

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ
PRÓ-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Washington Luiz de Lima Praxedes Filho

**Uma proposta de framework de blockchain em Internet das Coisas
com dados de geolocalização**

Fortaleza – CE

1 de setembro de 2026

Washington Luiz de Lima Praxedes Filho

Uma proposta de framework de blockchain em Internet das Coisas com dados de geolocalização

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia do Ceará, como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Linha de Pesquisa: Internet das Coisas e Software Distribuído

Orientador: Prof. Dr. Cidcley Teixeira de Souza

Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação (PRPI)

Programa de Pós-Graduação em Ciência da Computação (PPGCC)

Fortaleza – CE

1 de setembro de 2026

Dados Internacionais de Catalogação na Publicação
Instituto Federal do Ceará - IFCE
Sistema de Bibliotecas - SIBI
Ficha catalográfica elaborada pelo SIBI/IFCE, com os dados fornecidos pelo(a) autor(a)

P919p Praxedes Filho, Washington Luiz de Lima.
Uma proposta de framework de blockchain em internet das coisas com dados de geolocalização / Washington Luiz de Lima Praxedes Filho. - 2026.
80 f. : il. color.

Dissertação (Mestrado) – Instituto Federal do Ceará, Mestrado em Ciência da Computação, Campus Fortaleza, 2026.
Orientação: Prof. Dr. Cidcley Teixeira de Souza.

1. Blockchain. 2. Internet das coisas. I. Título.

CDD 004



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ
Av. 13 de maio, 2081 - Bairro Benfica - CEP 60040-531 - Fortaleza - CE - www.ifce.edu.br

FOLHA DE APROVAÇÃO

Processo: 23256.000529/2026-74

Interessado: Washington Luiz de Lima Praxedes Filho

WASHINGTON LUIZ DE LIMA PRAXEDES FILHO

"Uma proposta de framework de blockchain em Internet das Coisas com dados de geolocalização"

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE) *Campus* de Fortaleza, como requisito parcial para obtenção do Título de Mestre em Ciência da Computação.

Aprovada em: **24/02/2026**.

BANCA EXAMINADORA

Prof. Dr. Cidley Teixeira de Souza (Orientador)

Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

Prof. Dr. Carlos Henrique Leitão Cavalcante

Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

Profa. Dra. Atslands Rego da Rocha

Universidade Federal do Ceará - UFC



Documento assinado eletronicamente por **Atslands Rego da Rocha, Usuário Externo**, em 24/02/2026, às 18:41, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Cidley Teixeira de Souza, Professor do Ensino Básico, Técnico e Tecnológico**, em 24/02/2026, às 19:58, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Carlos Henrique Leitao Cavalcante, Professor do Ensino Básico, Técnico e Tecnológico**, em 25/02/2026, às 23:08, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade do documento pode ser conferida no site https://sei.ifce.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **8365987** e o código CRC **ADA8186F**.

Dedico este trabalho à minha família, pelo apoio, incentivo e compreensão ao longo de toda esta caminhada.

A todos que estiveram ao meu lado nos momentos de desafio e de conquista, contribuindo, de diferentes formas, para que eu pudesse chegar até aqui.

E, especialmente, àqueles que sempre acreditaram em mim e me ensinaram que dedicação, persistência e conhecimento são capazes de transformar caminhos.

Agradecimentos

Essa jornada rumo ao título de mestre tem mérito das pessoas mais importantes para mim: minha esposa, Bárbara, e minha família. Sem elas, eu não teria a base necessária para chegar neste lugar. Agradeço ao meu orientador, Prof. Cidcley, que me guiou durante o programa e insistiu em minha trajetória, diante de todos os percalços e dificuldades pelas quais passamos; aos docentes e servidores do Programa de Pós Graduação em Ciência da Computação, que deixaram marcas definitivas na minha formação; ao Instituto Federal, por dar o recurso necessário para eu desenvolver minha pesquisa e evoluir na Ciência da Computação.

“A ciência é mais do que um corpo de conhecimento; é uma maneira de pensar.”
(Carl Sagan)

Resumo

As aplicações de Internet das Coisas têm obtido notoriedade nos últimos anos, em especial aquelas voltadas ao tratamento de dados de geolocalização, como captura, monitoramento, rastreamento e roteirização; contudo, a natureza centralizada dessas arquiteturas, aliada a vulnerabilidades de segurança, desafios de escalabilidade e às limitações computacionais dos dispositivos, impõe restrições ao desenvolvimento de soluções confiáveis para esse domínio. Nesse contexto, a tecnologia de blockchain tem sido investigada como alternativa para o tratamento seguro e auditável dessas informações. Este trabalho apresenta um framework baseado em blockchain, com execução de nós na borda da rede, voltado a aplicações de Internet das Coisas que lidam com dados de geolocalização, no qual, a partir de uma revisão da literatura, são discutidas contribuições relacionadas à integração entre IoT e blockchain e os desafios associados à performance, à segurança, à integridade e à privacidade dos dados. O framework proposto é avaliado experimentalmente considerando diferentes abordagens de execução, métricas de desempenho e casos de teste relacionados às propriedades de segurança e privacidade analisadas. Os resultados obtidos permitem discutir a viabilidade da abordagem proposta e os impactos da proximidade computacional no uso de blockchain para aplicações baseadas em geolocalização, fornecendo subsídios para a adoção de frameworks mais adequadas a esse tipo de cenário.

Palavras-chave: Internet da Coisas. Blockchain. Geolocalização.

Abstract

Internet of Things applications have gained increasing attention in recent years, particularly those focused on the handling of geolocation data, such as data collection, monitoring, tracking, and routing; however, the centralized nature of these architectures, combined with security vulnerabilities, scalability challenges, and the limited computational resources of devices, imposes constraints on the development of reliable solutions in this domain. In this context, blockchain technology has been investigated as an alternative for the secure and auditable handling of such information. This work presents a blockchain-based framework, with nodes executed at the network edge, aimed at Internet of Things applications that handle geolocation data, in which, based on a literature review, contributions related to the integration of IoT and blockchain are discussed, as well as challenges associated with performance, security, data integrity, and privacy. The proposed framework is experimentally evaluated considering different execution approaches, performance metrics, and test cases related to the analyzed security and privacy properties. The obtained results allow for a discussion on the feasibility of the proposed approach and the impacts of computational proximity on the use of blockchain for location-based applications, providing insights to support the adoption of more appropriate architectures for this type of scenario.

Keywords: Internet of things. Geolocation. Blockchain

Lista de Figuras

Figura 1 – Distribuição de trabalhos nos repositórios buscados. FONTE: o próprios autores.	30
Figura 2 – Resultado da análise dos trabalhos buscados nos repositórios indicados. FONTE: os próprios autores.	31
Figura 3 – Exemplo de uma blockchain simplificada.	38
Figura 4 – Exemplo de uma blockchain simplificada.	39
Figura 5 – Fluxograma de autenticação e armazenamento de dados de geolocalização no Framework proposto.	42
Figura 6 – Proposta de framework com duas instâncias de blockchain para registrar dados de geolocalização.	43
Figura 7 – Visão comparativa dos cenários experimentais avaliados.	49
Figura 8 – Evolução do throughput (TPS) nas abordagens avaliadas.	57
Figura 9 – Evidência dos registros de autenticação no <i>smart contract</i>	60
Figura 10 – <i>log</i> do registro de ancoragem do estado da blockchain na borda, para garantir a integridade dos dados registrados.	61

Lista de Tabelas

Tabela 1	–	Estruturação do protocolo de busca	28
Tabela 2	–	Termos-chave considerados na etapa de triagem	29
Tabela 3	–	Síntese dos aspectos tratados pelos trabalhos relacionados e pelo framework proposto	31
Tabela 4	–	Pilares e propriedades de segurança endereçados pelo framework	43
Tabela 5	–	Resumo dos cenários experimentais avaliados	48
Tabela 6	–	Tecnologias e ferramentas utilizadas na implementação experimental	53
Tabela 7	–	Comparação dos resultados de desempenho entre blockchain na borda e blockchain na nuvem	56
Tabela 8	–	Coefficiente de variação do tempo de resposta nas últimas cinco rodadas válidas	56
Tabela 9	–	Registros de geolocalização com rotação de <i>pseudoId</i> a cada 10 registros	62
Tabela 10	–	Resultado da seleção de trabalhos a partir dos Critérios de Qualidade	80

Lista de Algoritmos

1	Geração de pseudônimo rotativo (<i>pseudoId</i>)	61
---	--	----

Sumário

1	INTRODUÇÃO	23
1.1	Motivação para a Dissertação	23
1.2	Descrição do problema	24
1.3	Objetivos Geral e Específicos	24
1.4	Estrutura da Dissertação	25
2	TRABALHOS RELACIONADOS	27
2.1	Metodologia da Revisão Sistemática	27
2.1.1	Questões de Pesquisa	27
2.1.2	Protocolo de Busca	27
2.1.3	Critérios de Inclusão e Exclusão	28
2.1.3.1	Critérios de Inclusão	28
2.1.3.2	Critérios de Exclusão	29
2.1.4	Critérios de Qualidade	29
2.1.5	Condução	29
2.1.6	Resultados	31
2.1.6.1	Nós da blockchain na borda da rede	32
2.1.6.2	Tratamento da integridade e veracidade da informação	32
2.1.6.3	Lacuna de análise na literatura	33
3	FUNDAMENTAÇÃO TEÓRICA	35
3.1	Internet das Coisas	35
3.1.1	Definição	35
3.1.2	Vulnerabilidades em IoT	36
3.1.3	Pilares de Segurança em IoT	36
3.2	Blockchain	37
3.2.1	Definição	37
3.2.1.1	Prova de Trabalho	38
3.2.1.2	Prova de Participação	38
3.2.2	Computação em Borda	39
4	PROPOSTA	41
4.1	Detalhamento	41
4.2	Validação da proposta	44
4.2.1	Caso de uso	45
4.3	Contribuição	45

5	EXPERIMENTOS	47
5.1	Estruturação do ambiente	47
5.1.1	Definição do modelo da blockchain	49
5.2	Métricas de desempenho e avaliação experimental	50
5.2.1	Desempenho e tempo de resposta	50
5.2.2	Segurança, integridade e privacidade do dado	50
5.2.3	Tecnologias e ferramentas utilizadas	52
6	RESULTADOS E DISCUSSÕES	55
6.1	Desempenho de interações com Blockchain	55
6.2	Casos de teste	58
6.2.1	Caso de teste de segurança	58
6.2.2	Caso de teste de integridade	60
6.2.3	Caso de teste de privacidade	61
7	CONCLUSÃO	65
	REFERÊNCIAS	67
	Apêndices	73
8	– SMART CONTRACTS UTILIZADOS NO EXPERIMENTO	75
8.1	Smart contract da blockchain na borda	75
8.2	Smart contract da blockchain na nuvem	77
9	– PONTUAÇÃO DE TRABALHOS NA REVISÃO SISTEMÁTICA	79

1 Introdução

1.1 Motivação para a Dissertação

Dados de geolocalização desempenham papel fundamental em um amplo conjunto de aplicações modernas, permitindo a identificação da posição espacial de pessoas, dispositivos e ativos ao longo do tempo. Informações como endereços, coordenadas geográficas e trajetórias espaciais são consideradas sensíveis, uma vez que sua exposição indevida pode permitir inferências sobre rotinas, comportamentos e padrões de deslocamento, acarretando riscos à privacidade e à segurança dos indivíduos ou organizações envolvidas.(LI; HU; LAN, 2020). Em cenários adversos, o vazamento ou a manipulação desses dados pode ser explorado por agentes maliciosos para fins como vigilância não autorizada, fraudes, sabotagem de operações logísticas ou comprometimento de infraestruturas críticas. Nesse contexto, aplicações que lidam com informações de geolocalização inserem-se em um ecossistema próprio de serviços de computação, no qual requisitos de segurança, integridade e confiabilidade tornam-se elementos centrais de seu framework.

Serviços Baseados em Localização (LBS) e em Localização em Tempo Real dependem da autenticidade e da integridade da informação de geolocalização do ativo que está sendo monitorado (HELO; SHAMSUZZOHA, 2020). Nesse contexto, o controle de informações de geolocalização é apresentado com vulnerabilidades no caso de, por exemplo, aplicações de roteirização de entregas de mercadorias, em que a privacidade do dado do destinatário é trabalhada para incrementar o grau de segurança da aplicação (YAO et al., 2022).

Outro desafio inerente ao LBS é a prova de que a localização de um determinado dispositivo é realmente a que ele alega estar. A prova de localização tem papel importante em diversas áreas, como em aplicações de assistência médica, gestão da cadeia de abastecimento e redes veiculares (ZAFAR et al., 2020). Além disso, o processamento e o armazenamento dos dados espaciais é fator crucial a ser levado em conta na concepção do framework da aplicação.

A tecnologia de blockchain, portanto, pode ser uma alternativa viável para as questões de segurança em LBS, devido à sua natureza descentralizada e à possibilidade de aplicação em abordagens menos custosas. Há também o recurso da aplicação de *smart contracts* integrada à tecnologia que provisiona o controle de acesso para os dispositivos na aplicação IoT (KHALID et al., 2020). Parte da cadeia da blockchain é processada através de algoritmos mais custosos, de modo que a transação seja registrada dentro dela. Algumas propostas distribuem esse processamento em nós localizados na borda da rede, próximos

aos dispositivos, para reduzir a participação da infraestrutura remota nas operações da blockchain (LEI et al., 2020).

Os trabalhos que integram blockchain em uma aplicação de Internet das Coisas têm propósitos diversos, abordando autenticação, criptografia, controle de acesso, armazenamento, redução de latência etc. Na perspectiva desse trabalho, um ativo é um artefato (que representa um objeto com algum valor) e deve ser monitorado por um dispositivo para que sua localização seja conhecida e auditada. A integração entre IoT e blockchain endereça as algumas questões de segurança e aborda questões de performance como um aspecto a ser tratado.

1.2 Descrição do problema

Na literatura analisada ao longo do capítulo 2, os trabalhos que abordam blockchain como uma ferramenta no ecossistema IoT, num contexto de uso de dados de geolocalização, tratam de aspectos distintos que estão ligados à tecnologia: performance, vulnerabilidades de privacidade, autenticação e integridade do dado. No entanto, o desenvolvimento desses aspectos não é combinado, fazendo com que os trabalhos tenham um foco em poucos deles.

Neste trabalho, a contribuição principal consiste na proposta de um framework baseado em blockchain que combina mecanismos voltados ao desempenho, à privacidade, à autenticação e à integridade de dados de geolocalização em aplicações de IoT. A implementação e a avaliação experimental do framework fornecem os elementos necessários para analisar sua aplicabilidade e discutir os aspectos fortalecidos pela proposta.

1.3 Objetivos Geral e Específicos

O objetivo geral deste trabalho é propor um framework baseado em blockchain para aplicações de Internet das Coisas que tratam dados de geolocalização. O framework combina a execução de nós blockchain na borda e na nuvem com mecanismos destinados a tratar aspectos de autenticação, integridade e privacidade dos dados, bem como de desempenho operacional. Como parte da proposta, o framework é implementado e avaliado experimentalmente em diferentes cenários de execução, a fim de analisar sua aplicabilidade e os resultados obtidos nos aspectos considerados.

Para alcançar o objetivo geral, foram definidos os seguintes objetivos específicos:

- Analisar os desafios de desempenho, autenticação, integridade e privacidade associados ao tratamento de dados de geolocalização em aplicações de IoT;
- Identificar, na literatura, contribuições que utilizam blockchain para tratar esses desafios e as lacunas que fundamentam a proposição do framework;

- Especificar os componentes, os fluxos de funcionamento e os mecanismos de blockchain que constituem o framework proposto;
- Implementar o framework em um estudo de caso com nós blockchain executados na borda e na nuvem;
- Avaliar experimentalmente o framework por meio de métricas de desempenho e de casos de teste relacionados às propriedades de segurança e privacidade dos dados;
- Analisar e discutir os resultados da avaliação, considerando as contribuições e as limitações do framework proposto.

