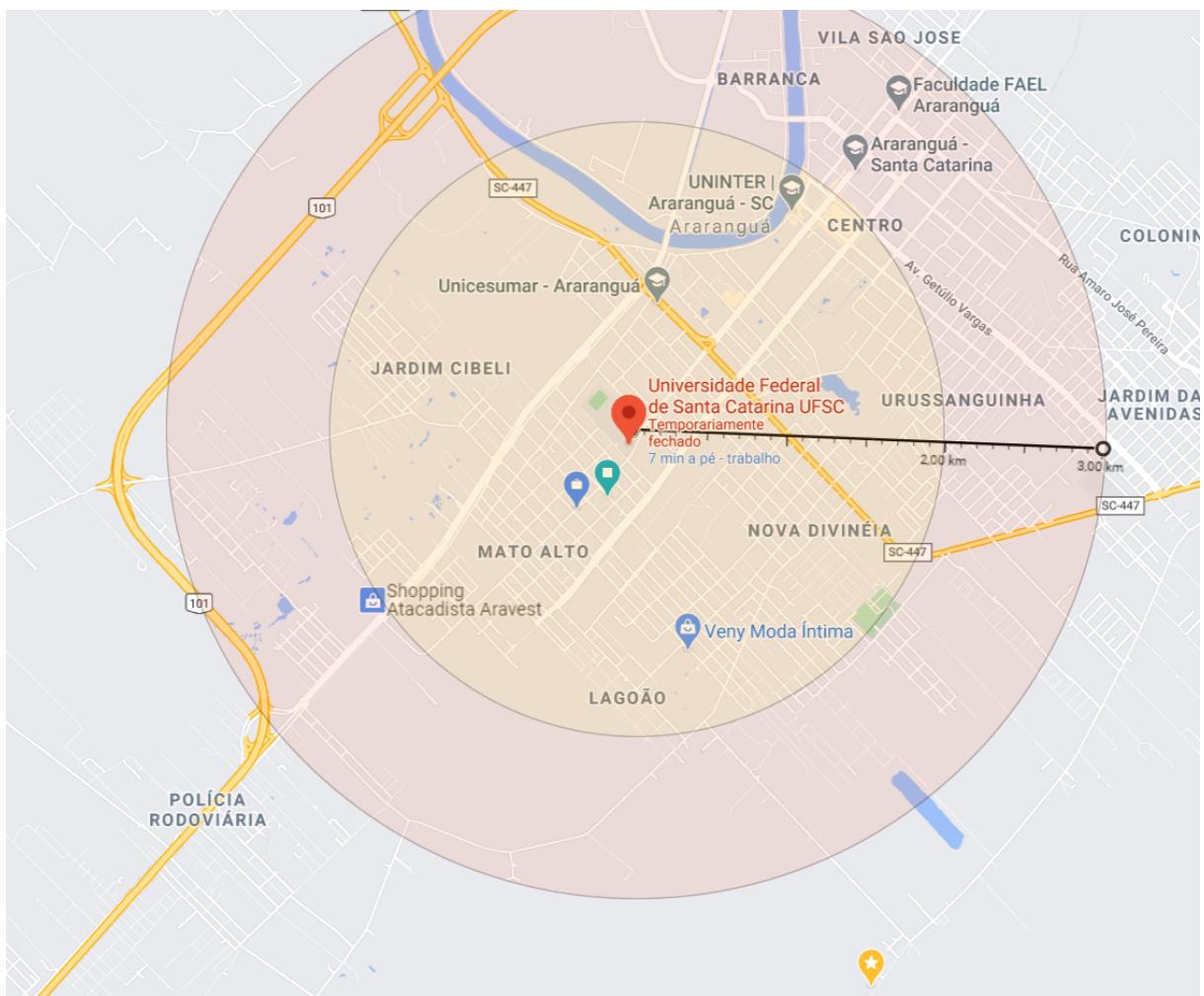
O dispositivo é configurado para obter dois MACs antes de enviar os dados para a rede, esse processo ocorre por um período de 5 segundos. Caso encontre apenas um sinal, deve enviá-lo e este será considerado sua localização. Caso contrário, uma localização é estimada levando em consideração os dois MACs enviados.

Tabela 8 – Validação experimental Geolocalização - MAC address e API Here

id	Medição	Período	Local	Pacotes de mensagem	Tempo total	Dado
1	Estática	10 min.	Figura 40	20	200 min.	2 MAC Address (Geolocalização)

Os resultados são apresentados na Seção 7.1.

Figura 40 – Área de cobertura para testes estáticos



Fonte – O autor, baseado no trabalho de Borges (2019)

6.0.2 Perda de pacotes Sigfox em movimento

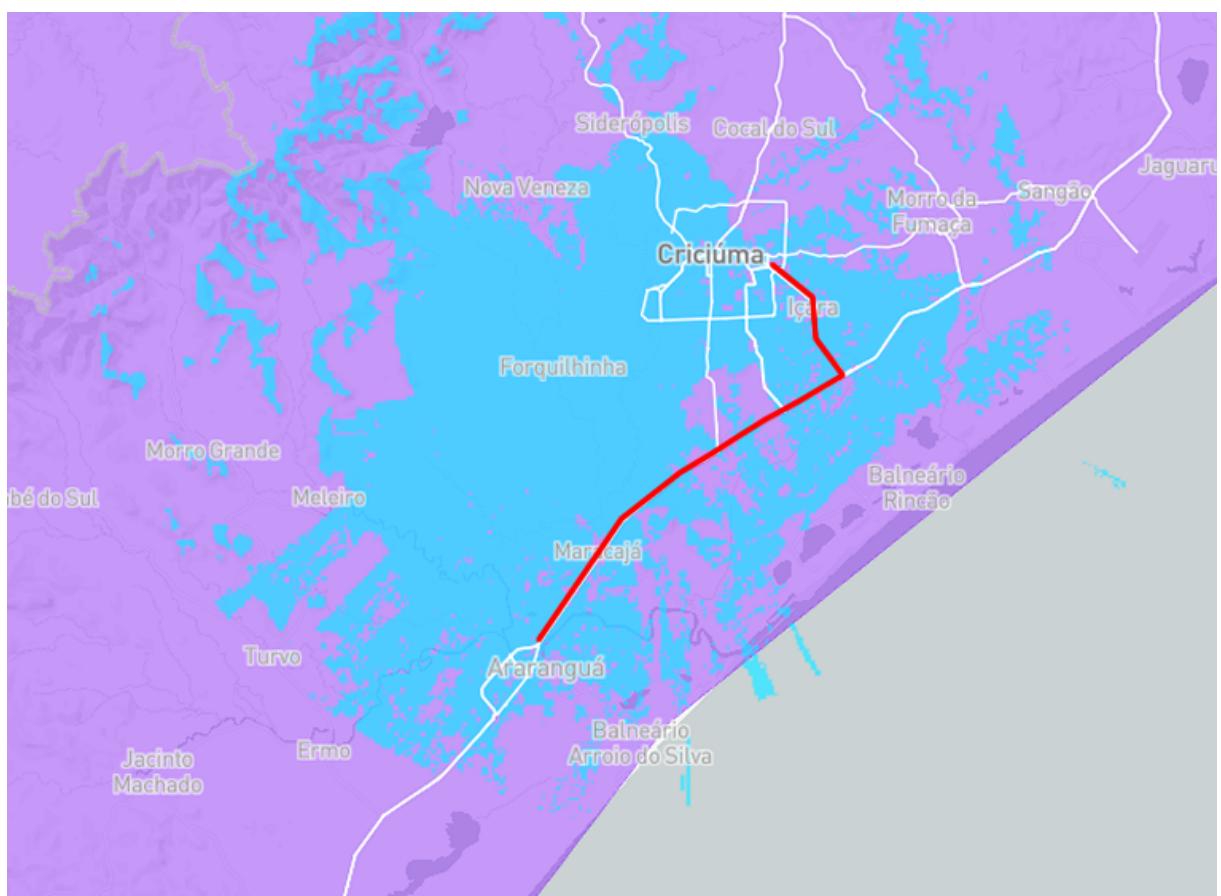
Como a rede Sigfox limita a quantidade de envios, existe uma preocupação com a quantidade de pacotes de mensagens perdidos. Os pacotes perdidos, com frequência, referem-se a mensagens que saíram do dispositivo e não encontraram uma antena Sigfox, ou ainda chegaram com muito ruído ou pouca intensidade. Na literatura, a perda de pacotes por movimento é pouco estudada, na verdade não foram encontrados trabalhos científicos que relacionem Sigfox com perda de pacotes por velocidade. Disk91 (2017) produziu um texto online, segundo seus resultados existem perdas substanciais em situações de alta velocidade. Isto foi verificado realizando testes estáticos dentro de uma área de cobertura e posteriormente, verificações experimentais em movimento (BDISK91, 2017).

6.0.2.1 Ambiente de pesquisa

Os dados de cobertura apresentados pelo site da Sigfox (SIGFOX, 2021) apresentam uma grande área de cobertura entre a cidade de Criciúma/SC e Araranguá/SC (Figura 41). Essa área é importante para realização de testes em movimento, especialmente por contar com uma rodovia de alta velocidade.

A experimentação é, portanto, executada dentro da área de cobertura apresentada na Figura 41. Os dados serão enviados em distâncias regulares de 1km quando parado e 2km quando em movimento, buscando obter de maior quantidade de amostras. Os testes em movimento ocorreram a 90 km/h, para posteriormente compará-los com envios estáticos (0km/h). A velocidade escolhida é justificada pois trata-se de uma velocidade usual das rodovias executadas por veículos de transporte de cargas.

Figura 41 – Área de cobertura para testes dinâmicos



Fonte – O autor, baseado em Sigfox (2021)

A linha vermelha da Figura 41 apresenta o trajeto utilizado para realização dos testes, pois são rodovias de alta velocidade e trajeto comum para trânsito de caminhões e outros veículos de carga.

6.0.2.2 Metodologia de coleta de dados

Optou-se por utilizar o acelerômetro do dispositivo, pois permite envio imediato de dados do dispositivo pela ação do pesquisador. Nesse caso, o envio do dado é realizado girando o dispositivo 180º em menos de 0,5s. Para realizar esse experimento foi necessário também configurar a sensibilidade do acelerômetro para 1,094g, com taxa de dados de 50 Hz, buscando com isso, não realizar medições involuntárias e ao mesmo tempo, tornar a identificação do movimento de fácil medida.

Para validar as experimentações em movimento, são realizadas três experimentações, buscando restringir as influências do local exato da medição e aumentar a quantidade de amostras. A Tabela 9 sintetiza o método experimental realizado.

Tabela 9 – Validação experimental - perda de pacotes de mensagem

id	Medição	Intervalo	Local	Velocidade	Sensor
2	Estático	1 km	Figura 41	0 km/h	Acelerômetro
3	Dinâmica	2 km	Figura 41	90 km/h	Acelerômetro
4	Dinâmica	2 km	Figura 41	90 km/h	Acelerômetro
5	Dinâmica	2 km	Figura 41	90 km/h	Acelerômetro

Os resultados são apresentados na Seção 7.2.

6.0.3 Latência do sistema

Pode-se identificar também a viabilidade da aplicação mensurando a latência do sistema como um todo. Nesse caso, é obtido a latência entre o envio de dados do dispositivo até a inserção destes no Tangle. Ou seja, a latência é entendida como: o tempo que um dado é registrado pelo sistema embarcado, isto é, o processo de encaminhamento para Sigfox, passagem pela Ayga, envio para Here, retorno para Ayga, encaminhamento para o servidor e registro no Tangle.

6.0.3.1 Ambiente de pesquisa

As medições do dispositivo WS2 são realizadas em perímetro urbano, com garantia de cobertura Sigfox, apresentado na Figura 40, com medições estáticas há aproximadamente 500m da antena Sigfox. O servidor que receberá os dados está hospedado no Heroku (<https://herokuapp.com>). Para estes testes, realiza-se envios para a rede IOTA Mainnet, que é a rede principal da IOTA.

6.0.3.2 Metodologia de coleta de dados

Serão enviados *MAC address* em intervalos regulares de 10 minutos por um período de 24 horas, ou seja, 144 mensagens Sigfox. Os dados serão comparados por meio do *timestamp* do disparo e o *timestamp* de registro no Tangle. Sabe-se, com

base na literatura que o tamanho da mensagem (*payload*) é quase irrelevante para a latência na IOTA (BROGAN *et al.*, 2018), por este motivo optou-se por realizar teste com apenas um formato de arquivo. Optou-se pelo *MAC address* pois o dado passa também pela API da Here, dessa forma conseguir-se-á avaliar melhor a latência do ecossistema experimental desenvolvido.

A Tabela 10 sintetiza o experimento descrito nesta sessão.

Tabela 10 – Validação experimental - perda de pacotes de mensagem

id	Medição	Período	Local	Pacotes de mensagem	Tempo total	Dados por mensagem
6	Estática	10 min.	Figura 40	144	24h	2 MAC Address

Os resultados são apresentados na Seção 7.3.

6.0.4 Validação da prova de conceito - Viagem

A prova de conceito com todos os componentes do sistema proposto, foi avaliada realizando dois percursos diferentes. Os experimentos têm por objetivo verificar a transmissão dos dados em movimento para o Tangle e o funcionamento do ecossistema.

6.0.4.1 Ambiente de pesquisa

Para realizar esses testes, o sistema embarcado foi enviado pelos correios a partir da cidade de Araranguá/SC até a cidade de Bauru(Figura 42), em São Paulo e posteriormente foram realizadas medições ao redor dentro do estado de São Paulo, Baurú - Araçatuba - São José do Rio Preto (Figura 43).

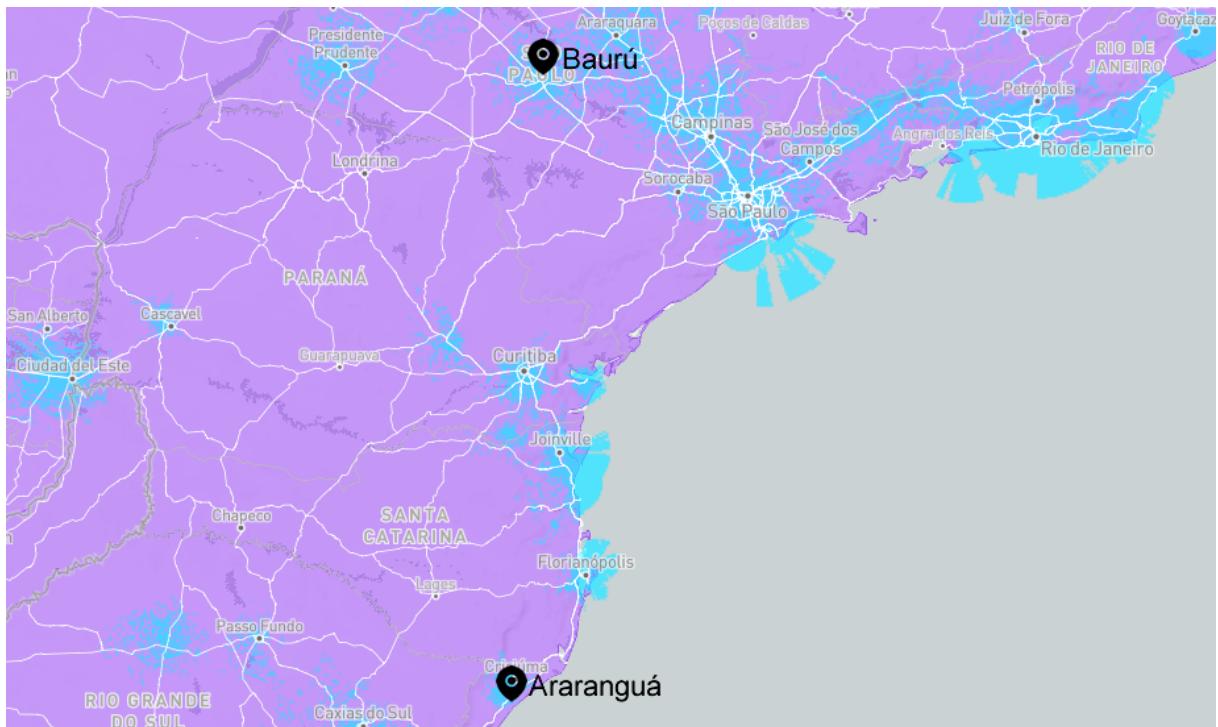
O dispositivo é despachado nos Correios, dentro de uma caixa de papelão, porém não se sabe ao certo a quantidade e volume de outras postagens que são enviadas junto em ele. O segundo percurso, Baurú - Araçatuba - São José do Rio Preto, o dispositivo de hardware foi posicionado em cima do painel de um veículo, passando por cidades com cobertura Sigfox, onde são realizadas entregas.

6.0.4.2 Metodologia de coleta de dados

A coleta de dados desse experimento requer proximidade com uma aplicação real. Optamos por realizar coletas de dados a cada 10 minutos de temperatura e localização.

A motivação da escolha está diretamente relacionada com os pacotes de dados Sigfox. Um dispositivo Sigfox possui planos de conectividade de até 144 mensagens por dia, o que implica em uma mensagem a cada 10 minutos, no máximo. No entanto, no decorrer da pesquisa, identificamos que ao comprar pacotes de dados para vários

Figura 42 – Área de cobertura Sigfox entre Araranguá/SC - Baurú/SP



Fonte – O autor, baseado em Sigfox (2021)

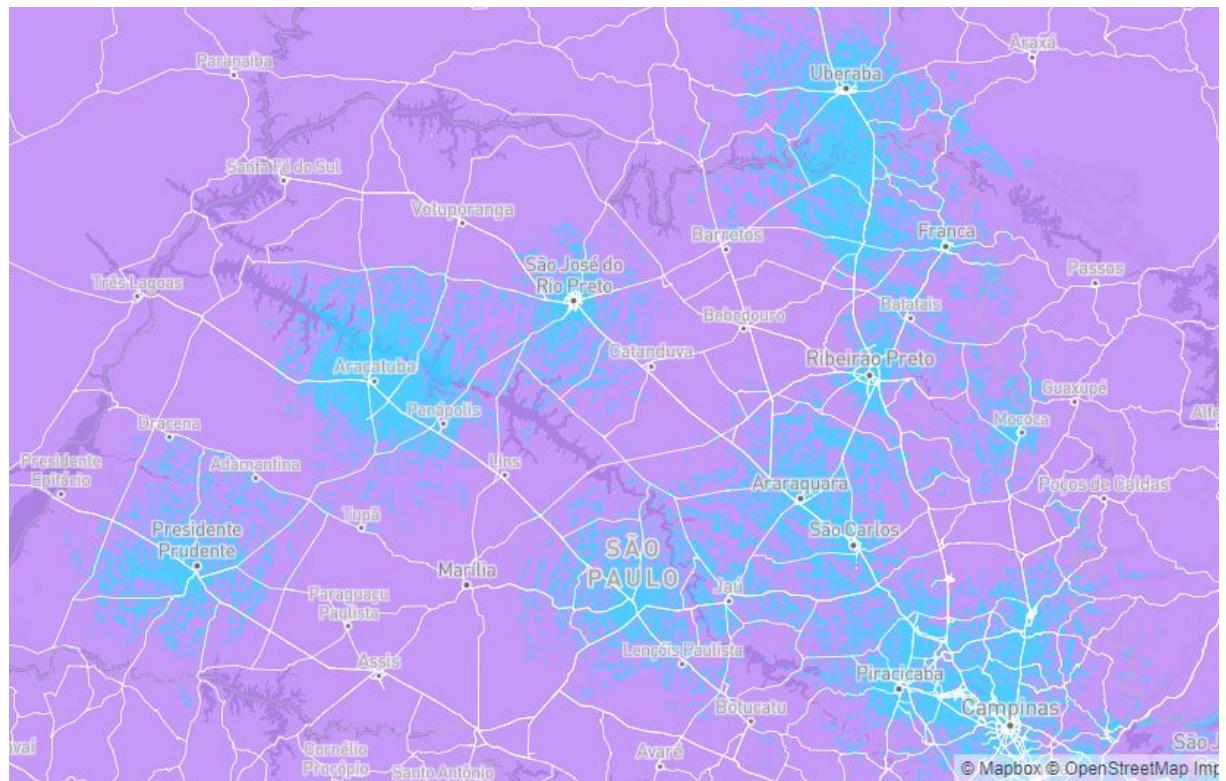
dispositivos com a mesma conta, a empresa Sigfox permite extrapolar o uso de 144 mensagens por dia por dispositivo, pois nesse caso um determinado dispositivo utiliza o pacote não utilizado de outros da mesma conta. Além disso, a limitação de 12 bytes por mensagem, limita a quantidade de dados que podem ser enviados pelo WS2. Cada pacote Sigfox pode enviar apenas 2 *MAC address* ou até 6 temperaturas por mensagens. Isso permitiu que optássemos por realizar medidas de temperatura a cada 10 minutos e 2 *MAC address* também a cada 10 minutos. A Tabela 11 sintetiza as experimentações descritas nesta sessão.

Tabela 11 – Validação experimental - perda de pacotes de mensagem

id Medição	Viagem	Período	Local	Tipo de dado
7	Dinâmica Araranguá/SC-> Baurú/SP	10 min.	Figura 42	temperatura e 2 MAC Address
8	Dinâmica Baurú - Araçatuba - São José do Rio Preto/SP	10 min.	Figura 43	temperatura e 2 MAC Address

Além de temperatura e *MAC address*, a empresa Ayga possui uma rotina para receber a diferença de potencial da bateria do dispositivo. A rotina deverá ser utilizada

Figura 43 – Área de cobertura Sigfox Araçatuba/SP e região



Fonte – O autor, baseado em Sigfox (2021)

para coleta de dados durante todos os dois percursos experimentais.

Os resultados são apresentados na Seção 7.4.

7 RESULTADOS E DISCUSSÕES

Essa sessão irá apresentar e discutir os resultados das experimentações do ecossistema proposto, bem como discutir outros pontos que não receberam experimentações, mas que, no entanto, são frutos da pesquisa. Tais como a segurança, custos e consumo de bateria.

Todas as experimentações ocorreram entre os dias 04/01/2021 e 13/04/2021. A data exata de cada experimento é descrita em sua respectiva sessão, quando pertinente.

7.1 GEOLOCALIZAÇÃO

As coletas de dados de geolocalização utilizando triangulação de sinais com o dispositivo WS-2(Seção 5.2.1) foram realizadas, conforme descrito na sessão 5.6.1. Os resultados são comparados com GPS celular e apresentados na Tabela 12.

Os pontos de latitude e longitude da Tabela 12 foram plotados em um mapa (Figura 44), destacando a identificação de *MAC address* (em verde) ou ausência de *MAC address* conhecido (em vermelho).

A Figura 44 evidencia quinze locais onde foi possível identificar a localização utilizando triangulação de sinais de rede *Wi-fi* e cinco pontos onde não foram encontradas redes ou *MAC address* conhecidos. É importante observar que a maioria dos pontos em vermelho são áreas com pouco comércio e prédios, esses fatos desfavorecem a identificação de roteadores, portanto inviabilizaram a geolocalização nesses cinco pontos.

Para os objetivos deste trabalho a exatidão determinística das medidas de localização é pouco relevante, ou seja, uma aproximação dentro de um raio de centenas de metros, foi definida internamente como suficiente. Apesar disso, identificar com clareza os limites da proposta favorece o entendimento do escopo do projeto e potencializa olhares para além do que foi imaginado. A exatidão das medidas de latitude e longitude em relação ao GPS, são apresentadas na Figura 45.

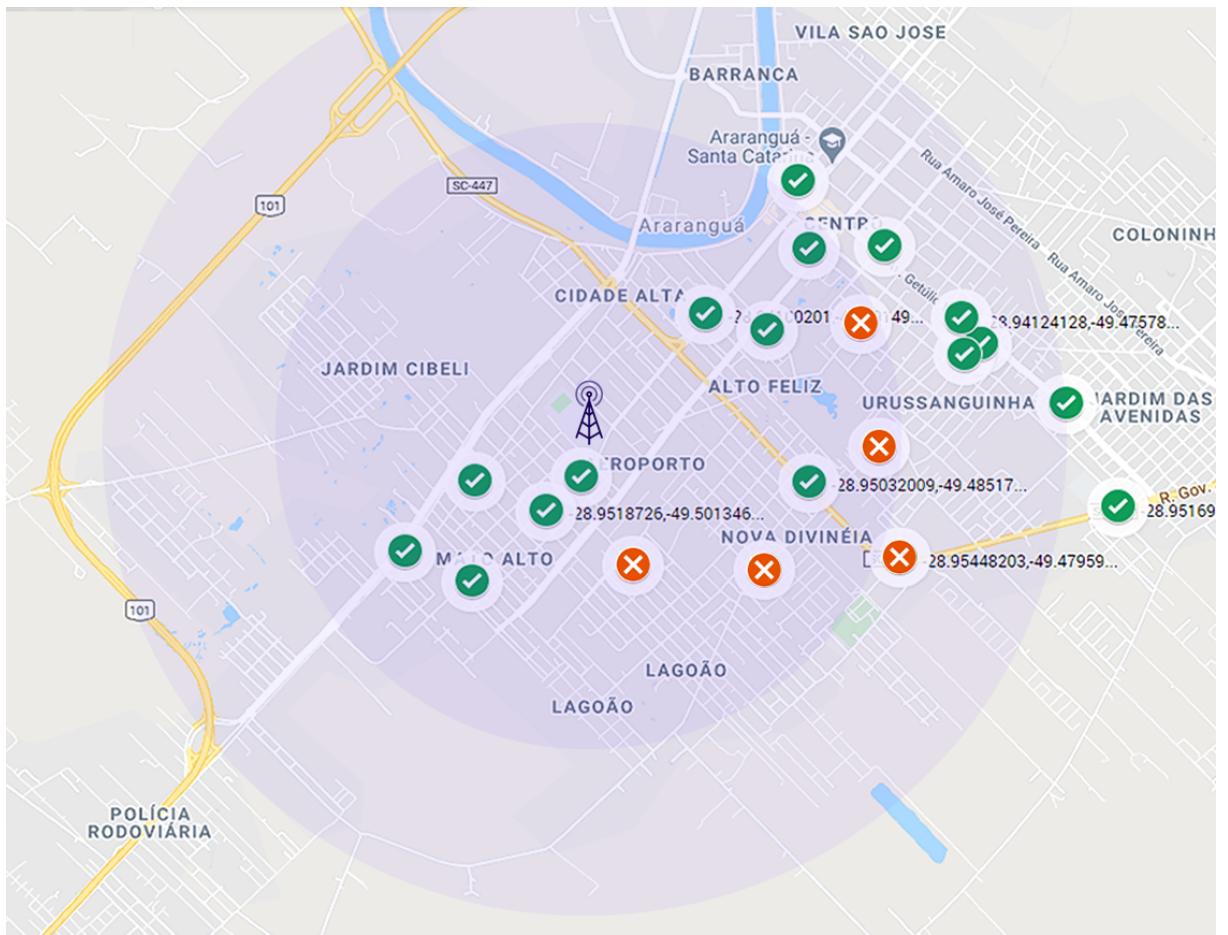
A Figura 45 torna mais evidente a faixa de precisão das medidas realizadas. É possível observar que, com a exclusão de um ponto, a maior parte das medidas estão dentro de uma margem de aproximadamente 100m de erro em relação à latitude e longitude do GPS. A Mediana também foi calculada para evidenciar a precisão das medidas, ela corresponde ao elemento central dentro do qual existem 50% das observações, nesse caso 24,50m. Uma medida que ajuda a entender a dispersão dos dados é o desvio padrão(σ), que indica o quanto o conjunto de dados é uniforme, ou ainda o quanto os dados estão dispersos sobre a média (33,37m).

$$\sigma = \sqrt{\sum \frac{(x_i - \bar{x})^2}{n}} \text{ onde,}$$

Tabela 12 – Resultados experimentais: Geolocalização MAC address Wi-fi

id GPS (Lat, Lon)	Triangulação de sinais Wi-fi (Lat, Lon)	Diferença (rad)	Exatidão (m)
1 -28.95002028, -49.49918242	-28.94999840, -49.49913795	-0.00002189, -0.00004447	2.43, 4.94
2 -28.9518726, -49.50134672	-28.9520064, -49.50156096	0.00013380, 0.00021424	14.87, 23.81
3 -28.95579686, -49.50582028	-28.9558088, -49.50604707	0.00001194, 0.00022679	1.33, 25.20
4 -28.95417199, -49.50996797	-28.9541551, -49.51005777	-0.00001689, 0.00008980	1.88, 9.98
5 -28.95028205, -49.50567613	-28.9499606, -49.50568979	-0.0003214, 0.00001366	35.72, 1.52
6 -28.95514484, -49.48787231	NaN	NaN	NaN
7 -28.94833944, -49.48091688	NaN	NaN	NaN
8 -28.94266136, -49.47462736	NaN	NaN	NaN
9 -28.94600511, -49.46941525	-28.9457291, -49.47016019	-0.00027601, 0.00074494	30.67, 82.78
10 -28.94124128, -49.47578198	-28.9407946, -49.47651905	-0.00044668, 0.00073707	49.64, 81.90
11 -28.93722555, -49.48050789	-28.9372525, -49.48067922	0.00002695, 0.00017133	2.99, 19.04
12 -28.93363847, -49.48583507	-28.933537, 49.48552433	-0.00010147, -0.00031074	11.28, 34.53
13 -28.937379, 49.48515939	-28.9376636, -49.48488333	0.00028460, -0.00027606	31.62, 30.68
14 -28.94188746, -49.48770414	-28.9410771, -49.48705257	-0.00081036, -0.00065157	90.05, 72.40
15 -28.94156639, -49.48195256	NaN	NaN	NaN
16 -28.94326438, -49.4756373	-28.9434336, -49.47514442	0.00016922, -0.00049288	18.80, 54.77
17 -28.95169659, -49.4661598	-28.9514848, -49.46478349	-0.00021179, -0.00137631	23.53, 152.94
18 -28.95448203, -49.47959389	NaN	NaN	NaN
19 -28.95032009, -49.48517056	-28.9510733, -49.48464984	0.00075321, -0.00052072	83.70, 57.86
20 -28.94100201, -49.49149896	-28.94099010, -49.49135786	-0.00001191, -0.00014110	1.32, 15.68

Figura 44 – Resultados experimentais de Geolocalização: Triangulação de sinal Wi-fi



Em verde, locais onde existem sinais de *Wi-fi* conhecidos; em vermelho, locais sem sinal de rede *Wi-fi* ou roteadores desconhecidos.

x_i : valor na posição i no conjunto de dados

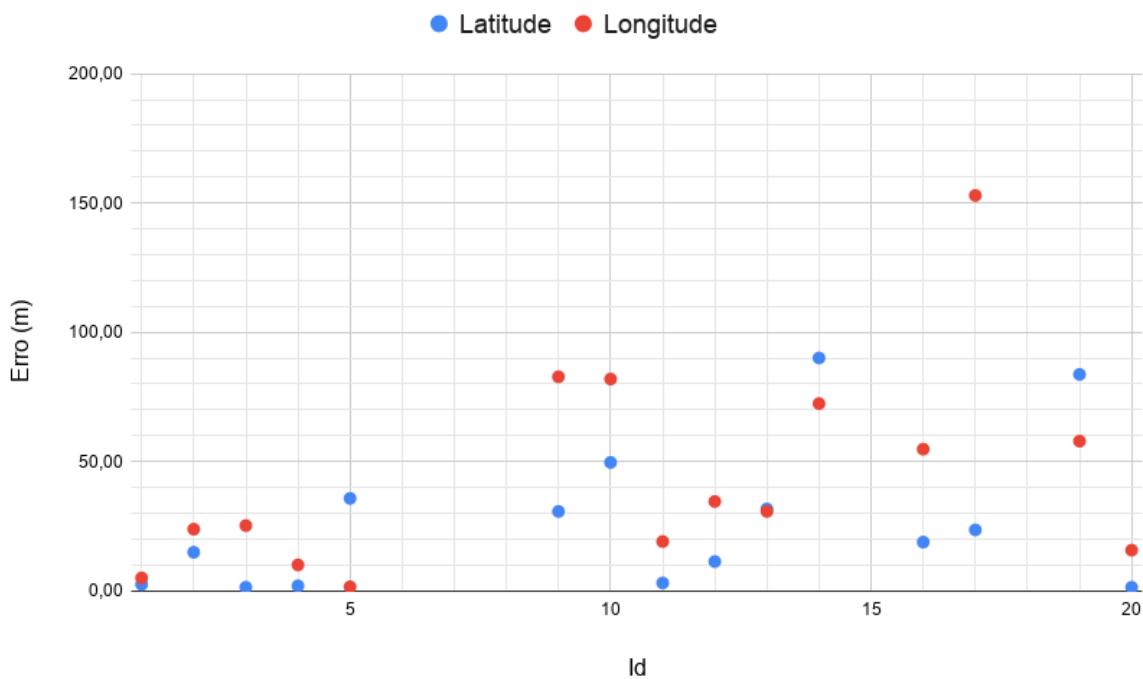
\bar{x} : média aritmética dos dados

n = quantidade de dados

Para o caso dos erros na precisão da localização, o desvio padrão(σ) é 35,56m. Constatase que, à exceção de seis pontos de maior imprecisão, todos os outros dados estão dentro do desvio padrão.

Portanto, para o escopo dessa dissertação a utilização de redes *Wi-fi* utilizando o dispositivo WS-2 e API da HERE para obter geolocalização, utilizando apenas 2 *MAC address* pode ser considerada validada, principalmente por considerarmos que o trajeto de um sistema de transporte, passará quase necessariamente por áreas urbanas, com prováveis *MAC address* conhecidos e com precisão de localização esperada em torno de 24,5m. Cabe ressaltar que a precisão pode e deve aumentar substancialmente ao adicionar a captura e envio de mais *MAC address* e a intensidade do sinal recebido

Figura 45 – Precisão das medidas de Latitude e Longitude



Fonte – O autor

(do inglês, *Received signal strength indication - RSSI*) das antenas. Contudo, não é utilizada nessa dissertação visando a economia de pacotes de mensagens Sigfox.

7.2 PERDA DE PACOTES SIGFOX EM MOVIMENTO

Seguindo a metodologia descrita na Seção 6.0.2, identificou-se primeiramente o comportamento da rede Sigfox na região apresentada na Figura 41. A cada 1km do percurso de 36km realizou-se o envio de sinais Sigfox. Os dados estão registrados na Tabela 13.