1.4 Estrutura da Dissertação

A presente dissertação está disposta na seguinte estrutura: o Capítulo 2 detalha uma revisão da literatura quanto aos trabalhos que tratam da aplicação de blockchain em IoT num contexto de tratamento de dados de geolocalização, levantando lacunas de contribuição e oportunidades de pesquisa. O Capítulo 3 realiza uma fundamentação teórica nos temas de Internet das Coisas e Blockchain, para contextualizar as tecnologias e conceitos aplicados neste trabalho, além de abordar com brevidade a conciliação das duas áreas de pesquisa. O Capítulo 4 descreve a proposta de contribuição deste trabalho, apresentando o framework baseado em blockchain.

O Capítulo 5 detalha o planejamento e a condução do experimento, descrevendo o estudo de caso adotado, os cenários avaliados, as métricas utilizadas e os procedimentos empregados para a coleta dos dados experimentais. No Capítulo 6, são apresentados e analisados os resultados obtidos a partir da execução dos experimentos, contemplando as métricas de desempenho e os casos de teste relacionados às propriedades de segurança e privacidade avaliadas. Por fim, o Capítulo 7 apresenta a avaliação final do trabalho, consolidando as discussões sobre os resultados alcançados, as limitações observadas e as perspectivas de trabalhos futuros.

2 Trabalhos Relacionados

Os trabalhos relacionados a esta Dissertação foram obtidos através de uma Revisão Sistemática, cujo protocolo de busca foi baseado em Internet das Coisas com Blockchain em um contexto de uso da informação de geolocalização.

2.1 Metodologia da Revisão Sistemática

A Revisão Sistemática tem por objetivo sumarizar as informações dispostas sobre um determinado tópico de pesquisa, de forma minuciosa e imparcial Keele et al. (2007). Segundo Kitchenham (2012), existem três fases em uma RS: Planejamento, Condução e Resultado.

2.1.1 Questões de Pesquisa

As Questões de Pesquisa para esta RS foram definidas como:

1. QP1: *Quais são os principais desafios enfrentados em aplicações de monitoramento da localização ou em LBS?*
2. QP2: *O que a blockchain busca resolver em aplicações que envolvem a geolocalização?*
3. QP3: *Quais frameworks vêm sendo aplicados em aplicações LBS que envolvem blockchain?*

2.1.2 Protocolo de Busca

Para estruturar o protocolo de busca, foi aplicada uma Tabela de combinação dos tópicos principais (aplicação de blockchain em sistemas de IoT) do objeto de pesquisa, juntamente com o propósito de aplicação deles (contexto de aplicações que tratam de geolocalização). Em diversos casos, as contribuições que tratam desse tema dizem respeito aos Serviços Baseados em Localização (da sigla em inglês LBS).

Fonte: o próprio autor

O protocolo de busca, portanto, foi estabelecido com a seguinte regra: os termos de C_1 são unidos pelo conector lógico "AND", enquanto que os de C_2 são concatenados por "OR". Por fim, C_1 e C_2 são conectados por "AND". A Tabela 1 representa a aplicação, em cada repositório, do protocolo então definido. Vale ressaltar, no entanto, que o termo

Tabela 1 – Estruturação do protocolo de busca

Descrição	Keywords	Referência
Todos os trabalhos que tratam de alguma solução de blockchain em um ecossistema de IoT	iot; blockchain	C_1
Trabalhos que tratam do tópico da geolocalização ou de LBS	location tracking; LBS; <i>location based service</i>	C_2

completo, em inglês, para Serviço Baseado em Localização deve ser utilizado de forma que seja interpretado como um elemento só na busca; cada repositório tem sua regra própria para tal comando (geralmente é com o uso de aspas simples).

Uma vez definido, a busca foi executada em 5 repositórios digitais de trabalhos científicos, sendo eles:

- ACM Digital Library¹
- IEEEExplore²
- ScienceDirect³
- Scopus⁴
- Springer⁵

Após a coleta dos trabalhos com base nos repositórios apresentados, os estudos que realizavam uma revisão ou análise de outros trabalhos da área foram examinados para determinar se deveriam ser incluídos como fontes de estudos a serem triados, podendo ser considerados, portanto, repositórios adicionais.

2.1.3 Critérios de Inclusão e Exclusão

2.1.3.1 Critérios de Inclusão

- Possui uma proposta de framework ou de uso de blockchain em um ecossistema de aplicações de IoT;
- Trabalha sua contribuição em um contexto de problema que tem relação com informações de geolocalização.

Os Critérios de Inclusão definidos acima são obrigatórios para que o trabalho seja considerado relevante.

¹ <https://dl.acm.org>

² <https://ieeexplore.ieee.org>

³ <https://www.sciencedirect.com>

⁴ <https://www.scopus.com>

⁵ <https://www.springer.com>

2.1.3.2 Critérios de Exclusão

- Trabalhos que possuem apenas resumo ou que não contenham resumo;
- Estudos duplicados;
- Trabalhos que não apresentem uma contribuição envolvendo o dado de geolocalização;
- *Surveys*, revisões sistemáticas e revisões bibliográficas que não contenham trabalhos que atendam aos critérios de inclusão; e
- Trabalhos que obtiveram pontuação menor que 2 de acordo com os Critérios de Qualidade.
- Trabalhos que não sejam artigos de *journal* ou trabalhos de conferência (prefácios de capítulos, workshops, editoriais etc.)

2.1.4 Critérios de Qualidade

Para avaliar a qualidade dos estudos elegíveis com base nos Critérios de Inclusão, assim como para dar suporte à resposta às Questões de Pesquisa, 4 Critérios de Qualidade foram definidos. Eles comporão a pontuação de cada trabalho. São eles:

- CQ1: O trabalho detalhou a sua motivação e o seu objetivo final?
- CQ2: Houve especificação, de forma clara, dos resultados obtidos?
- CQ3: A blockchain, no trabalho, tem um propósito claro?
- CQ4: O trabalho apresenta alguma proposta de framework utilizando a blockchain?

2.1.5 Condução

Conforme está detalhado na Tabela 1, a *string* de pesquisa foi aplicada em cada repositório digital e resultou na coleta de 892 trabalhos. A pesquisa foi atualizada em fevereiro de 2026.

Tabela 2 – **Termos-chave considerados na etapa de triagem**

Termos-chave
iot, internet of things, iov, internet of vehicles;
blockchain, distributed ledger;
location based service, LBS, location service, internet of vehicles;
location privacy;
positioning, geolocation , geofencing, geo location;
location information, location tracking, location data, location tracing;
device location

Dos 892 trabalhos identificados, 128 eram *surveys*, revisões sistemáticas ou revisões bibliográficas. A análise das referências desses estudos resultou na inclusão de 4 revisões

como fontes adicionais de trabalhos para esta RS.

A triagem inicial seguiu o critério de análise de títulos e resumos de trabalhos que contêm termo-chave definidas na Tabela 2, para aqueles que possuem uma proposta de solução para um determinado problema. Para otimizar o processo de seleção durante toda a RS, foi utilizada a ferramenta Rayyan (<https://www.rayyan.ai>).

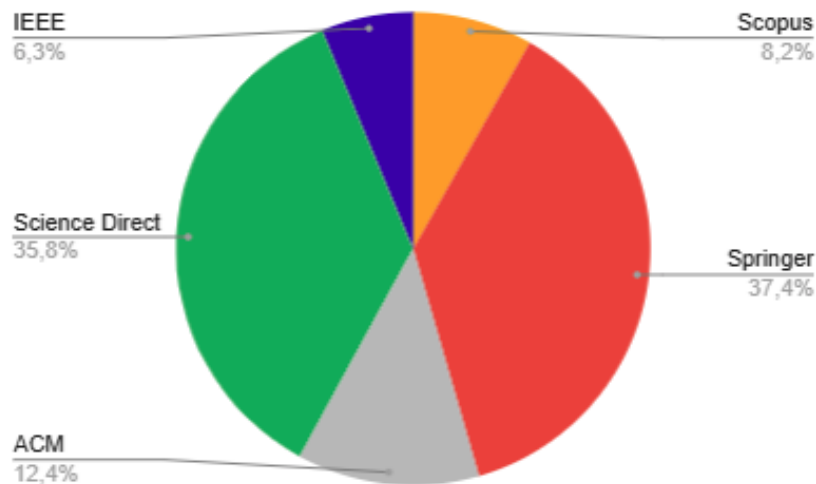


Figura 1 – Distribuição de trabalhos nos repositórios buscados.

FONTE: o próprios autores.

Após coleta dos trabalhos, os repositórios foram colocados sob análise. A distribuição da quantidade de trabalhos em cada repositório está definida na fig. 1.

Além da triagem inicial, uma análise mais aprofundada em revisões em geral (*surveys*, revisões bibliográficas e revisões sistemáticas) foi feita para identificar trabalhos que apresentam alguma contribuição na área de interesse desta RS. O mesmo protocolo da triagem foi utilizada para essa averiguação.

Em resumo, 50 trabalhos com contribuição própria foram incluídos na triagem, enquanto outros 6 foram identificados por meio das 4 revisões investigadas e incluídos conforme os critérios definidos. Assim, 56 trabalhos foram considerados após a primeira fase. Destes, 6 foram removidos em uma revisão posterior por não apresentarem blockchain como contribuição principal, restando 50 estudos para a aplicação dos Critérios de Qualidade.

Em seguida, os Critérios de Qualidade foram aplicados aos 50 estudos restantes. Desses, 36 obtiveram pontuação igual ou superior a 3 e compuseram o conjunto principal de análise da RS, sendo que 23 alcançaram a pontuação máxima. A Figura 2 apresenta o diagrama PRISMA atualizado, com as etapas da condução e suas respectivas quantidades.

Após a última fase, os trabalhos remanescentes foram considerados para responder às questões de pesquisa, para que os resultados finais desta RS pudessem ser alcançados.

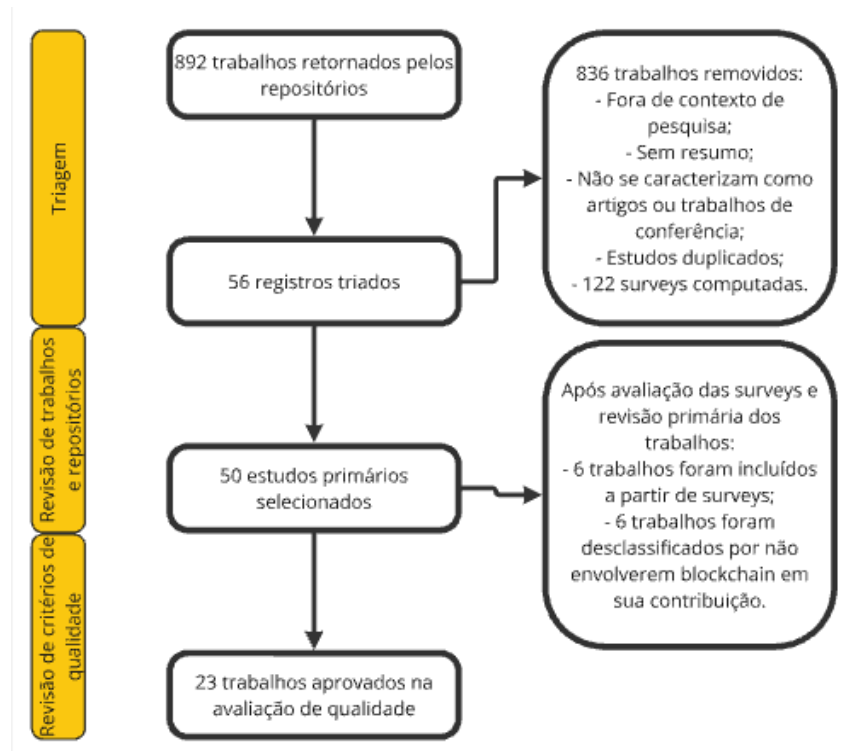


Figura 2 – Resultado da análise dos trabalhos buscados nos repositórios indicados.
FONTE: os próprios autores.

2.1.6 Resultados

Após a avaliação pelos Critérios de Qualidade, os 36 estudos com pontuação igual ou superior a 3 foram considerados para responder às Questões de Pesquisa da RS. A pontuação dos 50 estudos avaliados está apresentada no Apêndice 9.

Os estudos selecionados apresentam diferentes formas de aplicação de blockchain em IoT, com contribuições voltadas a aspectos específicos do tratamento de dados de geolocalização. A Tabela 3 sintetiza os trabalhos mais diretamente relacionados à proposta e indica os aspectos contemplados por cada um.

Tabela 3 – Síntese dos aspectos tratados pelos trabalhos relacionados e pelo framework proposto

Trabalho	Nós na borda	Autenticação	Integridade	Privacidade	Desempenho
(ZHANG et al., 2020)	✓	–	✓	✓	–
(WU et al., 2020)	✓	✓	–	✓	–
(SUN et al., 2021)	✓	–	–	✓	–
(REN et al., 2023)	–	–	✓	–	–
(LIANG et al., 2020)	✓	✓	✓	–	–
(DEDEOGLU et al., 2019)	–	–	✓	–	–
(PEELAM; SHAH; CHAMOLA, 2024)	–	✓	✓	✓	–
Framework proposto	✓	✓	✓	✓	✓

A comparação evidencia que os trabalhos relacionados contemplam apenas subconjuntos dos aspectos analisados. As propostas de Zhang et al. (2020), Wu et al. (2020) e Sun et al. (2021) utilizam nós na borda, mas não avaliam conjuntamente autenticação, integridade, privacidade e desempenho. Outros estudos tratam mecanismos específicos, como integridade, autenticação ou privacidade, sem combinar esses mecanismos com a execução da blockchain próxima aos dispositivos e com uma avaliação experimental de desempenho. Nesse conjunto, somente o framework proposto reúne os cinco aspectos apresentados na tabela. Essa ausência de uma abordagem integrada caracteriza a lacuna abordada pela dissertação.

2.1.6.1 Nós da blockchain na borda da rede

Zhang et al. (2020) propõe um modelo de aplicação de registro de dados de localização em uma rede veicular (VANET) cujos dispositivos fixos nas rodovias (RSU, da sigla em inglês) são nós de uma blockchain, instanciada na borda da rede, que recebem o pedido de leitura de um requerente e a solicitação de registro de dados por parte de um dispositivo veicular. A principal contribuição é voltada para a preservação da privacidade do autor do dado e a integridade da informação de geolocalização, portanto não há detalhes sobre a verificação da autenticidade e a autoridade para registrar novas informações na blockchain.

O trabalho de Wu et al. (2020) detalha a blockchain distribuída na borda da rede, com o papel de autenticar os dispositivos próximos como prova de localização. O papel da autenticação é impedir que informações sensíveis contidas do dispositivo não tenham que ser expostas na comunicação com aplicações remotas (na nuvem, por exemplo). Não há detalhamento de como o dado é mantido íntegro e verídico.

A proposta feita por Sun et al. (2021) trata da privacidade da informação de geolocalização em dois estágios: um para mascarar o dado que é trocado entre o dispositivo e um nó na borda da rede; e um outro estágio de privacidade garantido pelos mecanismos de validação e criptografia da blockchain. O trabalho aborda a distribuição de nós na rede para fins de escalabilidade, mas não trata os aspectos de autorização e autenticação, nem garante que o dado gerado é forjado de forma maliciosa. O foco é maior no mascaramento da informação transacionada na borda da rede.