O percurso avaliado, registra duas *Base Stations* Sigfox, com o identificador 7705 e 766B. O RSSI cai de -65 dB para -127 dB ao longo do percurso. Segundo dados obtidos no *Sigfox Cloud*, -65db é considerado um sinal bom, enquanto -127 dB o limite de captação. O percurso é de 36 km, portanto, não foram identificados 5 sinais. Porém durante a prática experimental não foi possível realizar 3 medições ao longo do percurso. Sendo assim, o percurso apresentado na Figura 41 possui cobertura Sigfox validada por esse teste. Ressalta-se, no entanto, 6 pontos com baixa cobertura, identificados na Tabela 13 como qualidade do sinal “Limite”.

Com o automóvel em movimento e medidas em intervalos de 2 km, esperava-se o registro de 18 dados. Houve dificuldade de medição em 3 locais, totalizando 15 envios

Tabela 13 – Testes estáticos: Intensidade de sinal Sigfox entre Araranguá e Criciúma

id	Qualidade do sinal	RSSI 1	Base Station 1	RSSI 2	Base Station 2
1	Limite	-130.00	766B	NaN	NaN
2	Médio	-119.00	766B	NaN	NaN
3	Limite	-133.00	7705	NaN	NaN
4	Limite	-116.00	7705	NaN	NaN
5	Médio	-123.00	766B	NaN	NaN
6	Médio	-124.00	766B	NaN	NaN
7	Médio	-126.00	766B	NaN	NaN
8	Médio	-115.00	766B	NaN	NaN
9	Bom	-113.00	766B	NaN	NaN
10	Limite	-131.00	7705	NaN	NaN
11	Médio	-125.00	7705	NaN	NaN
12	Médio	-123.00	7705	NaN	NaN
13	Bom	-112.00	7705	NaN	NaN
14	Médio	-109.00	7705	NaN	NaN
15	Limite	-127.00	7705	NaN	NaN
16	Médio	-116.00	7705	-130.00	766B
17	Médio	-119.00	7705	NaN	NaN
18	Médio	-121.00	7705	NaN	NaN
19	Bom	-113.00	7705	-131.00	766B
20	Bom	-105.00	7705	NaN	NaN
21	Bom	-96.00	7705	-126.00	766B
22	Limite	-131.00	766B	NaN	NaN
23	Bom	-130.00	766B	-109.00	7705
24	Bom	-112.00	7705	-129.00	766B
25	Bom	-106.00	7705	NaN	NaN
26	Bom	-101.00	7705	NaN	NaN
27	Bom	-73.00	7705	NaN	NaN
28	Bom	-68.00	7705	-136.00	766B
29	Bom	-65.00	7705	NaN	NaN
30	Bom	-65.00	7705	-139.00	766B
31	Bom	-78.00	7705	NaN	NaN

por experimentação. Os dados foram exportados do *Sigfox Cloud* e apresentados na Tabela 14.

Foram 34 mensagens Sigfox recebidas e 11 envios perdidos (aproximadamente 24% das medidas) que certamente não encontraram uma *Base Station* Sigfox. Portanto, existe uma perda significativa dos sinais Sigfox movimentando-se a 90 km/h. A perda de sinais em movimento foi estudada também por Disk91 (2017), com resultados similares. Esse autor relaciona a perda de mensagens com mudança de fase do sinal em conjunto com a modulação Sigfox baseada em BPSK.

7.3 LATÊNCIA

A latência do ecossistema apresentado na Seção 5.1 - Figura 26, foi medida conforme descrito na Seção 6.0.3. Como as tecnologias utilizadas nesta dissertação estão em constante desenvolvimento, ressalta-se que os dados foram registrados no dia 06/02/2020.

Tabela 14 – Testes dinâmicos: Intensidade de sinal Sigfox entre Araranguá e Criciúma

Experimento	Medida	Qualidade do sinal	RSSI 1	Base Station 1	RSSI 2	Base Station 2
Experimento 1	1	Médio	-106.00	766B	NaN	NaN
	2	Médio	-111.00	766B	NaN	NaN
	3	Limite	-130.00	7705	NaN	NaN
	4	Bom	-116.00	7705	NaN	NaN
	5	Limite	-115.00	7705	NaN	NaN
	6	Limite	-131.00	766B	NaN	NaN
	7	Bom	-103.00	7705	-116.00	766B
	8	Bom	-102.00	7705	NaN	NaN
	9	Bom	-89.00	7705	NaN	NaN
	10	Bom	-92.00	7705	NaN	NaN
	11	Bom	-78.00	7705	NaN	NaN
Experimento 2	1	Médio	-113.00	766B	NaN	NaN
	2	Médio	-105.00	766B	NaN	NaN
	3	Limite	-129.00	7705	NaN	NaN
	4	Bom	-106.00	7705	NaN	NaN
	5	Limite	-135.00	7705	NaN	NaN
	6	Médio	-119.00	766B	-109.00	766B
	7	Médio	-118.00	7705	-130.00	766B
	8	Bom	-100.00	7705	NaN	NaN
	9	Bom	-79.00	7705	NaN	NaN
	10	Bom	-88.00	7705	NaN	NaN
	11	Bom	-74.00	7705	NaN	NaN
	12	Bom	-68.00	7705	NaN	NaN
Experimento 3	1	Médio	-102.00	766B	NaN	NaN
	2	Médio	-104.00	766B	NaN	NaN
	3	Limite	-134.00	7705	NaN	NaN
	4	Bom	-99.00	7705	NaN	NaN
	5	Limite	-129.00	7705	NaN	NaN
	6	Limite	-131.00	766B	NaN	NaN
	7	Bom	-107.00	7705	-115.00	766B
	8	Bom	-103.00	7705	NaN	NaN
	9	Bom	-98.00	7705	NaN	NaN
	10	Bom	-94.00	7705	NaN	NaN
	11	Bom	-82.00	7705	NaN	NaN

Os dados coletados são apresentados na Tabela 15 e na Figura 46.

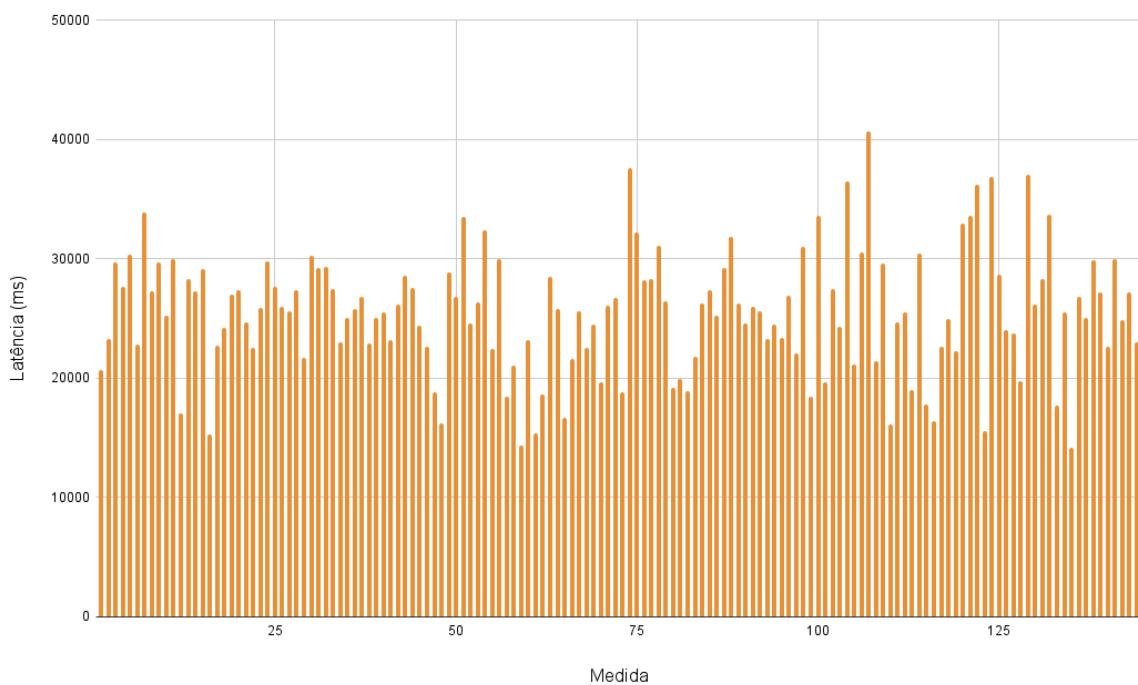
A latência mínima registrada foi de 14160 milissegundos e máxima de 40685 milissegundos. O tempo médio para registro dos dados foi de 25495 milissegundos com sua mediana muito próxima 25640 milissegundos. Entende-se que a mediana é o tempo mais próximo do provável para um registro individual. O desvio padrão encontrado foi de 5096 milissegundos.

Ao levar em consideração a quantidade de serviços utilizados, possíveis congestionamentos de rede e a prova de trabalho necessária para anexar transações no Tangle, considera-se que o desvio padrão variou pouco em relação à média. No contexto desta dissertação, não precisamos de resposta em “tempo real”, viabilizando a aplicação do projeto. Ressalta-se que os tempos registrados são satisfatórios para registro de dados em aplicações que não exigem tomada de decisão “instantânea”, enquanto o produto está em transporte.

Tabela 15 – Latência do ecossistema

Medida	Latência (ms)	Medida	Latência (ms)	Medida	Latência (ms)
1	20642	49	28904	97	22044
2	23315	50	26843	98	31017
3	29737	51	33531	99	18425
4	27697	52	24586	100	33563
5	30392	53	26332	101	19683
6	22839	54	32432	102	27487
7	33893	55	22423	103	24273
8	27236	56	29974	104	36468
9	29701	57	18436	105	21122
10	25243	58	21069	106	30510
11	29957	59	14379	107	40685
12	17024	60	23153	108	21428
13	28333	61	15345	109	29583
14	27313	62	18652	110	16097
15	29097	63	28513	111	24639
16	15312	64	25779	112	25500
17	22765	65	16661	113	19041
18	24234	66	21569	114	30436
19	27006	67	25604	115	17748
20	27334	68	22511	116	16416
21	24682	69	24518	117	22656
22	22489	70	19666	118	24971
23	25901	71	26061	119	22227
24	29837	72	26711	120	32946
25	27642	73	18785	121	33573
26	26004	74	37636	122	36190
27	25646	75	32236	123	15580
28	27405	76	28216	124	36827
29	21718	77	28306	125	28666
30	30275	78	31074	126	23992
31	29273	79	26413	127	23741
32	29360	80	19210	128	19711
33	27434	81	19917	129	37009
34	23010	82	18943	130	26167
35	25057	83	21797	131	28273
36	25826	84	26249	132	33692
37	26849	85	27375	133	17654
38	22949	86	25220	134	25547
39	25062	87	29222	135	14160
40	25551	88	31810	136	26776
41	23192	89	26289	137	25057
42	26118	90	24602	138	29844
43	28574	91	25963	139	27204
44	27526	92	25634	140	22639
45	24432	93	23253	141	29942
46	22671	94	24476	142	24844
47	18837	95	23412	143	27140
48	16197	96	26915	144	22983

Figura 46 – Latência do ecossistema



Fonte – O autor

7.4 VALIDAÇÃO DA PROVA DE CONCEITO - VIAGEM

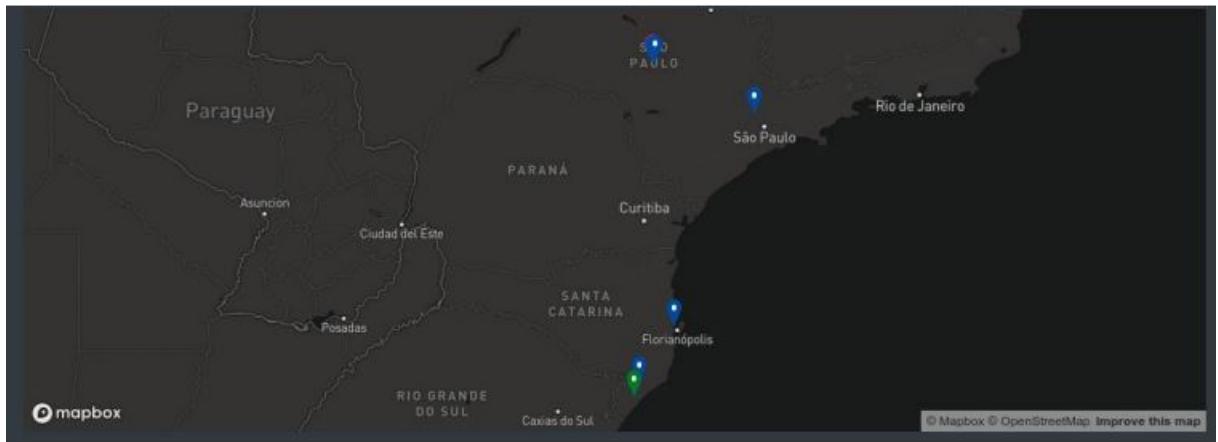
A metodologia apresentada na Seção 6.0.4 propiciou registros de dados de temperatura e localização, utilizando o sistema apresentado na Seção 5.1, Figura 24. Os dados coletados são apresentados e discutidos nesta sessão. Foram realizadas duas experimentações, “Araranguá/SC - Baurú/SP” e “Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP”.

7.4.1 Viagem 1: Araranguá/SC - Baurú/SP

O apêndice A e B contém todos os dados medidos pelo sistema embarcado e registrados no IOTA/Tangle. O apêndice A contém dados de localização, enquanto o B, temperatura. O sistema web desenvolvido permitiu visualização gráfica dos dados registrados e advindos diretamente do Tangle, e são apresentados na Figura 47 e Figura 48.

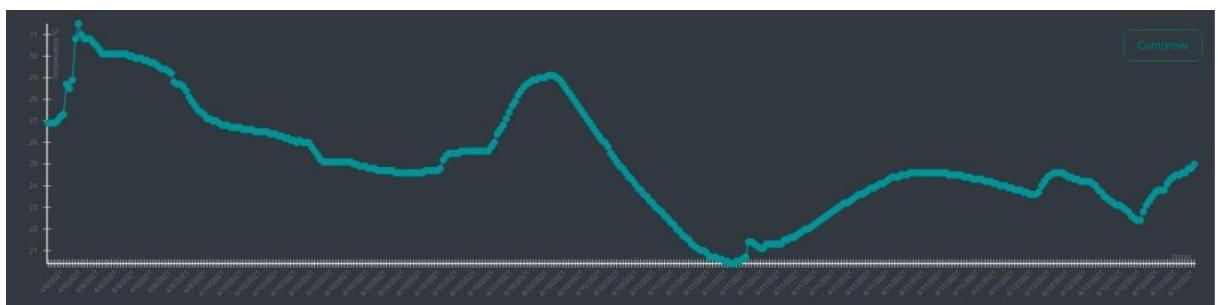
Pode-se identificar na Figura 47 cinco regiões com dados registrados. O primeiro registro, em verde, está a cidade de Araranguá, seguido de Criciúma e Florianópolis em Santa Catarina. Depois, Vila Nova e Baurú (em azul/vermelho), em São Paulo. Apesar de não explicitado na Figura 47 foram medidas várias vezes a mesma localidade, em

Figura 47 – Dados de localização - Viagem Araranguá/SC -> Baurú/SP



Fonte – O autor

Figura 48 – Dados de temperatura - Viagem Araranguá/SC -> Baurú/SP



Fonte – O autor

sua maioria pontos de armazenamento dos correios, um *zoom* no mapa, dentro do sistema, permite verificar esse fato com facilidade.