2.1.6.2 Tratamento da integridade e veracidade da informação

Ren et al. (2023) faz uma proposta de framework de diferentes instâncias de blockchain: uma online que armazena a referência do dado registrado e uma offline (local para os dispositivos que trocam informações de geolocalização) que transaciona o dado espaço-temporal. A principal contribuição do framework é lidar com o aspecto de armazenamento que big data pode trazer devido à natureza do dado. Há também a

proposição de um mecanismo de verificação de integridade do dado, apesar de não haver tratamento para a sua veracidade e para a autenticação de novos dispositivos.

Liang et al. (2020) cria 3 estruturas de instâncias de blockchain, em que elas têm o papel de gerenciar a reputação (modelo de confiança) dos dispositivos e o acesso à informação, de forma que a natureza do dado é categorizada em um dos grupos e o dado em si é armazenado no terceiro grupo. O trabalho é voltado também a dados de multimídia (áudio, vídeo e imagens), em um contexto em que diversas aplicações podem consultar os dados gerados pelos dispositivos. Portanto é adicionada uma camada de complexidade ao framework, com evidência de confiança e distribuição no armazenamento da informação.

Por outro lado, Dedeoglu et al. (2019) propõe um modelo de reputação de dados registrados utilizando blockchain, em que a informação é considerada como confiável com base na confiabilidade do dispositivo e na verificação do bloco no processo de geração dele. Na proposta a credibilidade da informação é tratada como principal contribuição.

2.1.6.3 Lacuna de análise na literatura

Diante desses trabalhos, garantir autenticação e autorização é necessário para que apenas dispositivos legítimos registrem e consultem informações, enquanto mecanismos de integridade e privacidade devem proteger os dados sensíveis de geolocalização. Entretanto, os estudos analisados não tratam conjuntamente esses aspectos com a execução de nós blockchain na borda e a avaliação experimental do desempenho. O framework proposto busca preencher essa lacuna ao integrar os mecanismos de autenticação, integridade e privacidade a uma abordagem com nós na borda, avaliando também o tempo de resposta e a capacidade de processamento das operações.

3 Fundamentação Teórica

Este capítulo apresenta o material teórico que fundamenta o trabalho e estabelece uma linha de raciocínio com os demais capítulos. São abordados os tópicos necessários à contextualização das aplicações de Internet das Coisas e de suas vulnerabilidades, em conjunto com a conceituação de blockchain e os benefícios que podem ser obtidos com essa tecnologia.

3.1 Internet das Coisas

3.1.1 Definição

Internet das Coisas (ou IoT, da sigla em inglês) é uma rede ubíqua de dispositivos inteligentes, chamados de "coisas", que conecta objetos físicos do mundo que viabiliza a coleta e troca de informações, bem como a atuação do dado que está sendo trabalhado. IoT está transformando o mercado de novos negócios, através, dentre outras coisas, do aprimoramento desses dados, dando espaço à integração com outras áreas da computação, como Computação em Nuvem e Inteligência Artificial (PANARELLO et al., 2018).

Os equipamentos de Internet das Coisas variam de dispositivos vestíveis à plataformas de desenvolvimento em *hardware*. A conexão de dispositivos em uma rede IoT promove a troca de informações sem a necessidade de intervenção humana, a ubiquidade torna a aplicação mais propensa a ataques. Além disso, uma aplicação IoT tende a ter como principal fonte de dados os dispositivos autônomos conectados em uma grande quantidade, com diferentes limitações de recursos, o que torna o tratamento de segurança e privacidade mais complexo (SHAMMAR; ZAHARY; AL-SHARGABI, 2021).

A conexão de dispositivos em uma rede IoT promove a troca de informações sem a necessidade de intervenção humana, a ubiquidade torna a aplicação mais propensa a ataques. Além disso, uma aplicação IoT tende a ter como principal fonte de dados os dispositivos autônomos conectados em uma grande quantidade, com diferentes limitações de recursos, o que torna o tratamento de segurança e privacidade mais complexo (SHAMMAR; ZAHARY; AL-SHARGABI, 2021). Existem suscetibilidades nos 4 níveis de uma aplicação IoT (sensores, rede, *middleware* e aplicação) que viabilizam desde a captação maliciosa de dados (risco de privacidade) à tomada de controle dos dispositivos (HASSIJA et al., 2019).

3.1.2 Vulnerabilidades em IoT

Das fragilidades mais pertinentes apontadas em sistemas de IoT, uma das mais comuns são as de autenticação, cujo caráter centralizador dos frameworks reforça a vulnerabilidade (KHALID et al., 2020). Outro desafio importante é o de garantir a privacidade dos dados em um sistema IoT, devido principalmente à diversidade de dispositivos, comunicações e à descentralização de agentes que manipulam a informação (DAI; ZHENG; ZHANG, 2019). A integridade do dado é outro fator sensível a ter em consideração; no caso de Sistemas de Transporte Inteligentes e de carros autônomos, a interceptação de informações pessoais e localização do veículo ou dos ocupantes podem comprometer de uma viagem, como detalham Shrivastava e Dwivedi (2022b).

Os serviços baseados em localização (ou LBS, da sigla em inglês), sobretudo em um contexto de IoT, devem tratar a informação de geolocalização como uma questão de segurança a ser endereçada (LI; HU; LAN, 2020). O controle de informações de geolocalização é apresentado com vulnerabilidades no caso de, por exemplo, aplicações de roteirização de entregas de mercadorias, em que a privacidade do dado do destinatário é trabalhada para incrementar o grau de segurança da aplicação Yao et al. (2022).

Outro desafio inerente ao LBS é a prova de que a localização de um determinado dispositivo é realmente a que ele alega estar. A prova de localização tem papel importante em diversas áreas, como em aplicações de assistência médica, gestão da cadeia de abastecimento e redes veiculares (ZAFAR et al., 2020). Além disso, o processamento e o armazenamento dos dados espaciais é fator crucial a ser levado em conta na concepção do framework da aplicação.

3.1.3 Pilares de Segurança em IoT

A segurança da informação é tradicionalmente estruturada a partir dos pilares de Confidencialidade, Integridade e Disponibilidade. No contexto institucional brasileiro, o Laboratório Nacional de Computação Científica (LNCC), unidade vinculada ao Governo Federal, acrescenta a Autenticidade a esse conjunto e apresenta quatro pilares para iniciativas governamentais: Confidencialidade, Integridade, Disponibilidade e Autenticidade (Laboratório Nacional de Computação Científica, 2024). A Confidencialidade busca impedir o acesso ou a exposição de informações a entidades não autorizadas; a Integridade visa preservar a correção e a consistência dos dados; a Disponibilidade corresponde à manutenção do acesso aos dados e serviços quando necessário; e a Autenticidade permite verificar a origem legítima das informações e operações. Em ambientes de IoT, a heterogeneidade dos dispositivos, as limitações computacionais e a comunicação distribuída ampliam os desafios relacionados a esses pilares (SICARI et al., 2015; YANG et al., 2017; HASSIJA et al., 2019).

No contexto internacional de IoT, compilações de padrões de segurança destacam o relatório NISTIR 8259A como um dos referenciais aplicáveis a dispositivos conectados (National Digital Security Authority,). O NISTIR 8259A é uma publicação técnica oficial do National Institute of Standards and Technology (NIST), órgão do governo dos Estados Unidos, e estabelece uma linha de base de capacidades de cibersegurança para dispositivos IoT. Seu objetivo é apoiar organizações na identificação das capacidades técnicas necessárias para proteger dispositivos, dados, sistemas e ecossistemas (FAGAN et al., 2020). O relatório não apresenta os quatro pilares como sua estrutura central, mas complementa essa perspectiva ao traduzir princípios de segurança em capacidades aplicáveis aos dispositivos IoT.

Além dos quatro pilares adotados neste trabalho, privacidade e auditabilidade são consideradas propriedades complementares. A privacidade limita a exposição e a possibilidade de associação dos dados de geolocalização aos dispositivos ou titulares. A auditabilidade, por sua vez, possibilita verificar posteriormente os registros e as operações realizadas. Essas propriedades são relevantes em aplicações que integram IoT e blockchain, nas quais segurança, privacidade e confiança precisam ser tratadas de forma articulada (SICARI et al., 2015; SHAMMAR; ZAHARY; AL-SHARGABI, 2021).

No escopo desta dissertação, Autenticidade, Integridade e privacidade são avaliadas diretamente por casos de teste. A Confidencialidade é analisada a partir do controle de acesso e do conteúdo exposto em cada camada do framework; a auditabilidade é examinada por meio do histórico da cadeia e da ancoragem criptográfica; e a Disponibilidade é discutida a partir da redução da dependência da infraestrutura remota, sem a realização de testes específicos de falha ou indisponibilidade. Tempo de resposta e throughput são tratados separadamente como métricas de desempenho, e não como pilares de segurança.

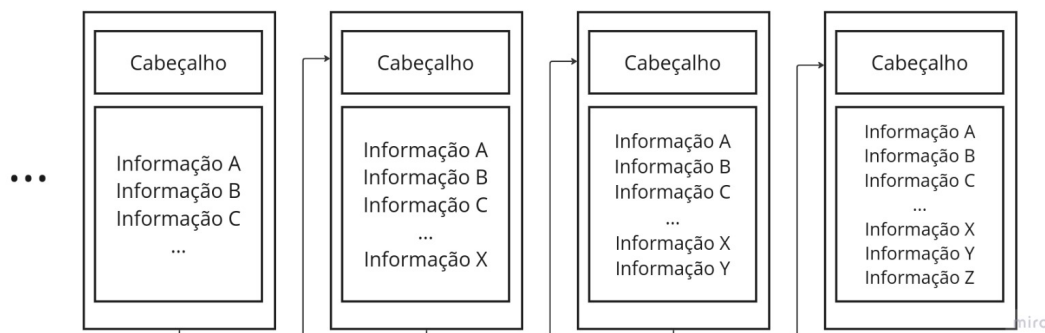
3.2 Blockchain

3.2.1 Definição

Blockchain pode ser definida como uma cadeia de blocos ordenada de forma cronológica, em que cada bloco é protegida por uma prova de trabalho (AITZHAN; SVETINOVIC, 2016). Eles têm basicamente dois blocos: um em que se armazena a transação em si (o dado que se deseja armazenar) e outro (cabeçalho) que armazena os dados sobre o bloco em si, como um *timestamp*, um *hash* dele e o *hash* do bloco anterior (HAMMI et al., 2018); a Figura 3 ilustra a configuração dos blocos. Isso caracteriza a blockchain como uma concatenação aninhada, de forma que um bloco não possa ser alterado sem que os anteriores o sejam também.

Uma blockchain é operada em uma rede *peer-to-peer*, totalmente descentralizada e

Figura 3 – Exemplo de uma blockchain simplificada.



Fonte: adaptado de (HAMMI et al., 2018).

distribuída. Ainda segundo (HAMMI et al., 2018), cada nó dessa rede mantém uma cópia completa de toda rede para se prevenir contra o Ponto Único de Falha. No entanto, eles podem funcionar de duas maneiras: os que podem ler dados (ou fatos) e os que podem ler e escrever dados na cadeia (também chamados de mineradores).

A adição de novos blocos na cadeia é feita de forma descentralizada e independe de confiança dos nós envolvidos, no entanto, é um tanto quanto desafiador realizar essa operação sem que o novo bloco seja em favor de nós maliciosos (DAI; ZHENG; ZHANG, 2019). Através de algoritmos de consenso, estabelece-se a confiança de que o bloco a ser adicionado é válido e íntegro. Um dos algoritmos mais conhecidos é o de Prova de Trabalho e o Prova de Participação.

3.2.1.1 Prova de Trabalho

A principal ponto sobre esse algoritmo é a existência de um desafio matemático extremamente difícil de se resolver, em que é necessário um grande gasto de recursos para que ele finalize. No entanto, o resultado do desafio é facilmente verificável (LI et al., 2020). Todo nó da rede pode participar do processo de verificação.

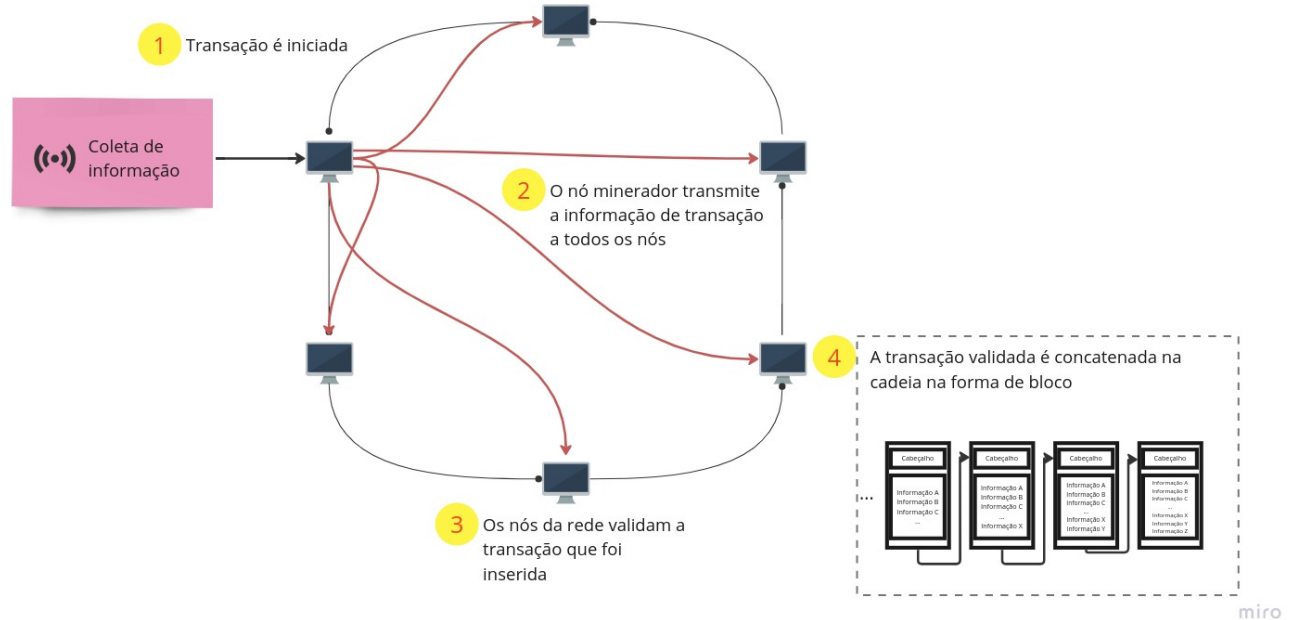
Esse tipo de algoritmo é baseado na confiança de que a maioria dos nós em uma rede é confiável. Quando um nó resolve o desafio e consegue adicionar um bloco à cadeia, há uma recompensa para ele. Geralmente, basta que 51% dos nós mineradores seja confiáveis para garantir a integridade da rede. Caso uma entidade maliciosa tente inserir registros falsos na rede, deve ter poder computacional e energia para ser, pelo menos, mais que a metade dos nós que inserem blocos à cadeia (DAI; ZHENG; ZHANG, 2019).

3.2.1.2 Prova de Participação

Enquanto que a Prova de Trabalho exige muitos recursos para funcionar, a Prova de Participação requer uma espécie de "autoridade" para que se faça o registro de novos blocos. Os nós que possuem mais valor monetário na rede (como uma abordagem muito

utilizada em criptomoedas) têm mais credibilidade em realizar mais registros (DAI; ZHENG; ZHANG, 2019).

Figura 4 – Exemplo de uma blockchain simplificada.



Fonte: adaptado de (DAI; ZHENG; ZHANG, 2019)

Uma das características da blockchain é a de pseudonimização, ou seja, a capacidade dela em garantir um certo nível de privacidade nas transações através de criptografia (DAI; ZHENG; ZHANG, 2019). A Figura 4 demonstra o fluxo de funcionamento de uma blockchain.

Uma quantidade menor de trabalhos utiliza a tecnologia de blockchain, em um contexto de IoT, para armazenar dados, dadas as premissas de segurança (privacidade) e o potencial de escalabilidade que ela pode oferecer.

3.2.2 Computação em Borda

A Computação em Borda é um paradigma de computação distribuída no qual recursos de processamento e armazenamento são posicionados próximos às fontes de dados e aos usuários, em vez de depender exclusivamente de centros de dados remotos. A borda pode ser composta por dispositivos com capacidade computacional, *gateways* ou servidores localizados próximos à rede de acesso. Essa proximidade permite que parte das operações seja executada antes do encaminhamento das informações à nuvem, estabelecendo uma relação complementar, e não necessariamente substitutiva, entre borda e nuvem (SHI et al., 2016; SATYANARAYANAN, 2017).

No contexto de IoT, dispositivos e sensores produzem dados continuamente, embora frequentemente possuam limitações de processamento, armazenamento, energia e

comunicação. A execução de serviços em nós próximos permite filtrar, validar e processar esses dados sem que todas as operações dependam de uma infraestrutura remota. Com isso, reduz-se o volume de informações transmitidas à nuvem e o percurso de comunicação envolvido no atendimento das requisições, aspecto relevante para aplicações que demandam respostas em intervalos curtos (KONG et al., 2023).

Entre os benefícios associados à Computação em Borda estão a redução dos atrasos de comunicação, a possibilidade de menores tempos de resposta ponta a ponta, o uso mais eficiente da largura de banda e a permanência de parte dos dados sensíveis em domínios locais. Entretanto, a proximidade do processamento não constitui, por si só, uma garantia de segurança ou privacidade. A distribuição dos recursos amplia desafios relacionados à heterogeneidade, ao gerenciamento dos nós, ao controle de acesso e à proteção de componentes potencialmente expostos (SHI et al., 2016; KONG et al., 2023).

Nesta dissertação, a Computação em Borda é utilizada para aproximar o processamento blockchain dos dispositivos que produzem os eventos de geolocalização. A blockchain executada na borda realiza o processamento e mantém os registros operacionais, enquanto a infraestrutura remota recebe apenas ancoragens criptográficas periódicas do estado da cadeia local. Dessa forma, a borda atende às operações próximas à origem dos dados, e a blockchain pública fornece uma referência externa para verificação e auditoria, explorando a complementaridade entre Computação em Borda e blockchain em aplicações de IoT (XUE et al., 2023).

4 Proposta

4.1 Detalhamento

O presente trabalho apresenta a proposta de um framework baseado em blockchain cuja aplicação está voltada para LBS. A proposta considera os pilares de Confidencialidade, Integridade, Disponibilidade e Autenticidade e as propriedades complementares de privacidade e auditabilidade, aplicando mecanismos específicos de acordo com o escopo e as limitações da avaliação realizada.

Uma característica a ser pontuada no framework é a distribuição de nós da blockchain em diferentes níveis na rede. Essa abordagem visa endereçar as questões ligadas ao desempenho, também tratadas em Zia (2021), com a redução do tempo de resposta das operações. Além disso, a aplicação de *smart contract* e a criptografia aplicada na tecnologia endereçam as questões de autenticidade, integridade e privacidade do dado Lv et al. (2020).

A proposta deste trabalho explora o uso da borda da rede como o principal ambiente de processamento e registro de dados de geolocalização em aplicações que utilizam blockchain. Nessa abordagem, os eventos de localização são validados e registrados em uma blockchain executada próxima às fontes de coleta, reduzindo a dependência de comunicação contínua com infraestruturas remotas e contribuindo para menores tempos de resposta no tratamento das informações. A utilização da borda permite ainda maior controle sobre o fluxo de dados sensíveis, ao limitar a exposição das informações a trechos mais curtos da rede e a domínios administrativos mais restritos.

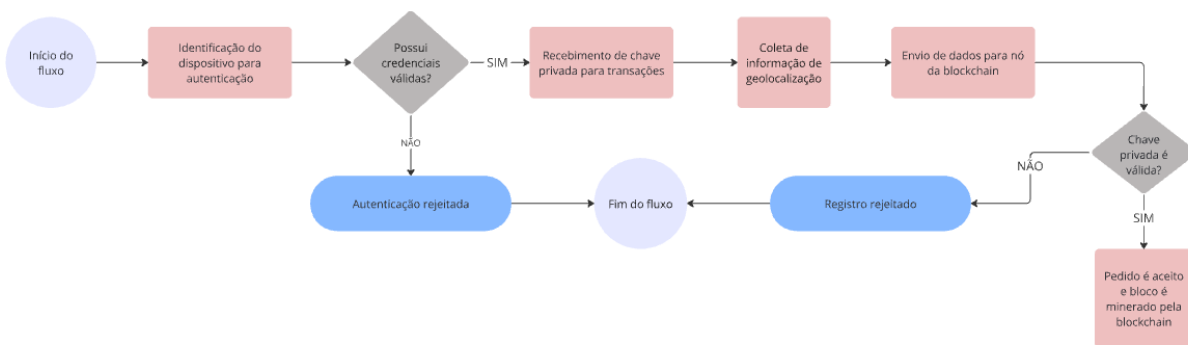
Para manter propriedades de integridade e privacidade, a abordagem incorpora mecanismos de ancoragem periódica do estado da blockchain local em uma infraestrutura remota, por meio do registro de resumos criptográficos. Dessa forma, busca-se conciliar requisitos de desempenho e privacidade com garantias de confiabilidade e verificabilidade dos dados ao longo do tempo. A proposta parte do pressuposto de que a proximidade entre o processamento blockchain e a origem dos dados de geolocalização pode oferecer uma solução mais adequada para aplicações sensíveis ao tempo de resposta e à exposição de informações, sem comprometer os princípios fundamentais associados ao uso de tecnologias de registro distribuído.

O framework adota uma blockchain permissionada na borda da rede, na qual a participação como nó validador e a submissão de transações são restritas a entidades previamente autorizadas. Essa cadeia mantém os registros operacionais de geolocalização, enquanto uma blockchain pública e não permissionada, executada na nuvem, recebe apenas

resumos criptográficos periódicos do estado da cadeia local. Essa composição busca conciliar controle de acesso, privacidade e previsibilidade operacional na borda com uma evidência externa e independente para auditoria da integridade dos registros.

A Figura 5 detalha o fluxo de funcionamento do framework durante o processo de escrita do dado de geolocalização. Desde a iniciação, o dispositivo realiza autenticação junto à blockchain através do envio de suas credenciais. Em seguida, uma chave privada é gerada e os blocos são gerados na blockchain com os dados do dispositivo, identificado pela chave privada.

Figura 5 – Fluxograma de autenticação e armazenamento de dados de geolocalização no Framework proposto.



Fonte: Autor.

Após o registro operacional dos dados de geolocalização na blockchain executada na borda da rede, o estado dessa cadeia local é periodicamente reduzido e encaminhado para a infraestrutura em nuvem por meio de um mecanismo de ancoragem. Esse processo consiste na geração de um resumo criptográfico representativo do estado atual da blockchain local, com o hash do último bloco gerado. O resumo gerado é então submetido como uma transação a uma blockchain executada na nuvem, que atua como camada de verificação e auditoria. Dessa forma, a infraestrutura remota não participa do processamento direto dos dados de geolocalização, mas mantém evidências criptográficas que permitem verificar, a posteriori, a integridade e a não adulteração dos registros produzidos na borda ao longo do tempo, sem gerar uma vulnerabilidade de privacidade na camada em nuvem.

A Figura 6 ilustra como os dispositivos interagem com nó da blockchain. Nela, o dispositivo que coleta a informação de geolocalização, responsável pela escrita do dado, interage diretamente com a instância na borda da rede.

Figura 6 – Proposta de framework com duas instâncias de blockchain para registrar dados de geolocalização.



Fonte: Autor.

No framework proposto, a leitura dos dados de geolocalização é realizada a partir da blockchain executada na borda da rede, onde os registros operacionais são mantidos. A blockchain executada na nuvem não armazena os dados de localização propriamente ditos, mas apenas resumos criptográficos do estado da cadeia local, utilizados para fins de verificação e auditoria. Dessa forma, consultas realizadas na nuvem permitem validar a integridade e a existência dos registros, mas não reconstruir seu conteúdo, preservando a privacidade dos dados sensíveis.

Esse tratamento articula os mecanismos do framework com os pilares e as propriedades de segurança definidos neste trabalho. A Tabela 4 sintetiza essa relação e delimita a forma de análise de cada propriedade.

Tabela 4 – Pilares e propriedades de segurança endereçados pelo framework

Propriedade	Mecanismo no framework	Forma de análise
Confidencialidade	Controle de acesso e manutenção dos dados de geolocalização na blockchain permissionada da borda; somente resumos criptográficos são enviados à rede pública.	Análise do conteúdo armazenado e exposto em cada camada.
Integridade	Registro encadeado na blockchain local e ancoragem periódica de seu estado em uma blockchain pública.	Comparação entre o estado local e os resumos criptográficos ancorados.
Disponibilidade	Processamento operacional na borda, reduzindo a dependência contínua da infraestrutura remota.	Discussão da abordagem; não foram realizados testes específicos de falha ou indisponibilidade.
Autenticidade	Registro de dispositivos, tokens temporários e validação das operações por <i>smart contracts</i> .	Casos de teste com operações autenticadas e não autenticadas.

Continua na próxima página

Tabela 4 – Pilares e propriedades de segurança endereçados pelo framework (continuação)

Propriedade	Mecanismo no framework	Forma de análise
Privacidade	Uso de identificadores pseudonimizados rotativos e ausência de dados de geolocalização na blockchain pública.	Análise da associação entre registros e da exposição dos dados persistentes.
Auditabilidade	Histórico da cadeia local e ancoragem externa dos resumos criptográficos.	Verificação posterior da existência e da integridade dos registros.

Fonte: Autor.

4.2 Validação da proposta

O framework proposto neste trabalho é avaliado por meio de um estudo de caso que mede as métricas de desempenho e analisa as propriedades de segurança e privacidade do fluxo proposto. Nele, os dispositivos que coletam informações de geolocalização e os que realizam a leitura dos dados são agentes que interagem diretamente com a blockchain que, por sua vez, armazena e transaciona os dados.

Por meio dessa exploração, o framework proposto é avaliado diante das vulnerabilidades existentes em aplicações de IoT que lidam com dados de geolocalização, apontadas no Capítulo 2.

A validação da proposta apresentada neste trabalho é realizada por meio da execução de experimentos controlados, estruturados para avaliar métricas de desempenho e propriedades de segurança e privacidade associadas ao uso de blockchain em aplicações que lidam com dados de geolocalização. A avaliação de desempenho concentra-se na medição do tempo de resposta ponta a ponta, do throughput e do consumo de recursos computacionais, considerando diferentes formas de estruturação da aplicação e distintas topologias de rede. Esses experimentos permitem analisar de forma comparativa o impacto da localização dos nós blockchain em relação aos dispositivos de coleta, considerando os efeitos combinados da proximidade computacional e do modelo de operação da blockchain.

Complementarmente à análise de desempenho, a validação da proposta inclui a execução de casos de teste relacionados às propriedades de segurança e privacidade dos dados de geolocalização. Esses casos de teste são definidos de maneira simples e objetiva, com o propósito de comparar como cada abordagem trata a proteção dos dados em trânsito, a preservação dos registros ao longo do tempo e o grau de exposição de informações sensíveis. A aplicação conjunta das métricas de desempenho e desses casos de teste permite discutir a robustez das abordagens avaliadas, fornecendo evidências empíricas sobre os efeitos do uso de nós blockchain na borda da rede em comparação com alternativas baseadas em infraestruturas mais centralizadas ou híbridas.

4.2.1 Caso de uso

O caso de uso explorado neste trabalho é o de um processo de auditoria contínua de ativos, de forma que os custos de logística e a precisão do dado gerado sejam melhorados. Nesse contexto, a aplicação do framework busca coletar informações de geolocalização dos ativos de forma periódica, segura e escalável, com a blockchain sendo uma ferramenta de armazenamento, autenticação e validação de dados, com tempos de resposta e desempenho de escrita e leitura adequados.

Os ativos, contendo dispositivos que coletam informações, realizam o processo de autenticação para que os dados espaciais sensíveis sejam enviados e persistidos. Cada etapa de validação utiliza um parâmetro diferente para a cadência da coleta dos dados de localização. Além disso, neste caso de uso, cada transação representa o registro dos dados em blocos na blockchain.

Nesse contexto de auditoria contínua de ativos, os experimentos são conduzidos a partir da simulação da geração periódica de eventos de geolocalização pelos dispositivos associados aos ativos monitorados. Esses eventos são enviados conforme diferentes cadências de coleta, representando distintos níveis de frequência de auditoria, e processados segundo as abordagens avaliadas no trabalho. Cada evento gerado corresponde a uma transação submetida à blockchain, permitindo medir o impacto da forma de estruturação da aplicação sobre métricas de desempenho, como tempo de resposta, throughput e consumo de recursos, bem como aplicar casos de teste relacionados às propriedades de segurança e privacidade. Dessa forma, o caso de uso fornece um cenário prático para a validação da proposta, aproximando a avaliação experimental de uma aplicação real de monitoramento e auditoria de ativos.

4.3 Contribuição

A proposta apresentada neste trabalho parte da hipótese de que a execução de nós blockchain próximos à origem dos dados de geolocalização pode favorecer o atendimento de requisitos de desempenho, sem deixar de endereçar segurança, integridade e privacidade em aplicações distribuídas. Nesse contexto, a contribuição consiste em realizar uma avaliação comparativa de diferentes abordagens de uso de blockchain, considerando variações na topologia de rede e na localização dos nós de validação, incluindo a borda da rede e infraestruturas remotas. Ao analisar essas abordagens por meio de métricas de desempenho e de casos de teste relacionados às propriedades de segurança e privacidade, o trabalho busca ampliar a compreensão sobre os impactos da proximidade computacional no uso de blockchain para o tratamento de dados de geolocalização em aplicações de Internet das Coisas, fornecendo subsídios para a escolha de soluções mais adequadas a esse tipo de aplicação.

5 Experimentos

Considerando a proposta de avaliar a aplicação de nós próximos aos dispositivos que coletam informações de geolocalização, o ambiente de experimentação foi estruturado para comparar métricas de desempenho, como tempo de resposta, throughput e consumo de recursos, e executar casos de teste relacionados às propriedades de segurança e privacidade dos dados de localização.

5.1 Estruturação do ambiente

O experimento foi estruturado de forma comparativa, considerando dois cenários de funcionamento distintos que diferem principalmente pela localização e pelo papel desempenhado pelos nós da blockchain em relação aos dispositivos de coleta de geolocalização. O Cenário A foi adotado como linha de base (*baseline*) por representar uma abordagem de integração direta, na qual os dispositivos submetem os eventos a uma blockchain pública executada remotamente, sem uma camada intermediária de processamento na borda. Esse cenário não pretende representar todas as implementações convencionais de blockchain em IoT, mas fornecer uma referência experimental para a comparação com o framework proposto.

Essa comparação não isola apenas o efeito da proximidade dos nós, pois os cenários também diferem quanto ao modelo de participação e às condições de consenso. Portanto, os resultados devem ser interpretados como efeitos combinados da distância da rede, da concorrência externa e do modelo de operação da blockchain.

No Cenário B, os nós blockchain são executados exclusivamente na borda da rede, formando uma blockchain local responsável pelo registro dos eventos de localização. Para garantir integridade e auditabilidade global dos dados, mecanismos de ancoragem periódica são empregados, registrando resumos criptográficos do estado da blockchain local em uma infraestrutura remota. A Tabela 5 sintetiza as configurações avaliadas e explicita as diferenças de processamento, rede, participação e ancoragem entre elas.