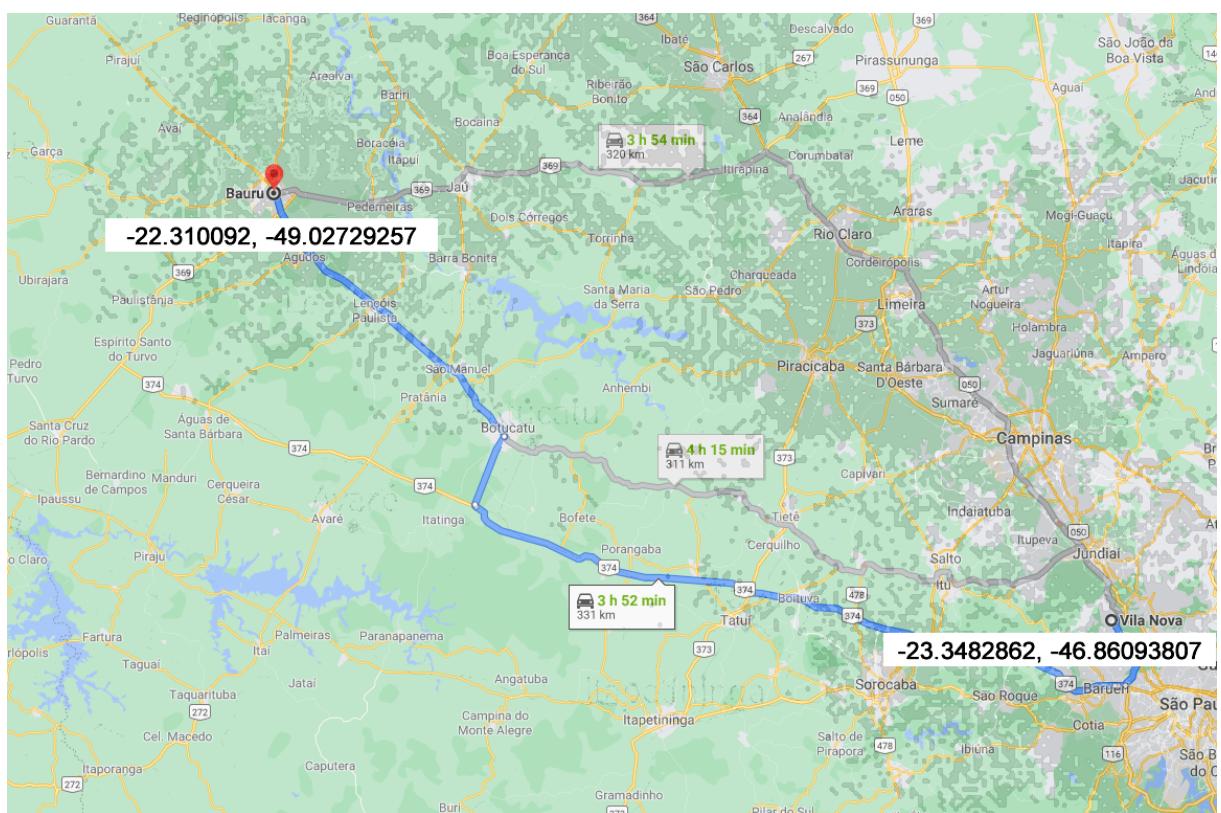
A ausência de dados entre Florianópolis e São Paulo/SP causa certa estranheza, com a ausência de dados em cidades como Joinville/SC e Curitiba/PR que possuem cobertura conforme apresentado na Figura 42. No entanto, após analisar os dados com mais cuidado, percebeu-se que em Florianópolis existem registros de dados de localização no Aeroporto, e por esse motivo, deduzimos que a remessa foi enviada de avião. Como não existem roteadores *Wi-fi* mapeados, dentro do avião e menos ainda cobertura *Sigfox*, não existem dados desse percurso.

Quando se compara a quantidade de dados de temperatura e localização, percebe-se também que foram registrados muito mais dados de temperatura. Foram 148 localizações registradas, contra 365 dados de temperatura. Utilizando a data de registro de temperatura, sabe-se que a primeira medida ocorreu dia 09/04/2021 às 13:08 e a última dia 12/04/2021 às 09:58 (Apêndice B), com medidas realizadas a

cada 10 minutos, esperavam-se 414 registros. Portanto, é correto afirmar que foram perdidos 49 dados de temperatura (aproximadamente 12% do total) e 266 dados de localização (aproximadamente 64% do total).

Pode-se observar, que os dados de temperatura e localização registrados no Tangle possuem um intervalo grande sem registro de dados. O maior intervalo sem dados de localização está entre o dia 11/04/2021 às 17:48:30 e 12/04/2021 às 00:28:28 (Apêndice A). O maior intervalo sem dados de temperatura está entre 11/04/2021 e 17:58:25 e 11/04/2021 às 22:08:22 (Apêndice B). Percebe-se que a maior ausência de registros ocorre em tempos próximos para temperatura e localização. O primeiro registro de temperatura ocorreu 04:09:57 depois, enquanto a localização apenas 06:39:58 depois. A Figura 52 apresenta a primeira e última latitude e longitude registrada, no intervalo mencionado. Para construir o mapa utilizou-se o Google maps, com ponto de partida (23.3482862, -46.86093807) e ponto de chegada (-22.310092, -49.02729257) e sobreposição do gráfico de Cobertura Sigfox.

Figura 49 – Maior área sem registro de dados



Fonte – O autor

Caso a rota em azul da Figura 52 tenha sido utilizada, a ausência de dados é justificada mais facilmente, pois a cobertura Sigfox é menor. São duas as hipóteses para a diferença de tempos de medida de temperatura e localização: a medição de

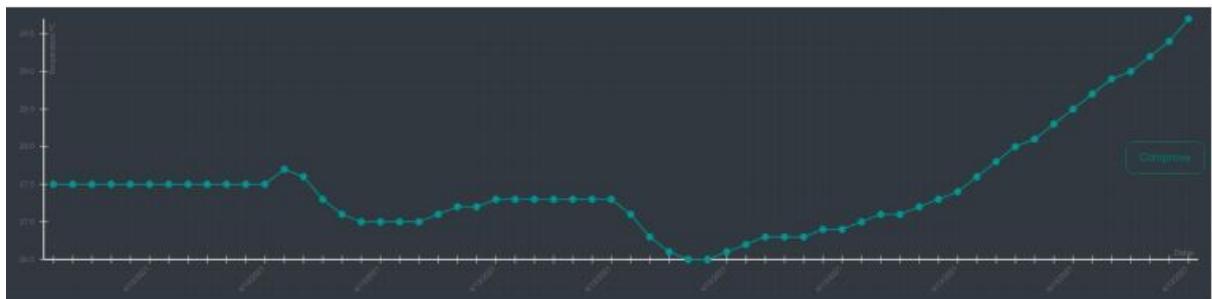
temperatura ocorre anteriormente porque atinge a área de cobertura próxima a Baurú, porém ainda sem cobertura de redes *Wi-fi*, pois ainda não atinge o perímetro mais urbano; Ou ainda, o volume de caixas ao redor do dispositivo é grande o suficiente para que o alcance do mapeamento de redes *Wi-fi* seja insuficiente para identificar roteadores, nesse caso o dispositivo só conseguiria identificar redes quando retirado do sistema de transporte. Analisando os dados do apêndice A, percebe-se que, a partir do primeiro registro de localização existem outros 34 dados da mesma localidade. Após o intervalo mencionado, corrobora-se com a segunda possibilidade, pois o dispositivo é retirado do caminhão e deixado na estação de tratamento dos correios. Pelo Google maps é possível identificar a localidade como uma estação de tratamento dos correios de fato.

7.4.2 Viagem 2: Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP

Buscando isolar uma das variáveis responsáveis pela perda de dados de localização na viagem 1, o hardware foi colocado em cima do painel de um caminhão que faz entregas entre cidades com cobertura Sigfox no estado de São Paulo: Baurú/SP, Araçatuba/SP e São José do Rio Preto/SP. Com isso é possível excluir a dificuldade de leitura de redes *Wi-fi* por conta de obstrução de sinais.

O apêndice C e D contém os dados registrados no Tangle na forma de tabelas. A Figura 50 e Figura 51 apresentam imagens do sistema web com os dados de temperatura e localização respectivamente.

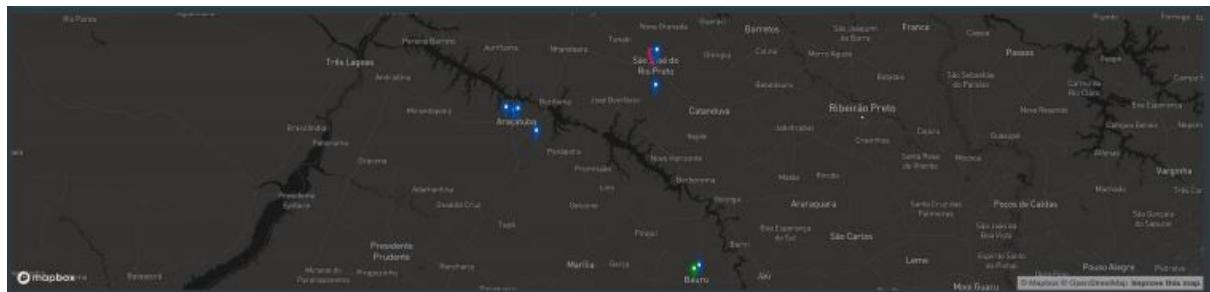
Figura 50 – Dados de temperatura - Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP



Fonte – O autor

Ao analisar os dados coletados de localização do Apêndice C Figura 50, observa-se que existem registros nas cidades de Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP, sem muitos registros entre as cidades. No entanto, ao comparar os dados coletados com a cobertura Sigfox na região (Figura 43), constata-se registro de dados nesses espaços. Outro ponto de análise é a passagem pela cidade de Coroados

Figura 51 – Dados de localização - Baurú/SP - Araçatuba/SP - São José do Rio Preto/SP



Fonte – O autor

(21.2127173, -50.42791367), entre Araçatuba e Baurú, segundo relato do motorista, a velocidade foi de aproximadamente 60 km/h, evidenciado o registro mesmo em movimento.

7.4.3 Consumo de bateria

O consumo de bateria durante todos os testes realizados, entre os dias 09/04/2021 e 13/04/2021, foram registrados pela Ayga e são apresentados na Figura 52.

Figura 52 – Consumo de bateria: viagem 1 e 2



Fonte – O autor, gerado com a plataforma Ayga

A bateria variou entre 3,48 V e 3,43 V, com restauração da diferença de potencial no mesmo intervalo. Pode-se dizer que o consumo nesse período de tempo foi

insignificante. Esse resultado reforça a escolha da Sigfox como rede de baixo consumo de energia, ou ainda alta vida útil da bateria.

7.4.4 Outras considerações

Os serviços da nuvem Ayga, Api da Here e nó publico IOTA permaneceram no ar durante as experimentações. No entanto, tivemos imprevistos com o Servidor hospedado no Heroku.

Após algum tempo de inatividade, devido à baixa cobertura Sigfox, percebeu-se que o Heroku entrava em modo “*Sleep*” e com isso deixava de realizar novas leituras da rota que continha os dados. Resolvemos essa situação utilizando uma CRON com o serviço grátis da cron-job.org. Este serviço permitiu configurar uma requisição para a aplicação em períodos determinados, evitando assim que a aplicação entrasse em modo *sleep*.

Durante uma parte do percurso da viagem 1, percebeu-se que alguns dados eram perdidos na comunicação entre o “servidor” e a IOTA. As perdas ocorreram pela demora no tempo de resposta (*timeout*) do Servidor com a IOTA. Segundo a documentação da Heroku, servidor onde foi hospedada a aplicação, encerra a espera de resposta das conexões HTTP que não retornam dados após 30 segundos (HEROKU, 2021). Em alguns momentos pontuais o *PoW* necessário para registrar os dados no Tangle passaram do tempo de espera da Heroku. São três motivos para a demora: tamanho dos dados (requer maior prova de trabalho), disponibilidade de processamento do servidor e disponibilidade do nó público da IOTA.

O problema foi solucionado, durante o tempo parado na estação de tratamento dos correios, em Florianópolis. A solução executada, foi adicionar um serviço a ser executado após 20 segundos sem resposta de inatividade. O serviço envia um “ ” (espaço) para a rota HTTP, estendendo o tempo por mais 55 segundos (HEROKU, 2021), quando necessário.

Os dados da aplicação são capturados diretamente de um *Fullnode* IOTA, isso implicou em um primeiro carregamento com elevado tempo, quando comparado a um banco de dados tradicional, de apresentação desses dados ao usuário (por volta de 2 minutos quando se tinha mais do que 200 registros).

7.5 CUSTO

A avaliação de custo para execução do projeto, não é um resultado experimental, mas é fruto da execução da pesquisa de campo e documental. Deve-se considerar os custos de Hardware (Ayga Wacs 2), rede Sigfox, conversão dos *MAC address* via API Here e caso seja de interesse rodar um *Fullnode* IOTA, levar em consideração a manutenção de um servidor.

Segundo conversas com representantes da empresa Ayga, o dispositivo Wacs 2 tem um custo de aproximadamente \$25,00. É possível desenvolver de forma independente, porém deve-se levar em consideração a realização de grandes pedidos para diminuir custos e o know-how da integração dos dispositivos.

A rede Sigfox possui duas principais variáveis ao tratar de custos, o número de mensagens necessárias por dia e o país/moeda de pagamento onde será realizado os envios. Considerando a compra do maior pacote de mensagem por dispositivo (144 mensagens por dia) e o Brasil como país de registro, o valor total para o uso da rede é de \$12,00 por ano, segundo conversas com representante da WND Brasil. A WND é dedicada à conectividades Sigfox na América Latina e no Reino Unido.

A Here, que facilita a conversão dos *MAC address* para dados de latitude e longitude, possui diferentes pacotes de serviços, um deles inclusive de graça, para até 250.000 transações por mês e/ou 2.5 GB por mês. O serviço ainda conta com pacotes no valor de \$45,00 e \$449,00 por mês, que incluem mais tráfego, e são ideais para grandes empresas com muitos dispositivos. Para fim dessa dissertação utilizamos o pacote com custo zero. Além disso, ressalta-se que existem bibliotecas *on-line* com *MAC address* mapeados, e, portanto, seria possível construir o próprio banco de dados.

A Fundação Iota facilitou a implantação de nós proprietários (*Fullnodes*) por meio de um serviço da Amazon AWS, dessa forma pode-se utilizar o serviço <<https://aws.amazon.com/kzhc52xmpmgpw>> para estimar os custos. Baseando-se nisso, um servidor hospedado no Brasil (apesar de não necessário) custaria pelo menos de \$0,074 por hora, ou aproximadamente \$53,28 por mês, para um servidor de 4GB de memória ram e 2 núcleos virtuais. O mesmo servidor nos estados Unidos custaria aproximadamente \$0,046 por hora, \$33,12 por mês. Ressalta-se, no entanto, que não há taxas para inserção de mensagens na rede IOTA e a criação de nó próprio é opcional, tendo em vista que existem nós públicos disponíveis.

Caso se opte por utilizar um servidor para rodar um Full Node, recomenda-se utilizar o mesmo para rodar a aplicação *Back-end* e *front-end*, proposta nesse trabalho, sem custos adicionais. Caso contrário será necessário contratar um servidor. O que deve ser levado em consideração é a velocidade, quantidade de tráfego necessária para a aplicação e os requisitos de infraestrutura, como NodeJs e MongoDB. No Brasil a Hostinger oferece esse serviço a partir aproximadamente \$4,50 mês, ou ainda \$54,00 por ano.

Os custos mínimos necessários para rodar o ecossistema proposto, envolvem a aquisição do hardware \$30,00, o servidor da aplicação \$54 por ano e a compra dos serviços de rede \$12,00 por ano. Totalizando \$66,00 por ano, mais \$30,00 do dispositivo. O primeiro ano teria um custo de \$96,00.

Ressalta-se que a estimativa de custos reflete um momento, um tempo e espaço determinado. No entanto, as tecnologias Sigfox e IOTA são realmente pouco custosas

por *design*, quando comparadas com 3G/4G e redes Blockchain como da Ethereum para inserir dados. A rede da Ethereum cobra taxas adicionais por registro, a depender do congestionamento da rede.

7.6 DISCUSSÃO INFORMAL SOBRE IMUTABILIDADE

Esta sessão busca identificar e apresentar questões importantes de segurança relacionadas ao ecossistema proposto, em especial segurança relativa à imutabilidade dos dados coletados e registrados. As reflexões apresentadas são frutos da pesquisa da dissertação e da experiência do desenvolvimento.

Esse projeto assume como premissa, que os dados do dispositivo, de fato referem-se ao ambiente de coleta imaginado. Ou seja, espera-se que não tenha ocorrido alteração no ambiente de coleta ou que o dispositivo não tenha sido alterado ou transportado para outro ambiente. Quando se trata de imutabilidade, essa questão deve ser pertinente, e merece atenção. Essa é uma questão atual quando se pensa em integrar sistemas distribuídos, como Blockchain, ao mundo físico. Portanto, precisa ser investigado com mais cuidado em projetos que envolvam *design* e engenharia.

Na arquitetura proposta, os dados passam por diversos serviços, de terceiros, que podem e precisam ser evitados quando se trata de projetos ditos imutáveis. Como já mencionado, os serviços da Ayga e da Here, ou similares, podem ser retirados do ecossistema, como apresentado na Figura 21. Ainda assim, antes do registro na DLT da IOTA, os dados passam por um servidor e pela rede LPWAN Sigfox. Isso levanta a seguinte questão: Qual a possibilidade real de se realizar modificações em dados pontuais, na Sigfox Cloud, no exato momento que chegam antes mesmo de serem reemitidos? Pode-se responder que sim é possível, porém altamente improvável.

O servidor que recebe os dados e cria o pacote (*package*) para anexar dados no Tangle merece atenção, pois os dados podem ser adulterados antes mesmo de serem enviados para a rede distribuída da IOTA. Considerando que os dados poderiam ser facilmente alterados com poucas linhas de código, como evitar que o sistema seja desonesto por *design*? Uma maneira de se evitar seria por meio de auditorias de código e verificação experimental de dispositivos ligados a ele, ou ainda acreditar no prestígio e/ou reputação dos desenvolvedores e mantenedores do sistema. Caso o sistema seja validado, é necessário que este seja publicado em um repositório ao estilo “Git”, e publicado no servidor diretamente por ele, para que fosse mantida uma auditoria pública. Com isso, pode-se também garantir por meio de *hash* dos arquivos que o sistema não foi alterado.

Um servidor é e sempre será um possível ponto de falha. Como mencionado na Seção 2.3 a arquitetura ideal seria registrar dados diretamente no sistema embarcado. No entanto, o baixo poder de processamento de sistemas embarcados, a necessidade, proposta nesse trabalho, do baixo consumo de energia, e ainda o pacote máximo de

12 bytes da Sigfox, implicam na necessidade de existência do servidor para esse tipo de aplicação. Esse é um desafio enorme para a fundação IOTA, diminuir a prova de trabalho necessária para anexar transações no Tangle, enquanto mantém a segurança do sistema e baixo consumo.