O experimento foi conduzido utilizando dispositivos de Internet das Coisas responsáveis pela coleta de coordenadas de geolocalização, os quais possuíam, em seu código-fonte, credenciais e identificadores associados ao ativo monitorado. A coleta dos dados ocorreu de forma periódica, com intervalo de 30 segundos entre as leituras, de modo a representar o acompanhamento do deslocamento de um ativo ao longo do tempo. Esses dados foram utilizados como entrada para a execução dos cenários experimentais avaliados.

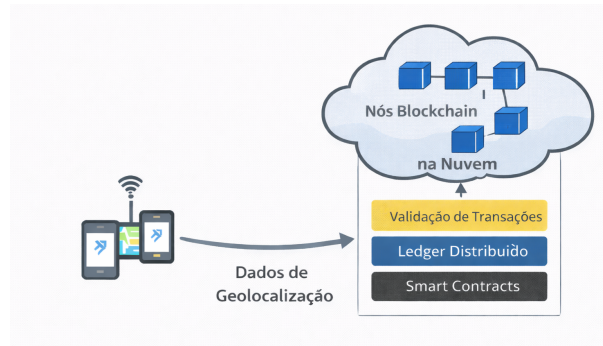
Tabela 5 – Resumo dos cenários experimentais avaliados

Característica	Cenário A	Cenário B
Processamento operacional	Remoto	Na borda
Rede utilizada	Pública	Local, com uso de rede pública para ancoragem
Participação	Não permissionada	Permissionada na cadeia local
Ancoragem	Não se aplica	Periódica, em blockchain pública
Finalidade experimental	Servir como linha de base (<i>baseline</i>), representando uma abordagem de integração direta em que os dispositivos submetem os dados a uma blockchain pública executada remotamente	Caracterizar o comportamento do processamento local com verificação externa

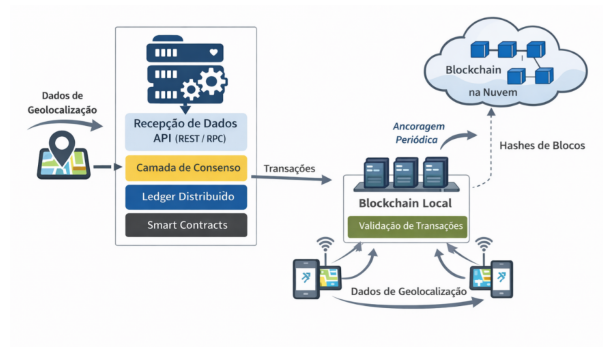
Fonte: Autor.

As abordagens avaliadas neste trabalho são ilustradas na Figura 7, que apresenta, de forma comparativa, os dois cenários considerados no experimento. O Cenário A corresponde à abordagem *baseline*, na qual os dispositivos de coleta de geolocalização comunicam-se diretamente com nós blockchain executados na nuvem, caracterizando maior dependência da latência de rede e do processamento remoto. Já o Cenário B adota uma abordagem na qual a blockchain local na borda é responsável por todo o processamento operacional dos eventos de geolocalização, enquanto a infraestrutura em nuvem atua apenas como mecanismo de ancoragem periódica do estado criptográfico da cadeia local. A comparação entre esses cenários fundamenta a hipótese central deste trabalho, segundo a qual a execução de nós blockchain próximos à origem dos dados de geolocalização contribui para o tratamento mais eficiente de requisitos de desempenho, especialmente no que se refere ao tempo de resposta e à capacidade de processamento, sem comprometer as propriedades de integridade e confiabilidade dos dados.

Figura 7 – Visão comparativa dos cenários experimentais avaliados.



(a) Cenário A – Baseline em nuvem



(b) Cenário B – Borda com ancoragem periódica

Fonte: Autor.

5.1.1 Definição do modelo da blockchain

Para o registro operacional dos eventos de geolocalização na borda, adotou-se uma blockchain permissionada. Essa escolha decorre do contexto do caso de uso, no qual dispositivos, validadores e operadores pertencem a um domínio administrativo previamente conhecido. A restrição de participação permite controlar quais entidades podem submeter e validar transações, revogar participantes comprometidos e reduzir a exposição de dados sensíveis a agentes externos. Além disso, o conjunto controlado de validadores reduz a sobrecarga de consenso e proporciona maior previsibilidade do tempo de resposta e da vazão, características relevantes para aplicações de IoT executadas próximas à origem dos dados.

O caráter permissionado da cadeia não substitui os mecanismos de autenticação implementados na camada de aplicação. Os *smart contracts* verificam a legitimidade das operações de escrita e leitura, enquanto as regras da rede controlam a participação na infraestrutura de consenso. Esses controles atuam de forma complementar: a permissão de ingresso restringe os participantes da rede, e a autenticação da aplicação determina quais operações cada dispositivo está autorizado a realizar.

Para fornecer uma evidência de integridade externa ao domínio administrativo da borda, o framework utiliza uma blockchain pública e não permissionada na nuvem. Essa

rede não recebe os dados de geolocalização nem participa do processamento operacional dos eventos; nela são registrados apenas resumos criptográficos periódicos do estado da cadeia permissionada. A independência dos validadores externos dificulta a alteração coordenada tanto dos registros locais quanto de suas âncoras, permitindo auditoria posterior sem expor o conteúdo sensível.

Dentre as blockchains públicas disponíveis, optou-se pela Ethereum devido à sua ampla adoção, maturidade tecnológica e suporte consolidado a contratos inteligentes. Seu modelo de execução permite implementar a lógica de ancoragem de forma verificável e favorece a reprodutibilidade dos experimentos. Assim, a avaliação contempla dois papéis distintos: a cadeia permissionada na borda processa e mantém os registros operacionais, e a cadeia pública na nuvem atua como camada independente de verificação.

5.2 Métricas de desempenho e avaliação experimental

5.2.1 Desempenho e tempo de resposta

Durante o experimento, foi medido o tempo de resposta ponta a ponta da operação de escrita, também denominado latência transacional neste trabalho. A métrica corresponde ao intervalo entre o envio do evento de geolocalização pelo dispositivo e a confirmação da transação pela blockchain. Portanto, abrange os tempos de comunicação, processamento da aplicação, execução do *smart contract*, consenso e confirmação, sem atribuir o valor observado exclusivamente à rede. Foram analisadas estatísticas descritivas, como média, mediana e percentis, a fim de caracterizar o comportamento típico e as variações observadas sob diferentes condições de carga.

Além do tempo de resposta, foi avaliado o throughput do sistema, medido como o número de transações de geolocalização confirmadas por unidade de tempo. Essa métrica é fundamental para analisar a capacidade da infraestrutura em suportar diferentes volumes de dispositivos e frequências de envio de eventos, especialmente em cenários que incorporam nós blockchain na borda da rede. A análise do throughput foi utilizada para identificar possíveis gargalos associados ao mecanismo de consenso e à distribuição dos nós, bem como comparar a escalabilidade relativa dos frameworks avaliados.

5.2.2 Segurança, integridade e privacidade do dado

As propriedades de Autenticidade, Integridade e privacidade são consideradas neste trabalho como critérios fundamentais para a avaliação da robustez dos dois cenários experimentais propostos. Os casos de teste relacionados às propriedades de segurança e privacidade permitem analisar, de forma complementar às métricas de desempenho, como diferentes formas de estruturação da aplicação influenciam a proteção e o tratamento de

dados de geolocalização em ambientes distribuídos. Ao considerá-las de maneira integrada, busca-se compreender não apenas o comportamento operacional do sistema, mas também sua capacidade de operar de forma confiável frente a riscos associados à exposição, à modificação indevida e ao uso inadequado de informações sensíveis.

Em relação aos pilares apresentados na Seção 3.1.3, os casos de teste avaliam diretamente Autenticidade, Integridade e privacidade. A Confidencialidade é analisada pelo controle de acesso e pelo conteúdo exposto nas blockchains da borda e da nuvem, enquanto a auditabilidade é verificada por meio da ancoragem criptográfica. A Disponibilidade não é submetida a testes de falha, sendo discutida apenas em relação à menor dependência operacional da infraestrutura remota.

Para avaliar esses aspectos, são definidos casos de teste específicos, cada um direcionado a um dos critérios analisados. O caso de teste de segurança concentra-se na verificação da autenticação da origem dos dados e na proteção das informações em trânsito entre os dispositivos e o primeiro ponto de validação. O caso de teste de integridade avalia a capacidade do sistema em preservar os registros de geolocalização ao longo do tempo e em detectar alterações retroativas nos dados armazenados. Por sua vez, o caso de teste de privacidade busca analisar o grau de exposição das informações sensíveis, considerando tanto o conteúdo efetivamente registrado na blockchain quanto o tráfego de dados em redes externas. Esses casos de teste são aplicados de forma comparativa aos três cenários, permitindo discutir diferenças de abordagem e seus impactos na robustez do sistema proposto.

1. Caso de teste de segurança: este caso de teste tem como objetivo verificar se eventos de geolocalização inválidos ou alterados são corretamente detectados e rejeitados pelo sistema antes de seu registro na blockchain. Para isso, são considerados cenários de envio de eventos válidos, eventos com conteúdo modificado após a assinatura e tentativas de reenvio de eventos já processados. A avaliação é realizada de forma comparativa nos dois cenários experimentais, observando-se o impacto da proximidade do primeiro ponto de validação na superfície de exposição dos dados em trânsito.
2. Caso de teste de integridade: o caso de teste de integridade tem como foco verificar a consistência entre o estado da blockchain executada na borda da rede e as evidências criptográficas ancoradas em uma blockchain pública. O teste consiste no registro sequencial de dados de geolocalização na blockchain local, seguido da realização do processo de ancoragem periódica do estado da cadeia, de forma a permitir a comparação posterior entre os hashes locais e os valores registrados externamente. A evidência de integridade é obtida a partir da correspondência entre o estado da blockchain na borda e as âncoras armazenadas na nuvem, sendo que qualquer modificação retroativa nos dados locais resulta em divergência detectável. Dessa

forma, ao validar a integridade da ancoragem, o teste também assegura a integridade dos registros mantidos na borda da rede.

3. Caso de teste de privacidade: este caso de teste busca analisar o grau de exposição dos dados de geolocalização em cada cenário experimental. A avaliação considera o conteúdo efetivamente transmitido pelos dispositivos, o tipo de informação registrada na blockchain e a possibilidade de reconstrução de trajetos a partir dos dados persistidos. A partir dessa análise, discute-se como diferentes formas de estruturação da aplicação influenciam a proteção da privacidade dos dados, com especial atenção à redução da exposição de informações sensíveis em cenários que privilegiam o processamento na borda da rede. Para o experimento, definiu-se a rotação do identificador pseudonimizado a cada 10 registros de geolocalização. Considerando o intervalo de coleta de 30 segundos, essa janela representa aproximadamente cinco minutos de eventos por dispositivo e permite observar o compromisso entre a redução da associação temporal dos registros e a manutenção de continuidade dentro de um intervalo operacional curto. O valor 10 constitui um parâmetro experimental configurável, e não um limiar universal de privacidade; sua escolha permite demonstrar o mecanismo de rotação de forma controlada, sem introduzir trocas de identificador a cada evento.

5.2.3 Tecnologias e ferramentas utilizadas

O framework proposto não estabelece dependência de linguagens, bibliotecas ou plataformas específicas. Para sua avaliação, foi desenvolvida uma implementação de referência composta por aplicações responsáveis pela geração, transmissão, validação e registro dos eventos de geolocalização, além das infraestruturas blockchain utilizadas nos cenários experimentais. A Tabela 6 apresenta as principais tecnologias e ferramentas empregadas nessa implementação e o papel desempenhado por cada uma.

Tabela 6 – Tecnologias e ferramentas utilizadas na implementação experimental

Tecnologia ou ferramenta	Papel no experimento
JavaScript	Implementação dos clientes experimentais, da geração dos eventos de geolocalização, do serviço de ancoragem e do processamento dos resultados
Node.js	Execução das aplicações e dos scripts utilizados nos cenários experimentais
Solidity	Implementação dos contratos inteligentes responsáveis pela autenticação dos dispositivos e pelo registro dos eventos de geolocalização
Hardhat e Hardhat Network	Compilação e implantação dos contratos inteligentes e execução da blockchain na borda
Ethers.js	Comunicação com as blockchains, assinatura e submissão de transações e interação com os contratos inteligentes
Ethereum Sepolia	Rede pública utilizada no cenário de linha de base e no registro das ancoragens criptográficas
Infura	Disponibilização do acesso RPC à rede Ethereum Sepolia
Docker	Isolamento e execução dos componentes do ambiente experimental
Arquivos CSV	Registro das medições das rodadas e suporte ao cálculo das métricas de desempenho

Fonte: Autor.

As aplicações de geração dos eventos de geolocalização, interação com os contratos e processamento dos resultados foram implementadas em JavaScript e executadas com Node.js. A biblioteca Ethers.js foi utilizada para estabelecer a comunicação por meio de interfaces JSON-RPC, assinar e submeter transações e interagir com os contratos inteligentes. Esses contratos foram escritos em Solidity, enquanto o Hardhat foi empregado para compilação, implantação e execução da blockchain na borda.

No cenário público, as operações foram submetidas à rede de testes Sepolia da Ethereum, acessada por meio do serviço Infura. O mesmo acesso foi utilizado pelo serviço de ancoragem para registrar, na rede pública, os resumos criptográficos do estado da blockchain mantida na borda. Os componentes do ambiente local foram executados em contêineres Docker, e as medições produzidas durante as rodadas experimentais foram registradas em arquivos CSV para posterior cálculo das métricas de desempenho.

O código-fonte, os contratos inteligentes e os arquivos de configuração empregados na implementação experimental estão disponíveis em repositório público (PRAXEDES, 2026). Esse material documenta a composição dos componentes apresentados nesta subseção e fornece suporte à verificação e à reprodução do ambiente avaliado.

6 Resultados e Discussões

Este capítulo apresenta os resultados obtidos a partir da execução dos experimentos definidos para a validação da proposta, bem como a discussão dos principais achados observados. A análise contempla métricas de desempenho e casos de teste relacionados às propriedades de segurança e privacidade no uso de blockchain em aplicações que lidam com dados de geolocalização, permitindo uma comparação entre as diferentes abordagens avaliadas. São discutidos resultados das métricas de desempenho relativas ao tempo de resposta ponta a ponta, ao throughput e ao consumo de recursos, bem como os comportamentos observados nos casos de teste relacionados à segurança, à integridade e à privacidade dos dados. A partir dessa análise, o capítulo busca relacionar os resultados observados com a hipótese central do trabalho, destacando padrões, implicações práticas e limitações identificadas ao longo da execução dos experimentos.

6.1 Desempenho de interações com Blockchain

A avaliação de desempenho entre os cenários é conduzida a partir da análise de métricas estatísticas e operacionais que permitem capturar tanto o comportamento típico quanto a variabilidade do sistema. Em particular, são utilizados percentis do tempo de resposta ponta a ponta (p50, p95 e p99) e a taxa de processamento de transações por segundo (*throughput* ou TPS), além de métricas auxiliares como valores mínimo, máximo e média dos tempos observados. Os percentis são calculados a cada rodada experimental com base em 200 amostras consecutivas de operações de escrita, refletindo a distribuição do tempo de resposta sob uma carga controlada. Para reduzir o impacto de flutuações pontuais e capturar um comportamento representativo ao longo do tempo, o valor final de cada percentil considerado na análise corresponde à mediana dos percentis obtidos em todas as rodadas realizadas. Essa abordagem permite uma avaliação mais robusta do desempenho, especialmente em sistemas baseados em blockchain, nos quais o tempo de confirmação pode apresentar distribuição assimétrica e cauda longa.