Excluindo ataques típicos a servidores web (como DDOS), pode-se identificar outros tipos de fragilidades como a descoberta voluntária ou não do canal MAM do dispositivo. De posse do nome do canal, poder-se-ia enviar mais mensagens de outros sistemas, para o mesmo grupo de dados, confundindo, ou inviabilizando a leitura correta dos dados. Essa situação pode ser minimizada utilizando o MAM em modo privado ou restrito, ver Seção 2.2.7. Essa situação inibe a possibilidade de descoberta do canal MAM por ser uma rede pública. A única possibilidade real, de um registro de dados advindo de outra fonte, seria identificar o canal MAM, as chaves de acesso, e o endereço da próxima mensagem (*next root*), no banco de dados centralizado. Ainda que isso seja feito, o dado precisará ser inserido mais rapidamente do que o próximo dado advindo do dispositivo “real” ou interrompendo as atividades do servidor.

No estado atual da aplicação, desenvolvida e publicada no Github, é necessário também criar sistemas de segurança adicionais para o login dos usuários. Pois esses sistemas permitem registrar dispositivos e/ou visualizar dados. No entanto, não implicam em alteração relativa a imutabilidade do dado. Todavia, possibilitaria a exclusão do canal MAM no banco de dados. Novamente, o dado não seria apagado, somente não visualizado na aplicação, apenas em *Fullnodes* IOTA.

Quando se trata de criptomoedas, como o caso da IOTA, tipicamente a preocupação de segurança está relacionada à possibilidade de gasto duplo, no entanto essa questão é pouco relevante quando trata-se de registro de dados nessa tecnologia de registro distribuído. A preocupação está relacionada com a possibilidade real de alteração nos dados. Isso só pode acontecer na IOTA em caso de “ataque parasita”, essa possibilidade refere-se a um determinado atacante, controlar a maior parte da rede, e ter seu “ramo” como principal, nesse caso o atacante passa a ter controle sobre a rede, e em teoria poderia alterar os dados. No entanto, utilizar o MAM em modo privado ou restrito, inviabiliza a alteração dos dados, devido à criptografia utilizada no MAM. Apesar da possibilidade remota do ataque parasita, a IOTA ainda possui o “coordenador” que atualmente inviabiliza esse tipo de situação, no entanto esse tipo de discussão é importante, caso a Fundação IOTA continue na evolução do projeto, buscando retirar o coordenador da rede.

Cabe relembrar que *Fullnodes* são nós na rede IOTA, esses nós são armazenados em servidores, e, portanto, também são possíveis alvos de ataques, como DDOS. Sendo assim, é importante que uma aplicação, como a proposta, tenha diversos domínios de *Fullnodes* como possibilidades para o caso de interrupção de serviço. Novamente, ressalta-se que os dados não serão apagados, pois são replicados na

rede, justamente a grande vantagem dos sistemas distribuídos.

8 CONCLUSÃO

A cadeia de suprimentos é favorecida pelo uso do Tangle da IOTA, especialmente na logística de transporte, pois durante esse processo outras soluções distribuídas, como Blockchains públicas, são pouco efetivas, principalmente em termos de custo. Qualquer tipo de mercadoria pode ser monitorada e/ou rastreada de maneira imutável por um ecossistema como o proposto. No entanto, cargas que exijam algum tipo de cuidado durante o transporte são potencialmente favorecidas, em termos de valor agregado, como é o caso de vacinas, carne, leite, frutas e outras cargas perecíveis.

O sistema proposto se mostrou eficiente para registros de dados, mesmo em movimento. O maior desafio está na área de cobertura Sigfox. As experimentações mostram dificuldades em conseguir capturar a localização do dispositivo. A dificuldade está relacionada a duas situações distintas, baixa cobertura Sigfox e baixa densidade de roteadores em áreas não urbanizadas. No Brasil a Sigfox só possui cobertura nas capitais e em 70% das cidades com mais de 200 mil habitantes (WND, 2021), o que implica em grandes áreas de sombreamento. Normalmente entre cidades existem áreas com baixa quantidade de roteadores, devido a baixa urbanização, isso implica em ausências *MAC address*. A obtenção da geolocalização em um sistema como esse "responde" conforme esperado em locais com alta taxa de roteadores por área e alta cobertura Sigfox, há vários locais na Europa com essas características, especialmente na França. Para funcionar bem no Brasil e/ou em cidades do Brasil, a cobertura Sigfox precisa crescer substancialmente.

Para melhor aproveitamento das características da IOTA e Sigfox, foi necessário tomar alguns cuidados, esse foi o caso da escolha do mapeamento de Geolocalização com *MAC address*. Para manter a premissa de baixo custo, foi necessário manter o baixo consumo de energia, típicos de dispositivos Sigfox. Para manter o baixo consumo, o dispositivo sai de modo "*sleep*" e busca redes *Wi-fi* por 5 segundos, em períodos de coleta de 10 minutos, com captura de dois *MAC address* de roteadores, quando disponíveis. Mesmo com estas restrições, o dispositivo foi encontrado com uma média de 24,5 metros de distância do seu local real. O consumo de bateria ao longo de 4 dias, enviando 2 *MAC address* a cada dez minutos e registrando um dado de temperatura também a cada 10 minutos, foi insignificante. Isso significa que a manutenção do dispositivo levaria muito tempo para ser realizada, diminuindo ainda mais os custos.

Um dos pontos de maior interesse é a latência do sistema. O tempo para um dado ser registrado no Tangle, passando por todas as etapas descritas na Figura 20 é de aproximadamente 25 segundos. Dentro desse espaço de tempo existem diversas possibilidades de uso, desde que esse tempo seja suficiente para a tomada de decisão. No entanto, ainda que melhorias não sejam implementadas durante o trajeto, o registro transparente e imutável dos dados é que fornece segurança entre as partes para a

melhor negociação. O uso de um ecossistema como esse gera valor agregado ao transporte, justamente porque traz segurança ao consumidor/cliente. Complementarmente ao proposto, poder-se-ia criar avisos técnicos para uma grande variância dos dados ambientais, ou ainda, identificação de limites de temperatura, umidade, nível de oxigênio entre outros, através dos quais uma negociação deixaria de acontecer.

O ecossistema proposto, possui algumas fragilidades que podem e devem ser aprimoradas. Optou-se por apresentar ao usuário dados diretamente do Tangle, essa decisão de projeto proporcionou um lento carregamento de dados quando o canal MAM continha muitos dados. Entende-se que essa situação possa ser mitigada armazenando todos os dados em um banco de dados e um *front-end* apresenta ao usuário esses dados enquanto o sistema valida o hash dos dados do banco e os compara com os registrados no Tangle. O *front-end* pode confirmar, ou não, a veracidade do dado ao usuário no devido tempo.

A princípio a Sigfox permite que um dispositivo emita, no máximo 144 mensagens por dia, uma mensagem a cada 10 minutos, seguindo a regulamentação de uso das bandas ISM não licenciadas (68 MHz na Europa, 915 MHz nas Américas, e 433 MHz na Ásia). No entanto, ao longo da pesquisa descobriu-se que, quando uma mesma conta de usuário Sigfox possui vários dispositivos cadastrados, um dispositivo pode usar as mensagens ainda não utilizadas de outro determinado dispositivo. Isso pode ser importante para alguns casos de uso, especialmente para grandes empresas.

A preocupação com a perda de pacotes também foi estudada, em especial a perda de pacotes em situações em que o sinal Sigfox foi emitido em movimento, encontrou-se uma perda de aproximadamente 24% das mensagens quando em movimento a 90 km/h e isso deve estar relacionado à modulação do Sinal Sigfox, ou seja, intrínseco da tecnologia. A perda de 24% de pacotes em movimento acena um alerta, pois não se pode confiar que sempre serão enviadas mensagens nos períodos estabelecidos para situações em movimento. Um ponto positivo do resultado dessa pesquisa é que a perda de mensagens em movimento representa a minoria dos dados coletados, do contrário inviabilizaria o projeto com Sigfox.

Outras discussões importantes sobre o trabalho referem-se à arquitetura proposta e o tipo de conectividade potencial para o caso de uso estudado. A necessidade de rodar o IOTA client e/ou MAM client, inviabilizou transacionar dados diretamente do dispositivo Sigfox. Primeiramente a necessidade de baixo consumo de energia, inviabiliza qualquer processamento adicional no dispositivo. Em segundo lugar, os pacotes via rede *Ultra Narrow Band* Sigfox, possuem capacidade máxima de 12 bytes por envio, e, portanto, não seria capaz de enviar um pacote IOTA, por volta de 530 bytes. Essas duas questões obrigam que uma estrutura em nuvem/servidor seja necessária. Se fosse possível e desejável, enviar o pacote via rede LPWAN Sigfox, as mensagens precisariam ser configuradas para serem encaminhadas, diretamente da Sigfox para

um *Fullnode* IOTA, essa tarefa também não seria trivial e caberia uma parceria entre a Fundação IOTA e Sigfox. No entanto, isso só seria possível caso, em desenvolvimentos futuros, o pacote mínimo da IOTA fosse reduzido substancialmente. Obviamente, conectividade 3G/4G/5G são favorecidas, no entanto os custos e consumo de energia aumentam e dificultam sua manutenção.

Como existe o servidor/nuvem responsável pela criação e envio do pacote IOTA, ele pode ser um ponto de falha. Além disso, o canal IOTA MAM e outros dados relativos, como o “next root” encontram-se no banco de dados, e são suscetíveis a ataques. De posse dos dados do banco, um atacante que consiga acesso, poderá adicionar mensagens subsequentes ao canal MAM, onde são depositados os dados, no entanto os dados registrados até então, se mostram seguros e inalteráveis.

A existência dos “*snapshots*” na rede IOTA, obriga-nos a refletir sobre o tempo de disponibilidades dos dados imutáveis na rede. A garantia de imutabilidade pode ser concretamente afirmada até que um *snapshot* ocorra. Pode-se evitar *snapshots* executando um *Fullnode* próprio, que realiza *snapshot* apenas quando o dado for descartável, ao final de uma viagem por exemplo, no entanto os dados deixam de estar distribuídos na rede. Pode-se ainda, utilizar uma solução de cadeia cruzada com uma Blockchain, porém com apenas uma transação ao fim da viagem, subtraindo substancialmente os custos de envios individuais, inviáveis em Blockchain públicas verdadeiramente transparentes. Além disso, a fundação IOTA poderia facilitar o uso de *Fullnodes* públicos indicando qual o tempo esperado para o próximo *snapshot* global via uma rota HTTP, por exemplo.

O conhecimento mais amplo do protocolo IOTA, permite dizer que a viabilidade de longo prazo do protocolo está relacionada a estímulos para rodar *Fullnodes* na rede. Sabe-se que operar um *FullNode* oferece um ponto de entrada seguro no Tangle, no entanto nós públicos resolvem a maior parte das aplicações. A Fundação IOTA vem trabalhando com o conceito de “mana” que pode ser um impulsionador importante nesse sentido. Essa linha de pesquisa e desenvolvimento, deve ser acompanhada com cuidado por pesquisas interessadas em tecnologias distribuídas baseadas em DAG, IoT e aplicações do protocolo IOTA.

É importante pontuar que durante o desenvolvimento deste trabalho o protocolo da IOTA, saiu do 1.0 para 1.5, os testes foram realizados durante essa mudança. A Fundação IOTA está finalizando as alterações da versão 1.5 e preparando-se para 2.0, esse passo é fundamental para o futuro do protocolo de dados/criptomoeda. Além disso, o MAM foi descontinuado, tendo como substituto o “Streams”, com funções muito similares.

A conectividade Sigfox junto com a tecnologia de registro distribuído da IOTA, aplicadas à infraestrutura proposta, possibilitou registrar dados de maneira imutável e com baixo consumo de energia por dispositivo e, portanto, são opções viáveis para

aplicação a logística de uma cadeia de suprimentos.

REFERÊNCIAS

- ABMUSHI. IOTA: Signature And Validation. **Medium**, 2018. Disponível em: <<https://medium.com/@abmushi/iota-signature-and-validation-b95b3f9ec534>>. Acesso em: 20 jul. 2021.
- AERNOOTS, Michiel et al. A comparison of signal strength localization methods with sigfox. In: **2018 15th Workshop on Positioning, Navigation and Communications (WPNC)**. IEEE, 2018. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8555743>>. Acesso em: 20 jul. 2021.
- AL-KASHOASH, Hayder AA; KEMP, Andrew H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. **Australian Journal of Electrical and Electronics Engineering**, v. 13, n. 4, p. 268-274, 2016. Disponível em: <<https://www.tandfonline.com/doi/abs/10.1080/1448837X.2017.1409920>>. Acesso em: 20 jul. 2021.
- AMMOUS, Saifedean. Blockchain Technology: What is it good for?. **SSRN**, 2832751, 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751>. Acesso em: 20 jul. 2021.
- BAHL, Paramvir; PADMANABHAN, Venkata N. RADAR: An in-building RF-based user location and tracking system. In: **Proceedings IEEE INFOCOM 2000**. Conference on computer communications. Nineteenth annual joint conference of the IEEE computer and communications societies (Cat. No. 00CH37064). Ieee, 2000. p. 775-784. Disponível em: <<https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/infocom2000.pdf>>. Acesso em: 20 jul. 2021.
- BARALLA, Gavina et al. Ensuring transparency and traceability of food local products: A blockchain application to a Smart Tourism Region. **Concurrency and Computation: Practice and Experience**, v. 33, n. 1, p. e5857, 2021. Disponível em: <<https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.5857>>. Acesso em: 20 jul. 2021.
- BARTOLOMEU, Paulo C.; VIEIRA, Emanuel; FERREIRA, Joaquim. IOTA feasibility and perspectives for enabling vehicular applications. In: **2018 IEEE Globecom Workshops (GC Wkshps)**. IEEE, 2018. p. 1-7. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8644201/>>. Acesso em: 20 jul. 2021.
- BORGES, Luan Lorenzo dos Santos. **Sistema de monitoramento de faltas em redes de distribuição de energia elétrica utilizando rede SigFox**. Trabalho de conclusão de curso (Bacharelado em Engenharia de Computação) - Departamento de Computação, Universidade Federal de Santa Catarina, Araranguá, 2019.
- BROGAN, James; BASKARAN, Immanuel; RAMACHANDRAN, Navin. Authenticating health activity data using distributed ledger technologies. **Computational and structural biotechnology journal**, v. 16, p. 257-266, 2018. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S2001037018300345>>. Acesso em: 20 jul. 2021.

BUCHMANN, Johannes; DING, Jintai (Ed.). **Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA October 17-19, 2008 Proceedings**. Springer Science & Business Media, 2008. Disponível em: <http://2017.qcrypt.net/wp-content/uploads/2015/10/Tutorial4_Johannes-Buchmann.pdf>. Acesso em: 20 jul. 2021.

BUTERIN, V. Ethereum sharding FAQs. **Github**, 2018. Disponível em: <<https://github.com/ethereum/wiki/wiki/Sharding>>. Acesso em: 20 jul. 2021.

CoinMarketCap. Crypto-Currency Capitalizations. **CoinMarketCap**, 2020. Disponível em: <<https://www.coinmarketcap.com>>. Acesso em: 20 jul. 2021.

CENTENARO, Marco et al. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. **IEEE Wireless Communications**, v. 23, n. 5, p. 60-67, 2016. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7721743/>>. Acesso em: 20 jul. 2021.

CHINTALAPUDI, Krishna; PADMANABHA IYER, Anand; PADMANABHAN, Venkata N. Indoor localization without the pain. In: **Proceedings of the sixteenth annual international conference on Mobile computing and networking**. 2010. p. 173-184. Disponível em: <<https://dl.acm.org/doi/abs/10.1145/1859995.1860016>>. Acesso em: 20 jul. 2021.

CHOHAN, Usman W. The Double Spending Problem and Cryptocurrencies. **SSRN**, 3090174, 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174>. Acesso em: 20 jul. 2021.

COOK, Deborah J.; MULROW, Cynthia D.; HAYNES, R. Brian. Systematic reviews: synthesis of best evidence for clinical decisions. **Annals of internal medicine**, v. 126, n. 5, p. 376-380, 1997. Disponível em: <<https://www.acpjournals.org/doi/abs/10.7326/0003-4819-126-5-199703010-00006>>. Acesso em: 20 jul. 2021.

CORDEIRO, Alexander Magno et al. Revisão sistemática: uma revisão narrativa. **Revista do Colégio Brasileiro de Cirurgiões**, v. 34, p. 428-431, 2007. Disponível em: <<https://www.scielo.br/j/rcbc/a/CC6NRNtP3dKLgLPwcmV6Gf/abstract/?lang=pt>>. Acesso em: 20 jul. 2021.

DISK91. Sigfox to move! **Disk91**, 2017. Disponível em: <<https://www.disk91.com/quiet-disk91/>>. Acesso em: 20 jul. 2021.

DIVYA, M.; BIRADAR, Nagaveni B. IOTA-next generation block chain. **International Journal of Engineering and Computer Science**, v. 7, n. 04, p. 23823-23826, 2018. Disponível em: <<http://ijecs.in/index.php/ijecs/article/view/4007>>. Acesso em: 20 jul. 2021.

DO, Minh-Tien; GOURSAUD, Claire; GORCE, Jean-Marie. Interference modelling and analysis of random fdma scheme in ultra narrowband networks. In: **AICT 2014**. 2014. Disponível em: <<https://hal.archives-ouvertes.fr/hal-01096493/>>. Acesso em: 20 jul. 2021.