O ambiente experimental é configurado de forma a garantir consistência e comparabilidade entre os cenários avaliados. Cada rodada experimental consiste na coleta de 200 amostras de operações de escrita de dados de geolocalização, com a interação simultânea de até 10 dispositivos, representando fontes independentes de dados na borda da rede. Esses dispositivos realizam autenticação e submetem transações à blockchain de acordo com uma cadência predefinida, permitindo avaliar o comportamento do sistema sob carga concorrente moderada. A limitação do número de dispositivos e do tamanho das rodadas visa controlar variáveis externas, assegurando que as diferenças observadas nos resultados

de desempenho estejam associadas predominantemente à topologia de rede e à estruturação da abordagem avaliada, e não a variações excessivas de carga ou volume de dados.

Tabela 7 – Comparação dos resultados de desempenho entre blockchain na borda e blockchain na nuvem

Métrica	Blockchain na borda	Blockchain na nuvem
Tempo de resposta p50 (ms)	121.0	11 942.0
Tempo de resposta p95 (ms)	145.0	20 414.2
Tempo de resposta p99 (ms)	158.1	22 129.2
TPS mediano (tx/s)	1.599	0.059

Fonte: Autor.

Os resultados evidenciam diferenças expressivas de desempenho entre a execução da blockchain na borda da rede e a execução em infraestrutura remota na nuvem. No cenário de borda, os tempos de resposta observados permanecem consistentemente abaixo de 200 ms, com valores medianos de 121 ms, 145 ms e 158 ms para os percentis p50, p95 e p99, respectivamente, indicando comportamento estável e baixa variabilidade mesmo nos extremos da distribuição. Em contraste, a blockchain na nuvem apresenta tempos de resposta significativamente superiores, com p50 acima de 11 segundos e p99 ultrapassando 22 segundos, além de elevada dispersão entre rodadas, característica de redes públicas sujeitas à variabilidade de consenso e comunicação. Essa diferença reflete-se diretamente na capacidade de processamento, com a abordagem na borda alcançando uma taxa mediana próxima de 1,6 transações por segundo, enquanto a execução na nuvem permanece abaixo de 0,1 transação por segundo. Os resultados indicam que a abordagem na borda oferece menor tempo de resposta e maior previsibilidade nas condições avaliadas, considerando os efeitos combinados da proximidade computacional e das diferenças entre os modelos de operação das blockchains.

Tabela 8 – Coeficiente de variação do tempo de resposta nas últimas cinco rodadas válidas

Rodada	Blockchain na borda (CV)	Blockchain na nuvem (CV)
Rodada 1	0.136	0.364
Rodada 2	0.163	0.754
Rodada 3	0.133	0.728
Rodada 4	0.141	0.646
Rodada 5	0.132	0.932

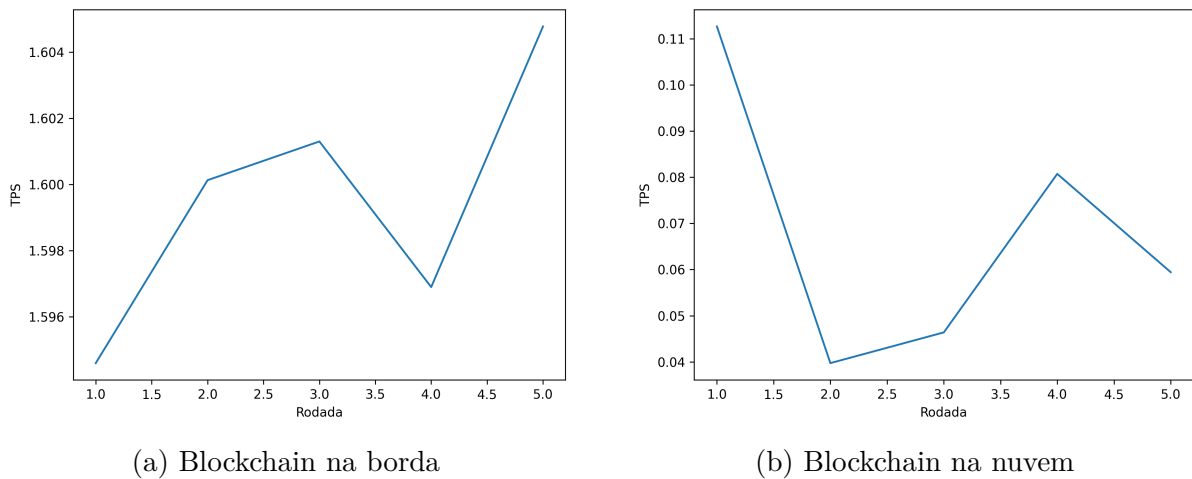
Fonte: Autor.

A Tabela 8 apresenta o coeficiente de variação (CV) do tempo de resposta para as rodadas experimentais válidas, considerando as abordagens de execução da blockchain na borda da rede e na nuvem. O CV é utilizado como métrica complementar por permitir avaliar a variabilidade relativa do desempenho, independentemente da magnitude absoluta

do tempo observado, sendo particularmente adequado para a comparação entre cenários com ordens de grandeza distintas. Os resultados indicam que a blockchain executada na borda apresenta valores de CV consistentemente baixos, refletindo comportamento previsível e estável entre rodadas. Em contraste, a blockchain executada na nuvem exibe coeficientes de variação significativamente mais elevados, evidenciando maior dispersão e instabilidade do tempo de resposta, característica associada à natureza pública e não permissionada da rede.

É importante destacar que o desempenho observado na blockchain executada na nuvem pode ter sido impactado pelo fato de se tratar de uma rede pública e não permissionada. Nesse tipo de ambiente, as transações submetidas competem por inclusão em blocos com transações de outros participantes da rede, o que introduz variabilidade adicional e limita a previsibilidade do tempo de confirmação. Além disso, a presença de mineradores ou validadores externos, que não estão sob controle do experimento, influencia diretamente o processo de consenso e a priorização das transações, constituindo um fator relevante a ser considerado na interpretação dos resultados de desempenho obtidos nesse cenário. Além do tempo de resposta das operações, a métrica de vazão também é importante para comparar o desempenho entre as abordagens.

Figura 8 – Evolução do throughput (TPS) nas abordagens avaliadas.



Fonte: Autor.

A análise da evolução do throughput evidencia diferenças significativas entre as abordagens avaliadas, conforme ilustrado nas figuras 8a e 8b. Na blockchain executada na borda da rede, observa-se comportamento estável do TPS ao longo das últimas cinco rodadas experimentais, com variações pouco expressivas entre medições consecutivas, indicando previsibilidade e capacidade consistente de processamento. Em contraste, a blockchain executada na nuvem apresenta valores de TPS substancialmente inferiores e maior variabilidade entre rodadas válidas, refletindo as características de uma rede pública e não permissionada, na qual a inclusão de transações depende da competição com

participantes externos e do processo de consenso. Essas diferenças reforçam o impacto da topologia de rede e da proximidade computacional sobre o desempenho, destacando a vantagem da execução na borda para aplicações que demandam processamento contínuo e previsível de dados de geolocalização.

6.2 Casos de teste

Os casos de teste têm como objetivo verificar se as propriedades de segurança consideradas na proposta são contempladas pelo framework desenvolvido. A autenticação dos dispositivos fornece evidências de Autenticidade; a comparação entre os registros locais e as âncoras públicas avalia a Integridade e a auditabilidade; e a rotação do *pseudoId*, juntamente com a restrição do conteúdo publicado na nuvem, subsidia a análise de privacidade e Confidencialidade. A Disponibilidade não foi avaliada por testes de interrupção ou falha e, portanto, não é apresentada como resultado experimental de segurança.

6.2.1 Caso de teste de segurança

O caso de teste de segurança tem como objetivo verificar a efetividade do mecanismo de autenticação aplicado às operações de leitura e escrita de dados de geolocalização na blockchain. Nesse contexto, a autenticação é utilizada como requisito obrigatório para que um dispositivo possa interagir com o *smart contract*, assegurando que apenas entidades previamente identificadas sejam capazes de registrar ou consultar informações sensíveis. O teste é estruturado a partir da tentativa de execução de operações sem autenticação prévia, bem como da utilização de credenciais inválidas, de forma a observar o comportamento do sistema diante de acessos não autorizados.

O trecho de código apresentado no Listagem 6.1 ilustra essa verificação, na qual o contrato compara o token informado pelo dispositivo com o token ativo previamente gerado durante o processo de autenticação. Essa abordagem assegura que a operação de registro de dados esteja condicionada à autenticação válida, funcionando como um mecanismo de controle de acesso no nível do contrato inteligente.

Trecho de Código 6.1 – Verificação de autenticação no registro de dados de geolocalização

```
function recordLocation(  
    bytes32 deviceId ,  
    bytes32 sessionToken ,  
    int256 latitude ,  
    int256 longitude  
) external {  
    require(  

```

```
        activeToken[deviceId] == sessionToken ,
        "invalid_token "
    );
    require(
        activeToken[deviceId] != bytes32(0) , "not_authenticated"
    );

    locations.push(Location({
        deviceId: deviceId ,
        latitude: latitude ,
        longitude: longitude ,
        timestamp: block.timestamp
    }));

    emit LocationRecorded(deviceId , latitude , longitude ,
    block.timestamp);
}
```

A evidência do atendimento a esse caso de teste é obtida a partir da análise das respostas do contrato inteligente e dos registros gerados durante a execução experimental. Tentativas de escrita realizadas sem a posse de um token de autenticação válido ou com informações de identificação inconsistentes resultam em falhas explícitas, com a reversão da transação, enquanto operações executadas após o processo de autenticação são concluídas com sucesso e registradas na blockchain. Esses comportamentos são observáveis tanto nos eventos emitidos pelo contrato inteligente quanto nos logs do cliente, demonstrando que o mecanismo de autenticação atua de forma efetiva como uma camada de segurança para o acesso aos dados de geolocalização.

A Figura 9a evidencia a interação com *smart contract* em casos em que o dispositivo não está autenticado previamente. No caso da Figura 9b, a evidência é de que o dispositivo está enviando uma identificação inválida para registrar dados. A Figura 9c, por sua vez, exibe o *log* de um caso de registro de dados com êxito.

Figura 9 – Evidência dos registros de autenticação no *smart contract*.

```

node-1 | eth_estimateGas
node-1 | Contract call:      DeviceAuthGeo#recordLocation
node-1 | From:                0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
node-1 | To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1 | Value:                0 ETH
node-1 |
node-1 | Error: reverted with reason string 'not authenticated'
node-1 |

```

(a) Tentativa de registro sem autenticação prévia.

```

node-1 | eth_estimateGas
node-1 | Contract call:      DeviceAuthGeo#recordLocation
node-1 | From:                0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
node-1 | To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1 | Value:                0 ETH
node-1 |
node-1 | Error: reverted with reason string 'invalid token'
node-1 |

```

(b) Tentativa de registro com token inválido.

```

node-1 | Contract call:      DeviceAuthGeo#recordLocation
node-1 | Transaction:        0xcce9f1516e06d245fb9647c02581ad42d00c4ad1508312708bcdade40232ef9d
node-1 | From:                0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
node-1 | To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
node-1 | Value:                0 ETH
node-1 | Gas used:            31813 of 31813
node-1 | Block #21:           0x00943f149ea09cbb50d8ffcd4c3351d68f6c345a78ef9a5448ea1c4532eb4da
node-1 |

```

(c) Registro realizado com token válido.

Fonte: Autor.

6.2.2 Caso de teste de integridade

A evidência do caso de teste de integridade é obtida a partir da comparação entre o estado da blockchain executada na borda da rede e as evidências criptográficas ancoradas em uma blockchain pública. Após o registro dos dados de geolocalização, o *hash* do último bloco da cadeia local é sintetizado e armazenado externamente por meio do mecanismo de ancoragem. Em uma etapa posterior, o estado local é verificado e comparado com o valor ancorado, sendo observada a correspondência entre os *hashes*. Essa correspondência evidencia que os registros mantidos na borda não sofreram alterações retroativas após a ancoragem, demonstrando que a integridade da cadeia local é preservada e pode ser auditada a partir das evidências externas.

Figura 10 – *log* do registro de ancoragem do estado da blockchain na borda, para garantir a integridade dos dados registrados.

```
On-chain latestSequence(edgeChainId): 0
OK seq=1 edgeBlock=212 latency_ms=5648 tx=0x05a46b96...
OK seq=2 edgeBlock=212 latency_ms=26505 tx=0x4edf13d0...
OK seq=3 edgeBlock=250 latency_ms=26553 tx=0xff887e0b...
OK seq=4 edgeBlock=307 latency_ms=26575 tx=0xafce56c7...
```

Fonte: Autor.

A figura 10 ilustra o processo de ancoragem, evidenciando a criação de uma transação na blockchain pública. Na primeira execução, não há registro de ancoragem realizado, sendo o primeiro a ser feito na linha seguinte, com a informação de número do bloco, tempo de resposta da operação e o *hash* do bloco da ancoragem na blockchain na nuvem. É possível observar que, após 2 rodadas de ancoragem, a blockchain na borda teve seu estado alterado (novos dados inseridos) e a ancoragem atrela os novos blocos a esse novo estado.

6.2.3 Caso de teste de privacidade

A evidência do atendimento ao caso de teste de privacidade é obtida por meio da análise da conectividade entre eventos e da possibilidade de reconstrução de trajetos de dispositivos, considerando um mecanismo de pseudonimização baseado na rotação periódica do identificador lógico utilizado nos registros de geolocalização.

Algoritmo 1 Geração de pseudônimo rotativo (*pseudoId*)

Exige: *deviceId*, *token*, *seq*

Garante: *pseudoId*

- 1: $batch \leftarrow \left\lfloor \frac{seq - 1}{10} \right\rfloor$
 - 2: $pseudoId \leftarrow \text{keccak256}(deviceId \parallel token \parallel batch)$
 - 3: **devolve** *pseudoId*
-

No experimento conduzido, o identificador persistido na blockchain não corresponde ao identificador real do dispositivo, sendo substituído por um pseudônimo (*pseudoId*) derivado criptograficamente do identificador do dispositivo, do token de autenticação e do número da janela calculado a partir da sequência do registro. Esse pseudônimo é exibido no Algoritmo 1 e é mantido constante apenas durante um intervalo limitado, correspondente a um conjunto de 10 registros consecutivos na blockchain da borda, sendo automaticamente rotacionado após esse limiar.

Como consequência direta dessa estratégia, eventos de geolocalização pertencentes a janelas distintas não compartilham um identificador comum nos dados observáveis.

A análise da conectividade evidencia que a associação determinística entre eventos fica restrita ao interior de cada janela de 10 registros, reduzindo a capacidade de um observador externo em correlacionar registros ao longo de períodos mais extensos.