EL IOINI, Nabil; PAHL, Claus. Trustworthy orchestration of container based edge computing using permissioned blockchain. In: **2018 Fifth International Conference on Internet of Things: Systems, Management and Security**. IEEE, 2018. p. 147-154. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8554470/>>. Acesso em: 20 jul. 2021.

FERNÁNDEZ-AHUMADA, Luis Manuel et al. Proposal for the design of monitoring and operating irrigation networks based on IoT, cloud computing and free hardware technologies. **Sensors**, v. 19, n. 10, p. 2318, 2019. Disponível em: <<https://www.mdpi.com/465388>>. Acesso em: 20 jul. 2021.

FERNÁNDEZ-GARCIA, Raul; GIL, Ignacio. An alternative wearable tracking system based on a low-power wide-area network. **Sensors**, v. 17, n. 3, p. 592, 2017. Disponível em: <<https://www.mdpi.com/185988>>. Acesso em: 20 jul. 2021.

FERRARO, Pietro; KING, Christopher; SHORTEN, Robert. Distributed ledger technology for smart cities, the sharing economy, and social compliance. **IEEE Access**, v. 6, p. 62728-62746, 2018. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8496756/>>. Acesso em: 20 jul. 2021.

FLOREA, Bogdan Cristian. Blockchain and Internet of Things data provider for smart applications. In: **2018 7th Mediterranean Conference on Embedded Computing (MECO)**. IEEE, 2018. p. 1-4. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8406041/>>. Acesso em: 20 jul. 2021.

FLOREA, Bogdan Cristian; TARALUNGA, Dragos Daniel. Blockchain IoT for smart electric vehicles battery management. **Sustainability**, v. 12, n. 10, p. 3984, 2020. Disponível em: <<https://www.mdpi.com/2071-1050/12/10/3984>>. Acesso em: 20 jul. 2021.

FOUNDATION IOTA. Chrysalis (IOTA 1.5) Phase 1 Now Live on Mainnets. **Foundation Iota**, 2020. Disponível em: <<https://blog.iota.org/chrysalis-iota-1-5-phase-1-now-live-on-mainnet-958ec4a4a415>>. Acesso em: 20 jul. 2021.

GADDAM, Sarath Chandu; RAI, Mritunjay Kumar. A comparative study on various LPWAN and cellular communication technologies for IoT based smart applications. In: **2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)**. IEEE, 2018. p. 1-8. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8529060/>>. Acesso em: 20 jul. 2021.

GAL, Alon. The Tangle: an Illustrated Introduction. **Blog Iota**, 2018. Disponível em: <<https://blog.iota.org/the-tangle-an-illustrated-introduction4d5eae6fe8d4>>. Acesso em: 20 jul. 2021.

GÖBEL, Johannes; KRZESINSKI, Anthony E. Increased block size and Bitcoin blockchain dynamics. In: **2017 27th International Telecommunication Networks and Applications Conference (ITNAC)**. IEEE, 2017. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8215367/>>. Acesso em: 20 jul. 2021.

GOMEZ, Carles et al. IPv6 over LPWANs: Connecting low power wide area networks to the Internet (of Things). **IEEE Wireless Communications**, v. 27, n. 1, p. 206-213, 2020. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8994201>>. Acesso em: 20 jul. 2021.

GOOGLE. Data collected by Google cars. **Google**, 2010. Disponível em: <<https://europe.googleblog.com/2010/04/data-collected-by-google-cars.html>>. Acesso em: 20 jul. 2021.

HANDY, Paul. Introducing masked authenticated messaging. **IOTA Foundation Medium blog**, 2017. Disponível em: <<https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/>>. Acesso em: 20 jul. 2021.

HASAN, Haya R. et al. Blockchain-based solution for the traceability of spare parts in manufacturing. **IEEE Access**, v. 8, p. 100308-100322, 2020. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9103086>>. Acesso em: 20 jul. 2021.

HASAN, Haya et al. Smart contract-based approach for efficient shipment management. **Computers & Industrial Engineering**, v. 136, p. 149-159, 2019. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0360835219304140>>. Acesso em: 20 jul. 2021.

HASSIJA, Vikas et al. A distributed framework for energy trading between UAVs and charging stations for critical applications. **IEEE Transactions on Vehicular Technology**, v. 69, n. 5, p. 5391-5402, 2020. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9019832>>. Acesso em: 20 jul. 2021.

HELO, Petri; HAO, Yuqiuge. Blockchains in operations and supply chains: A model and reference implementation. **Computers & Industrial Engineering**, v. 136, p. 242-251, 2019. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0360835219304152>>. Acesso em: 20 jul. 2021.

HELO, Petri; SHAMSUZZOHA, A. H. M. Real-time supply chain—A blockchain architecture for project deliveries. **Robotics and Computer-Integrated Manufacturing**, v. 63, p. 101909, 2020. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0736584518306665>>. Acesso em: 20 jul. 2021.

HERE. HERE Network Positioning API. **Here**, 2021. Disponível em: <https://developer.here.com/documentation/positioning/dev_guide/topics/whatis.html>. Acesso em: 20 jul. 2021.

HEROKU. Políticas da plataforma Heroku. **Heroku**, 2021. Disponível em: <<https://devcenter.heroku.com/articles/limits#router>>. Acesso em: 20 jul. 2021.

HILEMAN, Garrick; RAUCHS, Michel. Global cryptocurrency benchmarking study. **Cambridge Centre for Alternative Finance**, v. 33, p. 33-113, 2017. Disponível em: <<https://www.crowdfundinsider.com/wp-content/uploads/2017/04/Global-Cryptocurrency-Benchmarking-Study.pdf>>. Acesso em: 20 jul. 2021.

HÜLSING, Andreas. W-OTS+-shorter signatures for hash-based signature schemes. In: **International Conference on Cryptology in Africa**. Springer, Berlin, Heidelberg, 2013. p. 173-188. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-642-38553-7_10>. Acesso em: 20 jul. 2021.

IMERI, Adnan; KHADRAOUI, Djamel. The security and traceability of shared information in the process of transportation of dangerous goods. In: **2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)**. IEEE, 2018. p. 1-5. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8328751>>. Acesso em: 20 jul. 2021.

IOTA. What is IOTA? **IOTA**, 2020. Disponível em: <<https://www.iota.org/get-started/what-is-iota1>>. Acesso em: 20 jul. 2021.

IOTA. Coördicide Team. **Blog IOTA**, 2019. Disponível em: <<https://blog.iota.org/coördicide-update-autopeering-part-1-fc72e21c7e11>>. Acesso em: 20 jul. 2021.

IOTA, FAQ. What is the difference between a Light Node and Full Node? **IOTA**, 2020. Disponível em: <<https://www.iota.org/get-started/faqs>>. Acesso em: 20 jul. 2021.

IOTA, Suporte. How addresses are used in IOTA. **IOTA**, 2019. Disponível em: <<https://iotasupport.com/how-addresses-are-used-in-IOTA.shtml>>. Acesso em: 20 jul. 2021.

JANES, Martyn. MAM Client JS Library. **Github**, 2019. Disponível em: <<https://www.mdpi.com/2076-3417/7/9/936>>. Acesso em: 20 jul. 2021.

JANSSEN, Thomas; WEYN, Maarten; BERKVENS, Rafael. Localization in low power wide area networks using wi-fi fingerprints. **Applied Sciences**, v. 7, n. 9, p. 936, 2017. Disponível em: <<https://github.com/iotaledger/mam.client.js/>>. Acesso em: 20 jul. 2021.

JIANG, Yiming et al. A cross-chain solution to integrating multiple blockchains for IoT data management. **Sensors**, v. 19, n. 9, p. 2042, 2019. Disponível em: <<https://www.mdpi.com/1424-8220/19/9/2042>>. Acesso em: 20 jul. 2021.

LAMBERT, Douglas M.; COOPER, Martha C. Issues in supply chain management. **Industrial marketing management**, v. 29, n. 1, p. 65-83, 2000. Disponível em:

<<https://www.sciencedirect.com/science/article/abs/pii/S0019850199001133>>. Acesso em: 20 jul. 2021.

LAUMAIR. The official JavaScript client library for interacting with the Tangle. Github, 2020. Disponível em: <<https://github.com/iotaledger/iota.js>>. Acesso em: 20 jul. 2021.

LAURIDSEN, Mads et al. Interference measurements in the European 868 MHz ISM band with focus on LoRa and SigFox. In: **2017 IEEE Wireless Communications and Networking Conference (WCNC)**. IEEE, 2017. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7925650>>. Acesso em: 20 jul. 2021.

LEE, Jong-Hyouk; PILKINGTON, Marc. How the blockchain revolution will reshape the consumer electronics industry [future directions]. **IEEE Consumer Electronics Magazine**, v. 6, n. 3, p. 19-23, 2017. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7948864>>. Acesso em: 20 jul. 2021.

LEMIC, Filip et al. Enriched Training Database for improving the WiFi RSSI-based indoor fingerprinting performance. In: **2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)**. IEEE, 2016. p. 875-881. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7444904>>. Acesso em: 20 jul. 2021.

LEMIC, Filip et al. Experimental evaluation of RF-based indoor localization algorithms under RF interference. In: **2015 International Conference on Localization and GNSS (ICL-GNSS)**. IEEE, 2015. p. 1-8. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7217149>>. Acesso em: 20 jul. 2021.

LIN, Qijun et al. Food safety traceability system based on blockchain and EPCIS. **IEEE Access**, v. 7, p. 20698-20707, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8640818>>. Acesso em: 20 jul. 2021.

LYMBEROPoulos, Dimitrios et al. A realistic evaluation and comparison of indoor location technologies: Experiences and lessons learned. In: **Proceedings of the 14th international conference on information processing in sensor networks**. 2015. p. 178-189. Disponível em: <<https://dl.acm.org/doi/abs/10.1145/2737095.2737726>>. Acesso em: 20 jul. 2021.

MACIEL, Nelson Rafael Portela. **Sistema autónomo de monitorização da qualidade de águas fluviais baseado em tecnologia Sigfox**. Dissertação de mestrado (Mestrado Integrado em Engenharia Eletrotécnica e de Computadores) - Faculdade de Engenharia da Universidade do Porto, Portugal, 2020.

MAITI, Ananda et al. Estimating service quality in industrial internet-of-things monitoring applications with blockchain. **IEEE access**, v. 7, p. 155489-155503, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8876654>>. Acesso em: 20 jul. 2021.

MANUPATI, Vijaya Kumar et al. A blockchain-based approach for a multi-echelon sustainable supply chain. **International Journal of Production Research**, v. 58, n. 7,

p. 2222-2241, 2020. Disponível em: <<https://www.tandfonline.com/doi/abs/10.1080/00207543.2019.1683248>>. Acesso em: 20 jul. 2021.

MARINO, Francesco; MOISO, Corrado; PETRACCA, Matteo. Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems. **Computer Networks**, v. 148, p. 176-195, 2019. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1389128618312167>>. Acesso em: 20 jul. 2021.

MAROTO-MOLINA, Francisco et al. A low-cost IoT-based system to monitor the location of a whole herd. **Sensors**, v. 19, n. 10, p. 2298, 2019. Disponível em: <<https://www.mdpi.com/1424-8220/19/10/2298>>. Acesso em: 20 jul. 2021.

MEKKI, Kais et al. Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. In: **2018 ieee international conference on pervasive computing and communications workshops (percom workshops)**. IEEE, 2018. p. 197-202. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8480255>>. Acesso em: 20 jul. 2021.

MESTER, Gyula. Rankings scientists, journals and countries using h-index. **Interdisciplinary Description of Complex Systems: INDECS**, v. 14, n. 1, p. 1-9, 2016. Disponível em: <<https://hrcak.srce.hr/152011>>. Acesso em: 20 jul. 2021.

MIKHAYLOV, Konstantin; PETAJAEJAERVI, Juha; HAENNINEN, Tuomo. Analysis of capacity and scalability of the LoRa low power wide area network technology. In: European Wireless 2016; 22th European Wireless Conference. VDE, 2016. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7499263>>. Acesso em: 20 jul. 2021.

MONDAL, Saikat et al. Blockchain inspired RFID-based information architecture for food supply chain. **IEEE Internet of Things Journal**, v. 6, n. 3, p. 5803-5813, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8674550>>. Acesso em: 20 jul. 2021.

MONDRAGON, Adrian E. Coronado; MONDRAGON, Christian E. Coronado; CORONADO, Etienne S. Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry. In: **2018 IEEE International conference on applied system invention (ICASI)**. IEEE, 2018. p. 1300-1303. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8394531>>. Acesso em: 20 jul. 2021.

NAKAMOTO, Satoshi. Bitcoin P2P e-cash paper. **Mail Archive**, 2018. Disponível em: <<https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>>. Acesso em: 20 jul. 2021.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, 2008. Disponível em: <<https://www.debr.io/article/21260.pdf>>. Acesso em: 20 jul. 2021.

NGUYEN, Trong-Dat; LEE, Sang-Won. Optimizing mongodb using multi-streamed ssd. In: **Proceedings of the 7th International Conference on Emerging Databases**. Springer, Singapore, 2018. p. 1-13. Disponível em: <https://link.springer.com/chapter/10.1007/978-981-10-6520-0_1>. Acesso em: 20 jul. 2021.

OGBODO, Emmanuel U.; DORRELL, David; ABU-MAHFOUZ, Adnan M. Cognitive radio based sensor network in smart grid: Architectures, applications and communication technologies. **IEEE Access**, v. 5, p. 19084-19098, 2017. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8026117>>. Acesso em: 20 jul. 2021.

PAHL, Claus et al. An architecture pattern for trusted orchestration in IoT edge clouds. In: **2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)**. IEEE, 2018. p. 63-70. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8364046>>. Acesso em: 20 jul. 2021.

PARK, Seongjoon; OH, Seounghwan; KIM, Hwangnam. Performance analysis of DAG-based cryptocurrency. In: 2019 IEEE International Conference on Communications workshops (ICC workshops). IEEE, 2019. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8756973>>. Acesso em: 20 jul. 2021.

PECORARO, Giovanni et al. CSI-based fingerprinting for indoor localization using LTE signals. **EURASIP Journal on Advances in Signal Processing**, v. 2018, n. 1, p. 1-18, 2018. Disponível em: <<https://link.springer.com/article/10.1186/s13634-018-0563-7>>. Acesso em: 20 jul. 2021.

PERVEZ, Huma et al. A comparative analysis of DAG-based blockchain architectures. In: **2018 12th International Conference on Open Source Systems and Technologies (ICOSST)**. IEEE, 2018. p. 27-34. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8632193>>. Acesso em: 20 jul. 2021.

POPOV, Serguei. The tangle. **White paper**, v. 1, n. 3, 2016. Disponível em: <<http://www.descriptions.com/lota.pdf>>. Acesso em: 20 jul. 2021.

POPOV, Serguei; BUCHANAN, William J. Fpc-bi: Fast probabilistic consensus within byzantine infrastructures. **Journal of Parallel and Distributed Computing**, v. 147, p. 77-86, 2021. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0743731520303634>>. Acesso em: 20 jul. 2021.

PORTER, Preston; YANG, Shuhui; XI, Xuefeng. The Design and Implementation of a RESTful IoT Service Using the MERN Stack. In: **2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW)**. IEEE,

2019. p. 140-145. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9059381>>. Acesso em: 20 jul. 2021.

POWER COMPARE. Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland Most Countries In Africa. **Power Compare**, 2019. Disponível em: <<https://www.powercompare.co.uk/bitcoin>>. Acesso em: 20 jul. 2021.

ROGOZINSKI, Gal. The official node software that runs on the IOTA Mainnet and Devnet. **Github**, 2020. Disponível em: <<https://github.com/iotaledger/iri>>. Acesso em: 20 jul. 2021.

ROSENFIELD, Meni. Analysis of hashrate-based double spending. **arXiv preprint arXiv:1402.2009**, 2014. Disponível em: <<https://arxiv.org/abs/1402.2009>>. Acesso em: 20 jul. 2021.

RUBIO-APARICIO, Jesus et al. Design and implementation of a mixed IoT LPWAN network architecture. **Sensors**, v. 19, n. 3, p. 675, 2019. Disponível em: <<https://www.mdpi.com/408106>>. Acesso em: 20 jul. 2021.

SALAH, Khaled et al. Blockchain-based soybean traceability in agricultural supply chain. **IEEE Access**, v. 7, p. 73295-73305, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8718621>>. Acesso em: 20 jul. 2021.

SALLOUHA, Hazem; CHIUMENTO, Alessandro; POLLIN, Sofie. Localization in long-range ultra narrow band IoT networks using RSSI. In: **2017 IEEE International Conference on Communications (ICC)**. IEEE, 2017. p. 1-6. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/7997195>>. Acesso em: 20 jul. 2021.

SARFRAZ, Umair et al. Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions. **Computer Networks**, v. 148, p. 361-372, 2019. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1389128618306972>>. Acesso em: 20 jul. 2021.

SCOPUS. Scopus is the largest abstract and citation database of peer-reviewed literature. **Scopus**, 2018. Disponível em: <<https://www.elsevier.com/solutions/scopus>>. Acesso em: 20 jul. 2021.

SHAFEEQ, Sehrish et al. Curbing address reuse in the iota distributed ledger: A cuckoo-filter-based approach. **IEEE Transactions on Engineering Management**, v. 67, n. 4, p. 1244-1255, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8755275>>. Acesso em: 20 jul. 2021.

SHERMAN, Alan T. et al. On the origins and variations of blockchain technologies. **IEEE Security & Privacy**, v. 17, n. 1, p. 72-77, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8674176/>>. Acesso em: 20 jul. 2021.

SIGFOX. Sigfox Coverage. **Sigfox**, 2021. Disponível em: <<https://www.sigfox.com/en/coverage>>. Acesso em: 20 jul. 2021.

SIGFOX. Radio Technology Keypoints. **Sigfox**, 2020a. Disponível em: <<https://www.sigfox.com/en/sigfox-iot-radio-technology>>. Acesso em: 20 jul. 2021.

SIGFOX. Starting your Sigfox project. **Sigfox**, 2020b. Disponível em: <<https://build.sigfox.com/sigfox>>. Acesso em: 20 jul. 2021.

SIGFOX. M2M e IoT redefinidos por meio de conectividade otimizada em termos de custo e energia. **Lafibre**, 2018. Disponível em: <https://lafibre.info/images/3g/201302_sigfox_whitepaper.pdf>. Acesso em: 20 jul. 2021.

SIIM, Janno. DAG-Based Distributed Ledgers. **Research Seminar in Cryptology**, 2018. Disponível em: <https://courses.cs.ut.ee/MTAT.07.022/2018_spring/uploads/Main/janno-report-s17-18.pdf>. Acesso em: 20 jul. 2021.

SILVANO, Wellington. O Futuro das Criptomoedas I — [Bitcoin]. **Medium**, 2019. Disponível em: <<https://medium.com/@wellisilvano/o-futuro-das-criptomoedas-introdu%C3%A7%C3%A3o-e-bitcoin-689021ae43b6>>. Acesso em: 20 jul. 2021.

SILVANO, Wellington Fernandes et al. IoT sensors integrated with the distributed protocol IOTA/Tangle: Bosch XDK110 use case. In: **2020 X Brazilian Symposium on Computing Systems Engineering (SBESC)**. IEEE, 2020. p. 1-8. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/9277865/>>. Acesso em: 20 jul. 2021.

SILVANO, Wellington Fernandes; MARCELINO, Roderval. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. **Future Generation Computer Systems**, v. 112, p. 307-319, 2020. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0167739X19329048>>. Acesso em: 20 jul. 2021.

SINHA, Rashmi Sharan; WEI, Yiqiao; HWANG, Seung-Hoon. A survey on LPWA technology: LoRa and NB-IoT. **Ict Express**, v. 3, n. 1, p. 14-21, 2017. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2405959517300061>>. Acesso em: 20 jul. 2021.

SLUIJS, C. Antwerp Start-up T-Mining Develops Blockchain Solution for Safe, Efficient Container Release. **T-mining**, 2017. Disponível em: <<https://t-mining.be/news1/2018/1/4/secure-container-relase>>. Acesso em: 20 jul. 2021.

SONG, Qianwen; GUO, Songtao; LIU, Xing; YANG, Yuanyuan. CSI amplitude fingerprinting-based NB-IoT indoor localization. **IEEE Internet of Things Journal**, v. 5, n. 3, p. 1494–1504, 2017. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8187642>>. Acesso em: 20 jul. 2021.

SØNSTEBØ, David. IOTA Development Roadmap. **Blog IOTA**, 2017. Disponível em: <<https://blog.iota.org/iota-development-roadmap-74741f37ed01>>. Acesso em: 20 jul. 2021.

STANIEC, Kamil. **Radio Interfaces in the Internet of Things Systems: Performance Studies**. Springer Nature, 2020.

SUN, Shengjing et al. Indoor air-quality data-monitoring system: Long-term monitoring benefits. **Sensors**, v. 19, n. 19, p. 4157, 2019. Disponível em: <<https://www.mdpi.com/541352>>. Acesso em: 20 jul. 2021.

TSANG, Yung Po et al. Blockchain-driven IoT for food traceability with an integrated consensus mechanism. **IEEE access**, v. 7, p. 129000-129017, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8830460>>. Acesso em: 20 jul. 2021.

WALPORT, MGCSA et al. Distributed ledger technology: Beyond blockchain. **UK Government Office for Science**, v. 1, p. 1-88, 2016. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>. Acesso em: 20 jul. 2021.

WEB OF SCIENCE. Web of Science Trust the difference. **WEB OF SCIENCE**, 2018. Disponível em: <<https://clarivate.com/products/web-of-science/>>. Acesso em: 20 jul. 2021.

WND. WND Facebook. **Facebook**, 2021. Disponível em: <https://m.facebook.com/wndbrasiliocial/?locale2=pt_BR>. Acesso em: 20 jul. 2021.

XPORE, IEEE. About IEEE Xplore Digital Library. **IEEXPLORE**, 2018. Disponível em: <<https://ieeexplore.ieee.org/xpl/aboutUs.jsp>>. Acesso em: 20 jul. 2021.

YEOW, Kimchai et al. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. **IEEE Access**, v. 6, p. 1513-1524, 2017. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8168250>>. Acesso em: 20 jul. 2021.

YUAN, Yong; WANG, Fei-Yue. Blockchain and cryptocurrencies: Model, techniques, and applications. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, v. 48, n. 9, p. 1421-1428, 2018. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8419306>>. Acesso em: 20 jul. 2021.

ZHENG, Xiaochen et al. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. **Journal of medical Internet research**, v. 21, n. 6, p. e13583, 2019a. Disponível em: <<https://www.jmir.org/2019/6/e13583>>. Acesso em: 20 jul. 2021.

ZHENG, Xiaochen et al. Activity-aware essential tremor evaluation using deep learning method based on acceleration data. **Parkinsonism & related disorders**, v. 58, p. 17-22, 2019b. Disponível em: <<https://www.jmir.org/2019/6/e13583>>. Acesso em: 20 jul. 2021.

APÊNDICE A – TABELA DE LOCALIZAÇÃO - VIAGEM 1

Data e Hora	Latitude	Longitude	Raio (m)
09/04/2021 13:58:34	-28.941261	-49.49532448	66
09/04/2021 14:08:34	-28.9410586	-49.49549284	87
09/04/2021 14:18:34	-28.941261	-49.49532448	66
09/04/2021 14:48:34	-28.9412633	-49.49532388	67
09/04/2021 14:58:34	-28.9412606	-49.49533939	87
09/04/2021 15:08:34	-28.9412633	-49.49532388	68
09/04/2021 15:18:34	-28.9412633	-49.49532388	67
09/04/2021 15:28:34	-28.9411345	-49.4954028	68
09/04/2021 15:38:34	-28.945113	-49.49107777	82
09/04/2021 15:48:34	-28.945113	-49.49107777	82
09/04/2021 15:58:34	-28.9452866	-49.49132	96
09/04/2021 16:18:34	-28.9347376	-49.48477233	123
09/04/2021 16:28:34	-28.9346588	-49.48472322	168
09/04/2021 16:38:34	-28.9344288	-49.48356474	179
09/04/2021 16:48:34	-28.9344443	-49.48501898	78
09/04/2021 16:58:33	-28.9361735	-49.48298507	120
09/04/2021 17:38:33	-28.6822722	-49.38505736	58
09/04/2021 21:38:33	-27.576069	-48.61474422	202
09/04/2021 21:58:33	-27.5766501	-48.61414438	112
09/04/2021 22:08:33	-27.5777112	-48.61448093	121
09/04/2021 22:18:33	-27.5747941	-48.61361851	106
09/04/2021 22:28:33	-27.5747941	-48.61361851	106
09/04/2021 22:38:33	-27.576069	-48.61474422	202
09/04/2021 23:08:33	-27.576069	-48.61474422	202
10/04/2021 00:08:32	-27.5754331	-48.61391827	91
10/04/2021 00:28:32	-27.5754331	-48.61391827	91

10/04/2021 01:48:32	-27.5754331	-48.61391827	91
10/04/2021 03:18:32	-27.5754331	-48.61391827	91
10/04/2021 03:28:32	-27.5754331	-48.61391827	91
10/04/2021 04:58:35	-27.5754331	-48.61391827	91
10/04/2021 05:28:35	-27.5747941	-48.61361851	106
10/04/2021 05:38:35	-27.5752035	-48.61474951	90
10/04/2021 05:48:35	-27.5752035	-48.61474951	90
10/04/2021 06:38:31	-27.5747508	-48.6136647	113
10/04/2021 09:38:31	-27.5754331	-48.61391827	91
10/04/2021 11:28:29	-27.5754331	-48.61391827	91
10/04/2021 11:38:29	-27.5747508	-48.61366474	113
10/04/2021 11:48:29	-27.5747508	-48.61366474	113
10/04/2021 11:48:29	-27.5747508	-48.61366474	113
10/04/2021 11:58:29	-27.5754331	-48.61391827	91
10/04/2021 12:08:29	-27.5754331	-48.61391827	91
10/04/2021 12:18:29	-27.5754331	-48.61391827	91
10/04/2021 12:48:29	-27.5747508	-48.61366474	113
10/04/2021 12:58:29	-27.576069	-48.61474422	202
10/04/2021 13:08:35	-27.576069	-48.61474422	202
10/04/2021 13:18:35	-27.576069	-48.61474422	202
10/04/2021 13:28:35	-27.576069	-48.61474422	202
10/04/2021 13:38:35	-27.576069	-48.61474422	202
10/04/2021 13:48:35	-27.576069	-48.61474422	202
10/04/2021 13:58:35	-27.576069	-48.61474422	202
10/04/2021 14:18:35	-27.576069	-48.61474422	202
10/04/2021 14:28:35	-27.576069	-48.61474422	202
10/04/2021 14:38:35	-27.576069	-48.61474422	202

10/04/2021 14:48:35	-27.576069	-48.61474422	202
10/04/2021 14:58:35	-27.576069	-48.61474422	202
10/04/2021 15:08:34	-27.576069	-48.61474422	202
10/04/2021 15:18:34	-27.576069	-48.61474422	202
10/04/2021 15:28:34	-27.576069	-48.61474422	202
10/04/2021 15:38:34	-27.576069	-48.61474422	202
11/04/2021 08:28:31	-23.3483546	-46.86129052	250
11/04/2021 08:38:31	-23.3481898	-46.8609223	250
11/04/2021 08:48:31	-23.3482364	-46.86122262	234
11/04/2021 08:58:31	-23.3486694	-46.86214759	220
11/04/2021 09:08:31	-23.3485556	-46.86197638	185
11/04/2021 09:18:31	-23.3482862	-46.86129016	250
11/04/2021 09:28:31	-23.3482555	-46.86093431	250
11/04/2021 09:38:31	-23.3487058	-46.86195692	190
11/04/2021 09:58:31	-23.3483261	-46.86143186	247
11/04/2021 10:08:31	-23.3482364	-46.86122262	234
11/04/2021 10:28:31	-23.3481898	-46.8609223	250
11/04/2021 10:38:31	-23.3482555	-46.86093431	250
11/04/2021 10:48:31	-23.3482043	-46.86097057	250
11/04/2021 11:08:30	-23.3483261	-46.86143186	247
11/04/2021 11:18:30	-23.3486138	-46.8618225,	184
11/04/2021 12:08:30	-23.3483261	-46.86143186	247
11/04/2021 12:18:30	-23.3483546,	-46.86129052	250
11/04/2021 12:38:30	-23.3483261	-46.86143186	247
11/04/2021 12:48:30	-23.3485789	-46.86187453	167
11/04/2021 12:58:30	-23.3482862	-46.86143403	249
11/04/2021 13:18:30	-23.3483546	-46.86129052	250

11/04/2021 15:18:30	-23.3482862	-46.86129016	250
11/04/2021 15:28:30	-23.3483546	-46.86129052	250
11/04/2021 15:38:30	-23.3483546	-46.86129052	250
11/04/2021 15:48:30	-23.3483261	-46.86143186	247
11/04/2021 15:58:30	-23.3483261	-46.86143186	247
11/04/2021 16:08:30	-23.3482862	-46.86129016	250
11/04/2021 16:18:30	-23.3483261	-46.86143186	247
11/04/2021 16:28:30	-23.3483694	-46.86130285	250
11/04/2021 16:38:30	-23.3483546	-46.86129052	250
11/04/2021 16:48:30	-23.3482862	-46.86143403	249
11/04/2021 16:58:30	-23.3482862	-46.86143403	249
11/04/2021 17:08:30	-23.3483546	-46.86129052	250
11/04/2021 17:18:30	-23.3483694	-46.86130285	250
11/04/2021 17:28:30	-23.3482862	-46.86129016	250
11/04/2021 17:38:30	-23.3483546	-46.86129052	250
11/04/2021 17:48:30	-23.3482862	-46.86093807	171
12/04/2021 00:28:28	-22.310092	-49.02729257	71
12/04/2021 00:38:28	-22.3100929	-49.02729257	71
12/04/2021 00:48:28	-22.3100929	-49.02729257	71
12/04/2021 00:58:28	-22.3100929	-49.02729257	71
12/04/2021 01:08:28	-22.3100929	-49.02729257	71
12/04/2021 01:18:28	-22.3100929	-49.02729257	71
12/04/2021 01:28:28	-22.3100929	-49.02729257	71
12/04/2021 01:38:28	-22.3100929	-49.02729257	71
12/04/2021 01:48:28	-22.3100929	-49.02729257	71
12/04/2021 01:58:28	-22.3100929	-49.02729257	71
12/04/2021 02:08:27	-22.3100929	-49.02729257	71

12/04/2021 02:18:27	-22.3100929	-49.02729257	71
12/04/2021 02:28:27	-22.3100929	-49.02729257	71
12/04/2021 02:38:27	-22.3100929	-49.02729257	71
12/04/2021 02:48:27	-22.3100929	-49.02729257	71
12/04/2021 02:58:27	-22.3100929	-49.02729257	71
12/04/2021 03:08:27	-22.3100929	-49.02729257	71
12/04/2021 03:18:27	-22.3100929	-49.02729257	71
12/04/2021 03:28:27	-22.3100929	-49.02729257	71
12/04/2021 03:38:27	-22.3100929	-49.02729257	71
12/04/2021 03:48:27	-22.3100929	-49.02729257	71
12/04/2021 03:58:27	-22.3100929	-49.02729257	71
12/04/2021 04:08:27	-22.3100929	-49.02729257	71
12/04/2021 04:18:27	-22.3100929	-49.02729257	71
12/04/2021 04:28:27	-22.3100929	-49.02729257	71
12/04/2021 04:38:27	-22.3100929	-49.02729257	71
12/04/2021 04:48:27	-22.3100929	-49.02729257	71
12/04/2021 04:58:27	-22.3100929	-49.02729257	71
12/04/2021 05:08:27	-22.3100929	-49.02729257	71
12/04/2021 05:18:27	-22.3100929	-49.02729257	71
12/04/2021 05:28:27	-22.3100929	-49.02729257	71
12/04/2021 05:38:27	-22.3100929	-49.02729257	71
12/04/2021 05:48:27	-22.3100929	-49.02729257	71
12/04/2021 05:58:27	-22.3100929	-49.02729257	71
12/04/2021 07:08:27	-22.3262186	-49.09628013	99
12/04/2021 07:38:27	-22.3261729	-49.0962317	97
12/04/2021 07:48:27	-22.3250802	-49.09578775	250
12/04/2021 08:08:27	-22.3250802	-49.09578775	250

12/04/2021 08:18:27	-22.3250802	-49.09578775	250
12/04/2021 08:58:27	-22.3250802	-49.09578775	250
12/04/2021 09:08:27	-22.3262186	-49.09628013	99
12/04/2021 09:28:27	-22.3261729	-49.0962317,	97
12/04/2021 09:38:27	-22.3266237	-49.0967388	71
12/04/2021 09:48:27	-22.3262186	-49.09628013	99

APÊNDICE B – TABELA DE TEMPERATURA - VIAGEM 1

Data e Hora	Temperatura (°C)	Data e Hora	Temperatura (°C)
09/04/2021 13:08:29	26.9	10/04/2021 20:48:25	27.5
09/04/2021 13:18:29	26.9	10/04/2021 20:58:25	27.3
09/04/2021 13:28:29	26.9	10/04/2021 21:08:25	27.1
09/04/2021 13:38:29	27	10/04/2021 21:18:25	26.9
09/04/2021 13:48:29	27	10/04/2021 21:28:25	26.7
09/04/2021 13:58:29	27.3	10/04/2021 21:38:25	26.5
09/04/2021 14:08:29	27.4	10/04/2021 21:48:25	26.3
09/04/2021 14:18:29	27.6	10/04/2021 21:58:25	26.1
09/04/2021 14:28:29	28	10/04/2021 22:08:25	26
09/04/2021 14:38:29	28.4	10/04/2021 22:18:25	25.8
09/04/2021 14:48:28	28.3	10/04/2021 22:28:25	25.5
09/04/2021 14:58:28	28.3	10/04/2021 22:38:25	25.3
09/04/2021 15:08:28	28.7	10/04/2021 22:48:25	25.1
09/04/2021 15:18:28	28.5	10/04/2021 22:58:25	24.9
09/04/2021 15:28:28	28.9	10/04/2021 23:08:25	24.8
09/04/2021 15:38:28	30.8	10/04/2021 23:18:25	24.6
09/04/2021 15:48:28	31.5	10/04/2021 23:28:25	24.4
09/04/2021 15:58:28	31	10/04/2021 23:38:25	24.3
09/04/2021 16:08:28	30.8	10/04/2021 23:48:25	24.1
09/04/2021 16:18:28	30.8	10/04/2021 23:58:25	23.9
09/04/2021 16:28:28	30.8	11/04/2021 00:08:35	23.8
09/04/2021 16:38:28	30.6	11/04/2021 00:18:35	23.6
09/04/2021 16:58:28	30.3	11/04/2021 00:38:35	23.3
09/04/2021 17:08:28	30.1	11/04/2021 00:48:35	23.2
09/04/2021 17:18:28	30.1	11/04/2021 00:58:35	23
09/04/2021 17:28:28	30.1	11/04/2021 01:08:35	22.9