Tabela 9 – Registros de geolocalização com rotação de *pseudoId* a cada 10 registros

Bloco	deviceId	pseudoId	Timestamp	Latitude	Longitude
0x99ff...7ae3	D_001	P_A1	1700000001	-3.80785	-38.57571
0x99ff...7ae3	D_001	P_A1	1700000006	-3.80740	-38.57526
0x99ff...7ae3	D_001	P_A1	1700000011	-3.80695	-38.57481
0x99ff...7ae3	D_001	P_A1	1700000016	-3.80650	-38.57436
0x99ff...7ae3	D_001	P_A1	1700000021	-3.80605	-38.57391
0x99ff...7ae3	D_001	P_A1	1700000026	-3.80560	-38.57346
0x99ff...7ae3	D_001	P_A1	1700000031	-3.80605	-38.57391
0x99ff...7ae3	D_001	P_A1	1700000036	-3.80650	-38.57436
0x99ff...7ae3	D_001	P_A1	1700000041	-3.80695	-38.57481
0x99ff...7ae3	D_001	P_A1	1700000046	-3.80740	-38.57526
0x5e0a...93ee	D_001	P_B2	1700000051	-3.80785	-38.57571
0x5e0a...93ee	D_001	P_B2	1700000056	-3.80740	-38.57526
0x5e0a...93ee	D_001	P_B2	1700000061	-3.80695	-38.57481
0x5e0a...93ee	D_001	P_B2	1700000066	-3.80650	-38.57436
0x5e0a...93ee	D_001	P_B2	1700000071	-3.80605	-38.57391
0x5e0a...93ee	D_001	P_B2	1700000076	-3.80560	-38.57346
0x5e0a...93ee	D_001	P_B2	1700000081	-3.80605	-38.57391
0x5e0a...93ee	D_001	P_B2	1700000086	-3.80650	-38.57436
0x5e0a...93ee	D_001	P_B2	1700000091	-3.80695	-38.57481
0x5e0a...93ee	D_001	P_B2	1700000096	-3.80740	-38.57526

Fonte: Autor.

A Tabela 9 ilustra um trecho representativo dos registros observáveis durante a execução do experimento. Observa-se que o identificador real do dispositivo não é exposto nos dados persistidos, enquanto o *pseudoId* permanece constante apenas dentro do intervalo de 10 registros, sendo alterado na janela subsequente, apesar da continuidade temporal e espacial dos eventos. Dessa forma, a repetição de *pseudoId* fica limitada a 10 registros consecutivos. Para verificar o funcionamento do mecanismo, define-se a taxa de conformidade da rotação como

$$C_{\text{rot}} = \frac{|\{pseudoId_i \mid i \in [1, n]\}|}{\lceil n/10 \rceil}$$

Nessa expressão, o numerador representa a quantidade de pseudônimos distintos observados em n registros, e o denominador corresponde à quantidade esperada de janelas de rotação. O valor $C_{\text{rot}} = 1$ indica que foi gerado exatamente um pseudônimo para cada janela de até 10 registros. Esse indicador verifica a conformidade da implementação com a

política definida, mas não demonstra, isoladamente, ausência de rastreabilidade, pois um observador ainda pode tentar correlacionar eventos por proximidade temporal ou espacial.

A janela de 10 registros foi adotada como parâmetro do experimento para equilibrar a redução da associação persistente entre eventos e a continuidade operacional dentro de um intervalo curto. Como os registros são produzidos a cada 30 segundos, cada janela corresponde a aproximadamente cinco minutos. Não foram comparados diferentes tamanhos de janela; portanto, os resultados demonstram o funcionamento do mecanismo nessa configuração, mas não estabelecem que o valor 10 seja ótimo para todos os contextos de uso.

7 Conclusão

Este trabalho apresentou e avaliou um framework baseado em blockchain para o tratamento de dados de geolocalização, considerando a execução de nós na borda da rede e mecanismos de ancoragem em blockchain pública. Os resultados experimentais corroboram a hipótese de que a proximidade computacional entre a origem dos dados e os nós de validação contribui para o atendimento de requisitos de desempenho em relação à execução em infraestrutura remota na nuvem.

A execução da blockchain na borda da rede apresentou melhorias nas métricas de desempenho em relação à abordagem em nuvem, com menores tempos de resposta, maior throughput e comportamento mais estável ao longo das rodadas experimentais. Esses resultados indicam que a localização e o modelo de operação dos nós blockchain exercem influência sobre o desempenho de aplicações distribuídas baseadas em dados de geolocalização, sem que isso implique a eliminação de desafios inerentes a esse tipo de sistema.

Os casos de teste relacionados às propriedades de segurança e privacidade evidenciaram que o framework proposto é capaz de atender a requisitos de autenticação, integridade e privacidade quando esses aspectos são tratados na camada de aplicação. Os mecanismos de controle de acesso, ancoragem criptográfica e pseudonimização demonstraram-se eficazes dentro do escopo avaliado. Ressalta-se, contudo, que vulnerabilidades relacionadas à comunicação na ponta da rede não foram abordadas neste trabalho, permanecendo fora do seu escopo de análise.

Como contribuição, o framework apresenta aderência aos pilares e às propriedades de segurança definidos no trabalho. A Confidencialidade é favorecida pela restrição dos dados sensíveis à cadeia permissionada da borda; a Integridade e a auditabilidade são sustentadas pelo registro encadeado e pela ancoragem pública; a Autenticidade é tratada pelos mecanismos de registro e autenticação dos dispositivos; e a privacidade é reforçada pela pseudonimização dos identificadores. A execução na borda reduz a dependência contínua da infraestrutura remota, mas a Disponibilidade não foi validada por testes específicos de falha e permanece como uma propriedade a ser aprofundada.

A abordagem proposta não impõe dependência de uma tecnologia ou versão específica de blockchain, conferindo versatilidade à adoção de diferentes distribuições e configurações, desde que os mecanismos de segurança sejam adequadamente implementados na aplicação.

Como trabalho futuro, destaca-se a avaliação do framework em conjunto com baselines baseados em blockchains permissionadas, de modo a isolar as variáveis de rede

que influenciaram os resultados experimentais, bem como a investigação de novos cenários com diferentes configurações e distribuições de nós na borda da rede. Além disso, propõe-se a análise de mecanismos de segurança na comunicação entre os dispositivos de coleta e o nó de borda, a comparação de diferentes janelas de rotação do identificador pseudonimizado e a avaliação de diferentes estratégias de ancoragem, para que seja aprofundada a compreensão sobre o papel da blockchain em ecossistemas de Internet das Coisas.

Conclui-se, portanto, que o framework proposto é viável e se mostra competente para agregar ganhos de performance à aplicação, sem introduzir vulnerabilidades adicionais de segurança no escopo considerado, fornecendo subsídios para a escolha de frameworks de blockchain mais adequados a aplicações de geolocalização.

Referências

- AITZHAN, N. Z.; SVETINOVIC, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, IEEE, v. 15, n. 5, p. 840–852, 2016. Citado na página 37.
- AL-QARAFI, A. et al. Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. *Applied Sciences*, MDPI, v. 12, n. 12, p. 5893, 2022. Citado na página 80.
- AL-WESABI, F. N. et al. Integrated communication and location monitoring system for vehicle monitoring via smartphone calls. *Alexandria Engineering Journal*, Elsevier, v. 128, p. 1159–1167, 2025. Citado na página 80.
- ALEXANDRIDIS, A. et al. A stylized presence detection system in the era of blockchain and big data. In: IEEE. *2022 IEEE International Conference on Big Data (Big Data)*. [S.l.], 2022. p. 6575–6577. Citado na página 80.
- ALONSO-NÚÑEZ, J.; LLANOS, D. R. Secure architecture for iot and blockchain-based waste traceability. In: SPIE. *Remote Sensing Technologies and Applications in Urban Environments X*. [S.l.], 2025. v. 13672, p. 100–101. Citado na página 80.
- AMORETTI, M. et al. Blockchain-based proof of location. In: IEEE. *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. [S.l.], 2018. p. 146–153. Citado na página 80.
- BAUCAS, M. J.; SPACHOS, P. Federated kalman filter for secure iot-based device monitoring services. *IEEE Networking Letters*, IEEE, 2023. Citado na página 80.
- DAI, H.-N.; ZHENG, Z.; ZHANG, Y. Blockchain for internet of things: A survey. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 5, p. 8076–8094, 2019. Citado 3 vezes nas páginas 36, 38 e 39.
- DEDEOGLU, V. et al. A trust architecture for blockchain in iot. In: *Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services*. [S.l.: s.n.], 2019. p. 190–199. Citado 3 vezes nas páginas 31, 33 e 80.
- DONG, C. et al. Optimizing uav delivery for pervasive systems through blockchain integration and adversarial machine learning. *Computer Communications*, Elsevier, v. 236, p. 108113, 2025. Disponível em: <<https://doi.org/10.1016/j.comcom.2025.108113>>. Citado na página 80.
- DRAUGELYTĖ, P.; SUZDALEV, I. Blockchain-based secure communication for uav networks: a decentralized approach to gnss spoofing detection. *Aviation*, v. 29, n. 3, p. 191–200, 2025. Citado na página 80.
- FAGAN, M. et al. *IoT Device Cybersecurity Capability Core Baseline*. [S.l.], 2020. Disponível em: <<https://csrc.nist.gov/pubs/ir/8259/a/final>>. Citado na página 37.

- GAVRILĂ, M. et al. A blockchain-based system for monitoring sobriety and tracking location of traffic drivers. *Electronics*, MDPI, v. 14, n. 18, p. 3728, 2025. Citado na página 80.
- GEHLOT, A. et al. Dairy 4.0: Intelligent communication ecosystem for the cattle animal welfare with blockchain and iot enabled technologies. *Applied Sciences*, MDPI, v. 12, n. 14, p. 7316, 2022. Citado na página 80.
- GUAN, Z. et al. A blockchain-based verified locating scheme for iot devices. In: IEEE. *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*. [S.l.], 2021. p. 799–805. Citado na página 80.
- GUL, M. J. J.; PAUL, A. Iot geography chain: Blockchain-based solution for logistics ecosystem. In: SPRINGER. *The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021*. [S.l.], 2022. p. 191–194. Citado na página 80.
- HAMMI, M. T. et al. Bubbles of trust: A decentralized blockchain-based authentication system for iot. *Computers & Security*, Elsevier, v. 78, p. 126–142, 2018. Citado 2 vezes nas páginas 37 e 38.
- HASSIJA, V. et al. A survey on iot security: application areas, security threats, and solution architectures. *IEEE Access*, IEEE, v. 7, p. 82721–82743, 2019. Citado 2 vezes nas páginas 35 e 36.
- HELO, P.; SHAMSUZZOHA, A. Real-time supply chain—a blockchain architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*, Elsevier, v. 63, p. 101909, 2020. Citado na página 23.
- KAUSHIK, A.; PILLAI, A. S. Blockchain and iot based inventory monitoring system. In: IEEE. *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*. [S.l.], 2021. p. 827–831. Citado na página 80.
- KEELE, S. et al. *Guidelines for performing systematic literature reviews in software engineering*. [S.l.]: Technical report, ver. 2.3 ebse technical report. ebse, 2007. Citado na página 27.
- KHALID, U. et al. A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Cluster Computing*, Springer, v. 23, n. 3, p. 2067–2087, 2020. Citado 2 vezes nas páginas 23 e 36.
- KHAN, M. U. et al. From detection to prevention: a cyber-secure ai ecosystem for mitigating milk adulteration and dairy fraud. *Trends in Food Science & Technology*, Elsevier, p. 105503, 2025. Citado na página 80.
- KIM, B. Y.; CHOI, S. S.; JANG, J. W. Data managing and service exchanging on iot service platform based on blockchain with smart contract and spatial data processing. In: *Proceedings of the 1st international conference on information science and systems*. [S.l.: s.n.], 2018. p. 59–63. Citado na página 80.
- KITCHENHAM, B. A. Systematic review in software engineering: where we are and where we should be going. In: *Proceedings of the 2nd international workshop on Evidential assessment of software technologies*. [S.l.: s.n.], 2012. p. 1–2. Citado na página 27.

KONG, L. et al. Edge-computing-driven internet of things: A survey. *ACM Computing Surveys*, v. 55, n. 8, p. 1–41, 2023. Citado na página 40.

Laboratório Nacional de Computação Científica. *Os quatro pilares da segurança da informação: confidencialidade, disponibilidade, integridade e autenticidade*. 2024. Acesso em: 18 ago. 2026. Disponível em: <<https://www.gov.br/lbcc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade>>. Citado na página 36.

LAMBA, A. K. et al. Smart hospitals and iot-based healthcare automation. In: *Transforming Healthcare With AI And IoT*. [S.l.]: CRC Press, 2026. p. 18–37. Citado na página 80.

LEAL, M.; PISANI, F.; ENDLER, M. A blockchain-based service for inviolable presence registration of mobile entities. *Journal of the Brazilian Computer Society*, Springer, v. 27, n. 1, p. 1, 2021. Citado na página 80.

LEI, K. et al. Groupchain: Towards a scalable public blockchain in fog computing of iot services computing. *IEEE Transactions on Services Computing*, IEEE, v. 13, n. 2, p. 252–262, 2020. Citado na página 24.

LI, D.; HU, Y.; LAN, M. Iot device location information storage system based on blockchain. *Future Generation computer systems*, Elsevier, v. 109, p. 95–102, 2020. Citado 2 vezes nas páginas 23 e 36.

LI, H. et al. Blockchain meets vanet: An architecture for identity and location privacy protection in vanet. *Peer-to-Peer Networking and Applications*, Springer, v. 12, p. 1178–1193, 2019. Citado na página 80.

LI, X. et al. A survey on the security of blockchain systems. *Future generation computer systems*, Elsevier, v. 107, p. 841–853, 2020. Citado na página 38.

LIANG, H. et al. Fog-based secure service discovery for internet of multimedia things: a cross-blockchain approach. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, ACM New York, NY, USA, v. 16, n. 3s, p. 1–23, 2020. Citado 3 vezes nas páginas 31, 33 e 80.

LIU, H. et al. Improvement of blockchain-based multi-layer location data sharing scheme for internet of things. *Computer Communications*, Elsevier, v. 201, p. 131–142, 2023. Citado na página 80.

LIYANAGE, I. et al. Idairy: Intelligence and secure e-commerce platform for dairy production and distribution using block chain and machine learning. In: IEEE. *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*. [S.l.], 2022. p. 1–6. Citado na página 80.

LV, W.; QIU, X.; MENG, L. Blockchain localization spoofing detection based on fuzzy ahp in iot systems. *EURASIP Journal on Wireless Communications and Networking*, SpringerOpen, v. 2022, n. 1, p. 1–19, 2022. Citado na página 80.

LV, W. et al. Towards large-scale and privacy-preserving contact tracing in covid-19 pandemic: a blockchain perspective. *IEEE Transactions on Network Science and Engineering*, IEEE, v. 9, n. 1, p. 282–298, 2020. Citado 2 vezes nas páginas 41 e 80.

MUNASINGHE, U. J.; HALGAMUGE, M. N. Supply chain traceability and counterfeit detection of covid-19 vaccines using novel blockchain-based vacledger system. *Expert Systems with Applications*, Elsevier, v. 228, p. 120293, 2023. Citado na página 80.

NASRULIN, B.; MUZAMMAL, M.; QU, Q. A robust spatio-temporal verification protocol for blockchain. In: SPRINGER. *Web Information Systems Engineering–WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part I 19*. [S.l.], 2018. p. 52–67. Citado na página 80.

National Digital Security Authority. *IoT Security Standards*. Acesso em: 18 ago. 2026. Disponível em: <<https://nationaldigitalsecurityauthority.com/iot-security-standards/>>. Citado na página 37.

NOSOUHI, M. R. et al. Blockchain for secure location verification. *Journal of Parallel and Distributed Computing*, Elsevier, v. 136, p. 40–51, 2020. Citado na página 80.

PANARELLO, A. et al. Blockchain and iot integration: A systematic survey. *Sensors*, MDPI, v. 18, n. 8, p. 2575, 2018. Citado na página 35.

PEELAM, M. S.; SHAH, K.; CHAMOLA, V. V-track: blockchain-enabled iot system for reliable vehicle location verification. *Digital Communications and Networks*, Elsevier, 2024. Citado 2 vezes nas páginas 31 e 80.

PEELAM, M. S.; SHAH, K.; CHAMOLA, V. V-track: Blockchain-enabled iot system for reliable vehicle location verification. *Digital Communications and Networks*, Elsevier, v. 12, p. 119–133, 2026. Disponível em: <<https://doi.org/10.1016/j.dcan.2024.08.004>>. Citado na página 80.