09/04/2021 17:38:28	30.1	11/04/2021 01:18:35	22.8
09/04/2021 17:48:28	30.1	11/04/2021 01:28:35	22.6
09/04/2021 17:58:28	30.1	11/04/2021 01:38:35	22.5
09/04/2021 18:08:27	30.1	11/04/2021 01:48:35	22.3
09/04/2021 18:18:27	30.1	11/04/2021 01:58:35	22.2
09/04/2021 18:38:27	30	11/04/2021 02:08:25	22
09/04/2021 18:48:27	30	11/04/2021 02:18:25	21.9
09/04/2021 18:58:27	29.9	11/04/2021 02:28:25	21.7
09/04/2021 19:08:27	29.9	11/04/2021 02:38:25	21.6
09/04/2021 19:18:27	29.9	11/04/2021 02:48:25	21.5
09/04/2021 19:28:27	29.8	11/04/2021 02:58:25	21.3
09/04/2021 19:38:27	29.8	11/04/2021 03:08:25	21.2
09/04/2021 19:48:27	29.7	11/04/2021 03:18:25	21.1
09/04/2021 19:58:27	29.7	11/04/2021 03:28:25	21
09/04/2021 20:08:27	29.6	11/04/2021 03:38:25	21
09/04/2021 20:18:27	29.5	11/04/2021 03:38:25	20.9
09/04/2021 20:28:27	29.4	11/04/2021 03:58:25	20.7
09/04/2021 20:38:27	29.4	11/04/2021 04:08:25	20.7
09/04/2021 20:48:27	29.3	11/04/2021 04:18:25	20.7
09/04/2021 20:58:27	29.2	11/04/2021 04:28:25	20.6
09/04/2021 22:08:27	28.8	11/04/2021 04:38:25	20.6
09/04/2021 22:18:27	28.7	11/04/2021 04:48:25	20.5
09/04/2021 22:28:27	28.7	11/04/2021 04:58:25	20.5
09/04/2021 22:38:27	28.6	11/04/2021 05:08:25	20.4
09/04/2021 22:48:27	28.4	11/04/2021 05:18:25	20.4
09/04/2021 22:58:27	28.1	11/04/2021 05:28:25	20.5
09/04/2021 23:08:27	27.9	11/04/2021 05:38:25	20.5

09/04/2021 23:18:27	27.7	11/04/2021 05:48:25	20.6
09/04/2021 23:28:27	27.5	11/04/2021 05:58:25	20.7
09/04/2021 23:38:27	27.4	11/04/2021 07:08:25	21.4
09/04/2021 23:48:27	27.3	11/04/2021 07:18:25	21.4
09/04/2021 23:58:27	27.1	11/04/2021 07:28:25	21.3
10/04/2021 00:08:27	27.1	11/04/2021 07:38:25	21.2
10/04/2021 00:18:27	27	11/04/2021 07:48:25	21.1
10/04/2021 00:28:27	27	11/04/2021 07:58:25	21.1
10/04/2021 00:38:27	26.9	11/04/2021 10:08:25	21.5
10/04/2021 00:48:26	26.8	11/04/2021 10:18:25	21.5
10/04/2021 00:58:26	26.8	11/04/2021 10:28:25	21.6
10/04/2021 01:08:26	26.8	11/04/2021 10:38:25	21.6
10/04/2021 01:18:26	26	11/04/2021 10:48:25	21.7
10/04/2021 01:28:26	26	11/04/2021 10:58:25	21.8
10/04/2021 01:38:26	26	11/04/2021 11:08:24	21.9
10/04/2021 01:48:26	26	11/04/2021 11:18:24	22
10/04/2021 01:58:26	26.6	11/04/2021 11:28:24	22
10/04/2021 02:08:26	26.6	11/04/2021 11:38:24	22.1
10/04/2021 02:18:26	26.6	11/04/2021 11:48:24	22.2
10/04/2021 02:28:26	26.6	11/04/2021 11:58:24	22.3
10/04/2021 02:38:26	26.5	11/04/2021 12:08:24	22.4
10/04/2021 02:48:26	26.5	11/04/2021 12:18:24	22.5
10/04/2021 02:58:26	26.5	11/04/2021 12:28:24	22.6
10/04/2021 03:08:26	26.5	11/04/2021 12:38:24	22.7
10/04/2021 03:18:26	26.5	11/04/2021 12:48:24	22.8
10/04/2021 03:28:26	26.4	11/04/2021 12:58:24	22.9
10/04/2021 03:38:26	26.4	11/04/2021 13:08:24	23

10/04/2021 03:48:26	26.4	11/04/2021 13:18:24	23.1
10/04/2021 03:58:26	26.3	11/04/2021 13:28:24	23.2
10/04/2021 04:08:26	26.3	11/04/2021 13:38:24	23.2
10/04/2021 04:18:26	26.2	11/04/2021 13:48:24	23.3
10/04/2021 04:28:26	26.2	11/04/2021 13:58:24	23.4
10/04/2021 04:38:26	26.1	11/04/2021 14:08:24	23.5
10/04/2021 04:48:26	26.1	11/04/2021 14:18:24	23.6
10/04/2021 04:58:26	26	11/04/2021 14:28:24	23.6
10/04/2021 05:08:26	26.1	11/04/2021 14:38:24	23.7
10/04/2021 05:18:26	26	11/04/2021 14:48:24	23.8
10/04/2021 05:28:26	26	11/04/2021 14:58:24	23.9
10/04/2021 05:38:26	26	11/04/2021 15:08:23	23.9
10/04/2021 05:48:26	25.8	11/04/2021 15:18:23	24
10/04/2021 05:58:26	25.6	11/04/2021 15:28:23	24.1
10/04/2021 06:08:25	25.4	11/04/2021 15:38:23	24.1
10/04/2021 06:18:25	25.2	11/04/2021 15:48:23	24.2
10/04/2021 06:28:25	25.1	11/04/2021 15:58:23	24.3
10/04/2021 06:38:25	25.1	11/04/2021 16:08:23	24.4
10/04/2021 06:48:25	25.1	11/04/2021 16:18:23	24.4
10/04/2021 06:58:25	25.1	11/04/2021 16:28:23	24.4
10/04/2021 07:08:24	25.1	11/04/2021 16:38:23	24.5
10/04/2021 07:18:24	25.1	11/04/2021 16:48:23	24.5
10/04/2021 07:28:24	25.1	11/04/2021 16:58:23	24.5
10/04/2021 08:08:24	25	11/04/2021 17:38:25	24.6
10/04/2021 08:18:24	25	11/04/2021 17:48:25	24.6
10/04/2021 08:28:24	24.9	11/04/2021 17:58:25	24.6
10/04/2021 08:38:24	24.9	11/04/2021 22:08:22	24.3

10/04/2021 08:48:24	24.9	11/04/2021 22:18:22	24.2
10/04/2021 08:58:24	24.8	11/04/2021 22:28:22	24.2
10/04/2021 09:08:24	24.8	11/04/2021 22:38:22	24.2
10/04/2021 09:18:24	24.8	11/04/2021 22:48:22	24.1
10/04/2021 09:28:24	24.7	11/04/2021 22:58:22	24.1
10/04/2021 09:38:24	24.7	11/04/2021 23:08:22	24
10/04/2021 09:48:24	24.7	11/04/2021 23:18:22	24
10/04/2021 09:58:24	24.7	11/04/2021 23:28:22	24
10/04/2021 10:08:24	24.7	11/04/2021 23:38:22	23.9
10/04/2021 10:18:24	24.7	11/04/2021 23:48:22	23.9
10/04/2021 10:28:24	24.6	11/04/2021 23:58:22	23.8
10/04/2021 10:38:24	24.6	12/04/2021 00:08:22	23.8
10/04/2021 10:48:24	24.6	12/04/2021 00:18:22	23.8
10/04/2021 10:58:24	24.6	12/04/2021 00:28:22	23.7
10/04/2021 11:08:24	24.6	12/04/2021 00:38:22	23.7
10/04/2021 11:18:24	24.6	12/04/2021 00:48:22	23.6
10/04/2021 11:28:24	24.6	12/04/2021 00:58:22	23.6
10/04/2021 11:38:24	24.6	12/04/2021 01:08:22	23.6
10/04/2021 11:48:24	24.6	12/04/2021 01:18:22	23.7
10/04/2021 11:58:24	24.6	12/04/2021 01:28:22	24
10/04/2021 12:08:24	24.7	12/04/2021 01:38:22	24.2
10/04/2021 12:18:29	24.7	12/04/2021 01:48:22	24.4
10/04/2021 12:28:29	24.7	12/04/2021 01:58:22	24.5
10/04/2021 12:38:29	24.7	12/04/2021 02:08:22	24.6
10/04/2021 12:48:29	24.7	12/04/2021 02:18:21	24.6
10/04/2021 12:58:29	24.8	12/04/2021 02:28:21	24.6
10/04/2021 13:08:29	25.2	12/04/2021 02:38:21	24.6

10/04/2021 13:18:29	25.4	12/04/2021 02:48:21	24.5
10/04/2021 13:28:29	25.5	12/04/2021 02:58:21	24.4
10/04/2021 13:38:29	25.5	12/04/2021 03:08:21	24.4
10/04/2021 13:48:29	25.5	12/04/2021 03:18:21	24.3
10/04/2021 13:58:29	25.5	12/04/2021 03:28:21	24.3
10/04/2021 14:08:29	25.6	12/04/2021 03:38:21	24.2
10/04/2021 14:18:28	25.6	12/04/2021 03:48:21	24.2
10/04/2021 14:28:28	25.6	12/04/2021 03:58:21	24.2
10/04/2021 14:38:28	25.6	12/04/2021 04:08:21	24.2
10/04/2021 14:48:28	25.6	12/04/2021 04:18:21	24.1
10/04/2021 14:58:28	25.6	12/04/2021 04:28:21	24
10/04/2021 15:08:28	25.6	12/04/2021 04:38:21	23.8
10/04/2021 15:18:28	25.6	12/04/2021 04:48:21	23.7
10/04/2021 15:28:28	25.6	12/04/2021 04:58:21	23.5
10/04/2021 15:38:28	25.6	12/04/2021 05:08:21	23.4
10/04/2021 15:48:28	25.8	12/04/2021 05:18:21	23.3
10/04/2021 15:58:28	26	12/04/2021 05:28:21	23.2
10/04/2021 16:08:25	26.4	12/04/2021 05:38:21	23.1
10/04/2021 16:18:25	26.6	12/04/2021 05:48:21	23.1
10/04/2021 16:28:25	26.8	12/04/2021 05:58:21	23
10/04/2021 16:38:25	27.1	12/04/2021 06:08:21	22.9
10/04/2021 16:48:25	27.4	12/04/2021 06:18:21	22.8
10/04/2021 16:58:25	27.7	12/04/2021 06:28:21	22.6
10/04/2021 17:08:25	27.9	12/04/2021 06:38:20	22.5
10/04/2021 17:18:25	28.2	12/04/2021 06:48:20	22.4
10/04/2021 17:28:25	28.4	12/04/2021 06:58:20	22.4
10/04/2021 17:38:25	28.6	12/04/2021 07:08:20	22.8

10/04/2021 17:48:25	28.7	12/04/2021 07:18:20	23.1
10/04/2021 17:58:25	28.8	12/04/2021 07:28:20	23.3
10/04/2021 18:08:25	28.9	12/04/2021 07:38:20	23.5
10/04/2021 18:18:25	28.9	12/04/2021 07:48:20	23.7
10/04/2021 18:28:25	29	12/04/2021 07:58:20	23.8
10/04/2021 18:38:25	29	12/04/2021 08:08:20	23.8
10/04/2021 18:48:25	29	12/04/2021 08:18:20	23.8
10/04/2021 18:58:25	29.1	12/04/2021 08:28:20	24.1
10/04/2021 19:08:25	29.1	12/04/2021 08:38:20	24.3
10/04/2021 19:18:25	29.1	12/04/2021 08:48:20	24.4
10/04/2021 19:28:25	29	12/04/2021 08:58:20	24.5
10/04/2021 19:38:25	28.9	12/04/2021 09:08:20	24.5
10/04/2021 19:48:25	28.7	12/04/2021 09:18:20	24.6
10/04/2021 19:58:25	28.5	12/04/2021 09:28:20	24.6
10/04/2021 20:08:25	28.3	12/04/2021 09:38:20	24.8
10/04/2021 20:18:25	28.1	12/04/2021 09:48:20	24.8
10/04/2021 20:28:25	27.9	12/04/2021 09:58:20	25
10/04/2021 20:38:25	27.7	--	--

APÊNDICE C – TABELA DE LOCALIZAÇÃO - VIAGEM 2

Data e Hora	Latitude	Longitude	Raio (m)
13/04/2021 01:58:12	-22.3426171	-49.08840661	108
13/04/2021 02:28:12	-22.3186114	-49.04978312	93
13/04/2021 04:28:12	-21.3675056	-50.28371356	65
13/04/2021 04:58:12	21.2127173	-50.42791367	101
13/04/2021 05:18:12	-21.2045345	-50.51406651	114
13/04/2021 05:28:12	-21.2045345	-50.51406651	114
13/04/2021 05:38:12	-21.2045345	-50.51406651	114
13/04/2021 05:48:12	-21.2045345	-50.51406651	114
13/04/2021 05:58:12	-21.2045345	-50.51406651	114
13/04/2021 06:08:12	-21.2045345	-50.51406651	114
13/04/2021 06:18:12	-21.2045345	-50.51406651	114
13/04/2021 06:28:12	-21.2045345	-50.51406651	114
13/04/2021 06:38:12	-21.2242434	-50.45448451	56
13/04/2021 06:48:12	-21.0480452	-49.37897668	90
13/04/2021 09:38:12	-20.7976711	-49.36772442	49
13/04/2021 09:48:12	-20.8176549	-49.38175672	61
13/04/2021 10:08:12	-20.8220284	-49.38424157	75
13/04/2021 10:18:12	-20.8066587	-49.37681191	124
13/04/2021 10:38:12	-20.8219274	-49.37781725	89
13/04/2021 10:58:12	-20.8239619	-49.40149454	78

APÊNDICE D – TABELA DE TEMPERATURA - VIAGEM 2

Data e Hora	Temperatura (°C)	Data e Hora	Temperatura (°C)
13/04/2021 00:08:16	27.5	13/04/2021 05:18:15	26.8
13/04/2021 00:18:16	27.5	13/04/2021 05:28:15	26.6
13/04/2021 00:28:16	27.5	13/04/2021 05:38:15	26.5
13/04/2021 00:38:16	27.5	13/04/2021 05:48:15	26.5
13/04/2021 00:48:16	27.5	13/04/2021 05:58:15	26.6
13/04/2021 00:58:16	27.5	13/04/2021 06:08:14	26.7
13/04/2021 01:08:16	27.5	13/04/2021 06:18:14	26.8
13/04/2021 01:18:16	27.5	13/04/2021 06:28:14	26.8
13/04/2021 01:28:16	27.5	13/04/2021 06:38:14	26.8
13/04/2021 01:38:16	27.5	13/04/2021 06:48:14	26.9
13/04/2021 01:48:16	27.5	13/04/2021 06:58:14	26.9
13/04/2021 01:58:16	27.5	13/04/2021 07:08:14	27
13/04/2021 02:08:14	27.7	13/04/2021 07:18:14	27.1
13/04/2021 02:18:14	27.6	13/04/2021 07:28:14	27.1
13/04/2021 02:28:14	27.3	13/04/2021 07:38:14	27.2
13/04/2021 02:38:14	27.1	13/04/2021 07:48:14	27.3
13/04/2021 02:48:14	27	13/04/2021 07:58:14	27.4
13/04/2021 02:58:14	27	13/04/2021 08:08:14	27.6
13/04/2021 03:08:14	27	13/04/2021 08:18:14	27.8
13/04/2021 03:18:14	27	13/04/2021 08:28:14	28
13/04/2021 03:28:14	27.1	13/04/2021 08:38:14	28.1
13/04/2021 03:48:14	27.2	13/04/2021 08:48:14	28.3
13/04/2021 03:58:14	27.3	13/04/2021 08:58:14	28.5
13/04/2021 04:08:15	27.3	13/04/2021 09:08:14	28.7
13/04/2021 04:18:15	27.3	13/04/2021 09:18:14	28.9
13/04/2021 04:28:15	27.3	13/04/2021 09:28:14	29

13/04/2021 04:38:15	27.3	13/04/2021 09:38:14	29.2
13/04/2021 04:48:15	27.3	13/04/2021 09:48:14	29.4
13/04/2021 04:58:15	27.3	13/04/2021 09:58:14	29.7
13/04/2021 05:08:15	27.1	--	--