PRAXEDES, W. *Eth Experimento Mestrado: implementação e ambiente dos experimentos*. 2026. Acesso em: 18 ago. 2026. Disponível em: <<https://github.com/washingtonpraxedes/eth-experimento-mestrado>>. Citado na página 53.

QU, Z. et al. Oracle-inspired rfid-based indoor positioning architecture for sharing. In: SPRINGER NATURE. *2nd International Conference on Big Data, IoT, and Cloud Computing: ICBICC 2024*. [S.l.], 2026. p. 49. Citado na página 80.

RABIEI, R. et al. Transition toward smart hospitals: A scoping review of features, technologies, and challenges. *Health Science Reports*, Wiley Online Library, v. 8, n. 12, p. e71601, 2025. Citado na página 80.

RAWAL, D.; SEEDORF, J.; PATIL, B. An approach that utilizes blockchain to effectively and securely preserve data privacy for location data from iot in smart cities. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Copernicus Publications Göttingen, Germany, v. 48, p. 201–208, 2025. Citado na página 80.

REN, Y. et al. Bsmd: A blockchain-based secure storage mechanism for big spatio-temporal data. *Future Generation Computer Systems*, Elsevier, v. 138, p. 328–338, 2023. Citado 3 vezes nas páginas 31, 32 e 80.

RENGAN, B. K. Smart acquiring platform in contactless payments using advanced machine learning: Security controls using device recognition, geo fencing and customer on file. In: IEEE. *2023 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. [S.l.], 2023. p. 1–7. Citado na página 80.

- SAAD, M. et al. Blockchain-enabled vanet for smart solid waste management. *IEEE Access*, IEEE, v. 11, p. 5679–5700, 2023. Citado na página 80.
- SAKTHI, U. et al. Blockchain-based internet of vehicles for intelligent transportation system using fog computing. In: *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021*. [S.l.]: Springer, 2022. p. 827–835. Citado na página 80.
- SATYANARAYANAN, M. The emergence of edge computing. *Computer*, v. 50, n. 1, p. 30–39, 2017. Citado na página 39.
- SHAHID, A. R. et al. Quantifying location privacy in permissioned blockchain-based internet of things (iot). In: *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. [S.l.: s.n.], 2019. p. 116–125. Citado na página 80.
- SHAHZAD, A.; ZHANG, K.; GHERBI, A. Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain. *Sensors*, MDPI, v. 20, n. 13, p. 3760, 2020. Citado na página 80.
- SHAMMAR, E. A.; ZAHARY, A. T.; AL-SHARGABI, A. A. A survey of iot and blockchain integration: Security perspective. *IEEE Access*, IEEE, v. 9, p. 156114–156150, 2021. Citado 2 vezes nas páginas 35 e 37.
- SHI, W. et al. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, v. 3, n. 5, p. 637–646, 2016. Citado 2 vezes nas páginas 39 e 40.
- SHRIVASTAVA, A. L.; DWIVEDI, R. K. Designing a secure vehicular internet of things (iot) using blockchain. In: *Inventive Systems and Control: Proceedings of ICISC 2022*. [S.l.]: Springer, 2022. p. 669–679. Citado na página 80.
- SHRIVASTAVA, A. L.; DWIVEDI, R. K. A secure design of the smart vehicular iot system using blockchain technology. In: IEEE. *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*. [S.l.], 2022. p. 616–620. Citado na página 36.
- SICARI, S. et al. Security, privacy and trust in internet of things: The road ahead. *Computer networks*, Elsevier, v. 76, p. 146–164, 2015. Citado 2 vezes nas páginas 36 e 37.
- SUN, Z. et al. A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing. *International Journal of Intelligent Systems*, Wiley Online Library, v. 36, n. 5, p. 2058–2080, 2021. Citado 3 vezes nas páginas 31, 32 e 80.
- TOKKOZHINA, U. et al. Decentralizing online food delivery services: A blockchain and iot model for smart cities. *Mobile Networks and Applications*, Springer, p. 1–11, 2023. Citado na página 80.
- WANG, J.; LIU, G.; ZHAO, G. Two-attribute privacy protection method of mcs based on blockchain smart contract. *Computer Communications*, Elsevier, v. 193, p. 126–135, 2022. Citado na página 80.
- WEERAPANPISIT, P. et al. A decentralized location-based reputation management system in the iot using blockchain. *IEEE Internet of Things Journal*, IEEE, v. 9, n. 16, p. 15100–15115, 2022. Citado na página 80.

WU, W. et al. Blockchain based zero-knowledge proof of location in iot. In: IEEE. *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. [S.l.], 2020. p. 1–7. Citado 3 vezes nas páginas 31, 32 e 80.

XUE, H. et al. Integration of blockchain and edge computing in internet of things: A survey. *Future Generation Computer Systems*, v. 144, p. 307–326, 2023. Citado na página 40.

YADAV, R. et al. Preserving location privacy using blockchain. In: SPRINGER. *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*. [S.l.], 2020. p. 1–5. Citado na página 80.

YANG, Y. et al. A survey on security and privacy issues in internet-of-things. *IEEE Internet of things Journal*, IEEE, v. 4, n. 5, p. 1250–1258, 2017. Citado na página 36.

YAO, Y. et al. Internet of things positioning technology based intelligent delivery system. *IEEE Transactions on Intelligent Transportation Systems*, IEEE, 2022. Citado 2 vezes nas páginas 23 e 36.

ZAFAR, F. et al. Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis. *Electronics*, MDPI, v. 9, n. 11, p. 1776, 2020. Citado 2 vezes nas páginas 23 e 36.

ZHANG, J. et al. A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, IEEE, v. 22, n. 4, p. 2299–2313, 2020. Citado 3 vezes nas páginas 31, 32 e 80.

ZHANIKEEV, M. The last man standing technique for proof-of-location in iot infrastructures at network edge. *Wireless Communications and Mobile Computing*, Hindawi Limited, v. 2019, p. 1–12, 2019. Citado na página 80.

ZHAO, J. et al. An intelligent service method for grid spatio-temporal big data based on beidou. In: *Proceedings of the 3rd International Conference on Information Technologies and Electrical Engineering*. [S.l.: s.n.], 2020. p. 574–578. Citado na página 80.

ZIA, M. B-drive: A blockchain based distributed iot network for smart urban transportation. *Blockchain: Research and Applications*, Elsevier, v. 2, n. 4, p. 100033, 2021. Citado 2 vezes nas páginas 41 e 80.

ZOU, S. et al. Crowdblps: A blockchain-based location-privacy-preserving mobile crowdsensing system. *IEEE transactions on industrial informatics*, IEEE, v. 16, n. 6, p. 4206–4218, 2019. Citado na página 80.

Apêndices

8 *Smart contracts* utilizados no experimento

Este apêndice apresenta os smart contracts empregados no framework proposto, com o objetivo de documentar os mecanismos utilizados pelas aplicações cliente para o registro de dados de geolocalização na blockchain da borda e para a ancoragem desses dados em uma blockchain pública na nuvem.

8.1 Smart contract da blockchain na borda

O smart contract da blockchain na borda é responsável pelo registro de dispositivos, autenticação baseada em token temporário e emissão de eventos de geolocalização associados a identificadores pseudonimizados.

Trecho de Código 8.1 – Smart contract da blockchain na borda

```
contract DeviceAuthGeo {
    address public owner;

    mapping(bytes32 => bytes32) private deviceCodeHash;
    mapping(bytes32 => bytes32) public activeToken;
    mapping(bytes32 => uint256) public tokenExpiry;

    uint256 public tokenTTLSeconds = 15 minutes;

    event DeviceRegistered(bytes32 indexed deviceId);
    event Authenticated(bytes32 indexed deviceId,
        bytes32 sessionToken, uint256 expiresAt);
    event LocationRecorded(bytes32 indexed pseudoId,
        int32 latE7, int32 lonE7, uint256 timestamp);

    modifier onlyOwner() {
        require(msg.sender == owner, "only_owner");
        _;
    }

    constructor() {
        owner = msg.sender;
    }
}
```

```
function registerDevice(bytes32 deviceId, bytes32 codeHash)
external onlyOwner {
    require(deviceId != bytes32(0));
    require(codeHash != bytes32(0));
    deviceCodeHash[deviceId] = codeHash;
    emit DeviceRegistered(deviceId);
}

function authenticate(bytes32 deviceId, string calldata code)
external
returns (bytes32 sessionToken)
{
    bytes32 stored = deviceCodeHash[deviceId];
    require(stored != bytes32(0));

    bytes32 providedHash = keccak256(abi.encodePacked(code));
    require(providedHash == stored);

    sessionToken = keccak256(
        abi.encodePacked(block.prevrandao, block.timestamp,
            msg.sender, deviceId)
    );

    activeToken[deviceId] = sessionToken;
    tokenExpiry[deviceId] = block.timestamp + tokenTTLSeconds;

    emit Authenticated(deviceId, sessionToken, tokenExpiry[deviceId]);
    return sessionToken;
}

function recordLocation(
    bytes32 deviceId,
    bytes32 sessionToken,
    int32 latE7,
    int32 lonE7,
    bytes32 pseudoId
) external {
    require(activeToken[deviceId] == sessionToken);
    require(block.timestamp <= tokenExpiry[deviceId]);
```

```

        require(latE7 >= -9000000000 && latE7 <= 9000000000);
        require(lonE7 >= -18000000000 && lonE7 <= 18000000000);

        emit LocationRecorded(pseudoId , latE7 , lonE7 ,
                               block.timestamp);
    }
}

```

8.2 Smart contract da blockchain na nuvem

O smart contract da blockchain na nuvem implementa o mecanismo de ancoragem do estado da blockchain da borda, registrando evidências criptográficas associadas a uma sequência monotônica por identificador da cadeia da borda.

Trecho de Código 8.2 – Smart contract de ancoragem na blockchain na nuvem

```

contract EdgeAnchoring {
    struct AnchorRecord {
        bytes32 anchor;
        uint256 sequence;
        uint256 timestamp;
        address submitter;
    }

    mapping(bytes32 => AnchorRecord) private latest;
    mapping(bytes32 => mapping(uint256 => AnchorRecord))
    private history;

    event Anchored(
        bytes32 indexed edgeChainId,
        bytes32 indexed anchor,
        uint256 indexed sequence,
        uint256 timestamp,
        address submitter
    );

    function anchorState(bytes32 edgeChainId, bytes32 anchor,
        uint256 sequence) external {
        AnchorRecord memory last = latest[edgeChainId];
    }
}

```

```

    if (last.sequence == 0) {
        require(sequence == 1);
    } else {
        require(sequence == last.sequence + 1);
    }

    AnchorRecord memory rec = AnchorRecord({
        anchor: anchor,
        sequence: sequence,
        timestamp: block.timestamp,
        submitter: msg.sender
    });

    latest[edgeChainId] = rec;
    history[edgeChainId][sequence] = rec;

    emit Anchored(edgeChainId, anchor, sequence, block.timestamp,
msg.sender);
}

function latestAnchor(bytes32 edgeChainId) external view returns
(bytes32) {
    return latest[edgeChainId].anchor;
}

function latestSequence(bytes32 edgeChainId) external view returns
(uint256) {
    return latest[edgeChainId].sequence;
}

function getBySequence(bytes32 edgeChainId, uint256 sequence)
    external
    view
    returns (bytes32, uint256, address)
{
    AnchorRecord memory r = history[edgeChainId][sequence];
    return (r.anchor, r.timestamp, r.submitter);
}
}

```

9 Pontuação de trabalhos na Revisão Sistemática

A Tabela 10, apresentada no Apêndice, consolida a avaliação dos estudos selecionados com base nos Critérios de Qualidade definidos neste trabalho. Nesse apêndice, são detalhadas as pontuações atribuídas a cada artigo considerado elegível após as etapas de triagem, permitindo uma visão transparente e estruturada do processo de seleção. Essa organização visa melhorar a legibilidade da seção de Trabalhos Relacionados, ao mesmo tempo em que mantém disponível, para consulta, o conjunto completo de avaliações que fundamentam a escolha dos estudos analisados.

Referência	CQ1	CQ2	CQ3	CQ4	Pontuação
(ZHAO et al., 2020)	–	–	✓	✓	2
(SHAHID et al., 2019)	✓	✓	✓	–	3
(LV; QIU; MENG, 2022)	✓	–	–	–	1
(YADAV et al., 2020)	✓	–	✓	–	2
(GUL; PAUL, 2022)	✓	–	✓	✓	3
(SHRIVASTAVA; DWIVEDI, 2022a)	✓	–	–	–	1
(SAKTHI et al., 2022)	✓	✓	✓	✓	4
(LI et al., 2019)	✓	✓	✓	–	3
(TOKKOZHINA et al., 2023)	✓	–	✓	✓	3
(LEAL; PISANI; ENDLER, 2021)	✓	✓	✓	✓	4
(SHAHZAD; ZHANG; GHERBI, 2020)	✓	✓	–	–	2
(ZHANIKEEV, 2019)	–	✓	✓	–	2
(WU et al., 2020)	✓	✓	✓	✓	4
(GUAN et al., 2021)	✓	✓	✓	✓	4
(AL-QARAFI et al., 2022)	✓	✓	–	–	2
(LV et al., 2020)	✓	✓	✓	✓	4
(KIM; CHOI; JANG, 2018)	✓	–	✓	–	2
(GEHLOT et al., 2022)	–	–	–	–	0
(MUNASINGHE; HALGAMUGE, 2023)	✓	✓	✓	✓	4
(LIU et al., 2023)	✓	✓	✓	✓	4
(REN et al., 2023)	✓	✓	✓	✓	4
(ZIA, 2021)	✓	–	✓	✓	3
(WANG; LIU; ZHAO, 2022)	✓	✓	✓	–	3
(ZOU et al., 2019)	✓	✓	✓	✓	4
(SAAD et al., 2023)	✓	✓	✓	–	3
(KAUSHIK; PILLAI, 2021)	✓	✓	✓	–	3
(ALEXANDRIDIS et al., 2022)	✓	–	✓	–	2
(WEERAPANPISIT et al., 2022)	✓	✓	✓	✓	4
(BAUCAS; SPACHOS, 2023)	✓	–	✓	✓	3
(RENGAN, 2023)	–	–	–	–	0
(LIYANAGE et al., 2022)	✓	–	–	–	1
(NASRULIN; MUZAMMAL; QU, 2018)	✓	✓	✓	–	3
(SUN et al., 2021)	✓	✓	✓	✓	4
(AMORETTI et al., 2018)	✓	✓	✓	–	3
(NOSOUHI et al., 2020)	✓	✓	✓	–	3
(ZHANG et al., 2020)	✓	✓	✓	✓	4
(DEDEOGLU et al., 2019)	✓	✓	✓	✓	4
(LIANG et al., 2020)	✓	✓	✓	✓	4
(DONG et al., 2025)	✓	✓	✓	✓	4
(PEELAM; SHAH; CHAMOLA, 2026)	✓	✓	✓	✓	4
(GAVRILĂ et al., 2025)	✓	✓	✓	✓	4
(RABIEI et al., 2025)	✓	✓	✓	✓	4
(RAWAL; SEEDORF; PATIL, 2025)	✓	✓	✓	✓	4
(LAMBA et al., 2026)	–	–	✓	✓	2
(QU et al., 2026)	✓	✓	✓	✓	4
(PEELAM; SHAH; CHAMOLA, 2024)	✓	✓	✓	✓	4
(DRAUGELYTĖ; SUZDALEV, 2025)	✓	✓	✓	✓	4
(ALONSO-NÚÑEZ; LLANOS, 2025)	✓	✓		✓	4
(KHAN et al., 2025)	–	–	✓	✓	2
(AL-WESABI et al., 2025)	✓	✓	–	✓	3

Tabela 10 – Resultado da seleção de trabalhos a partir dos Critérios de Qualidade