UNIVERSIDADE FEDERAL DO CEARÁ

DEPARTAMENTO DE ENGENHARIA

CURSO DE GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

THIAGO ABREU LOPES

A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DE ESTRATÉGIAS BASEADAS EM BLOCKCHAIN PARA ARMAZENAMENTO DE DADOS EM APLICAÇÕES DE INTERNET DAS COISAS

SOBRAL

2023

THIAGO ABREU LOPES

A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DE ESTRATÉGIAS BASEADAS EM BLOCKCHAIN PARA ARMAZENAMENTO DE DADOS EM APLICAÇÕES DE INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Computação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Computação.

Orientador: Prof. Dr. Wendley S. Silva

SOBRAL

2023

THIAGO ABREU LOPES

A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DE ESTRATÉGIAS BASEADAS EM BLOCKCHAIN PARA ARMAZENAMENTO DE DADOS EM APLICAÇÕES DE INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Computação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Computação.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Wendley S. Silva (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Erick Aguiar Donato
Universidade Federal do Ceará (UFC)

Marcelo Franco Vieira
Universidade Federal do Ceará (UFC)

Aos meus pais, por todo sacrifício e esforço para me oferecer a melhor educação possível. Minha mãe, pelas noites mal dormidas, preocupações e toda dedicação. Meu pai, por todas as madrugadas trabalhando, ensinamentos e todo suporte ao longo dessa caminhada. Muito Obrigado!

AGRADECIMENTOS

Ao Prof. Dr. Wendley S. Silva, Professor Adjunto 4 da Universidade Federal do Ceará, campus Sobral, pela orientação na construção do meu trabalho de conclusão de curso.

Ao Prof. Dr. Reuber Regis de Melo, professor Adjunto na Universidade Federal do Ceará do campus de Russas, pela motivação nos estudos da área de Internet das Coisas e Automação.

Ao Doutorando em Engenharia Elétrica, Ednardo Moreira Rodrigues, e seu assistente, Alan Batista de Oliveira, aluno de graduação em Engenharia Elétrica, pela adequação do *template* utilizado neste trabalho para que o mesmo ficasse de acordo com as normas da biblioteca da Universidade Federal do Ceará (UFC).

Aos alunos da Universidade Federal do Ceará e meus colegas do Núcleo de Internet das Coisas Vitória Freitas, Anderson Ivanildo, Joyce Ximenes, Nájala Kelly e Lucas Braz pelos momentos experienciados no NUCLIC.

Aos meus amigos Ana Raquel, João Neto, Jorge Ruan, Maria Ianka, Maria Keyllane, Ygor Ribeiro, a pequena Maria Louise e sua mamãe Laís Maria que, nos momentos de minha ausência dedicados aos estudos, sempre compreenderam que o futuro é feito a partir da constante dedicação no presente. Sobrevivemos juntos!

À minha mãe Rita Sousa e ao meu pai Raimundo Nonato, por toda paciência, dedicação e esforço para fazer o seu filho alcançar seus sonhos.

Agradeço a todos os professores por me proporcionar o conhecimento não apenas racional, mas pela manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender.

“O que vale na vida não é o ponto de partida e sim a caminhada. Caminhando e semeando, no fim, terás o que colher.”

(Cora Coralina)

RESUMO

O presente trabalho tem por objetivo a realização de uma Revisão Bibliográfica Sistemática a fim de verificar as contradições presentes entre as normas vigentes na Lei Geral de Proteção de Dados(LGPD) referentes à tecnologia de Internet of Thing(IoT) que fazem uso de tecnologias baseadas em Blockchain para armazenar as informações capturadas. A organização do trabalho se divide nas partes introdutórias que apresenta conceitos a cerca dos termos abordados, na parte de pesquisa que detalha a metodologia adotada para a revisão bibliográfica e a parte conclusiva que sintetiza os resultados obtidos e apresenta as respostas paras as perguntas formuladas aos inicio da formulação da revisão.

Palavras-chave: Internet of Things. Lei Geral de Proteção de Dados. Blockchain. Revisão Bibliográfica Sistemática.

ABSTRACT

The present study aims to carry out a Systematic Bibliographic Review in order to verify the contradictions between the rules in the Brazilian General Data Protection Law(LGPD) reffering to Internet of Things(IoT) technology that make use of technologies Bockchain-based to store the captured information. The organization of this study is divided into introductory parts that present concepts about the terms addressed, the sistematic research part that details the methodology adopted for bibliographic review and the conclusive part which summarizes the result obtained and presents the answers to the questions asked to the beginning of the formulation of the review.

Keywords: Internet of Things. General Data Protection Law. Blockchain. Systematic Bibliographic Review.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CDC	Código de Defesa do Consumidor
GDPR	General Data Protection Regulation
IoT	Internet of Things
IoTWF	The Iot World Forum
IT	Information Technology
LGPD	Lei Geral de Proteção de Dados
OT	Operational Technology
RBS	Revisão Bibliográfica Sistemática

SUMÁRIO

1 INTRODUÇÃO

Os dispositivos de Internet of Things (IoT) são uma tecnologia emergente que consolidou seu espaço no mercado tecnológico mundial de tal modo, que acredita-se que em 2025 haverão cerca de 100 bilhões de dispositivos conectados na internet e que movimentará cerca de 11 trilhões de dólares. Isso se resulta da aplicação em larga escala desses dispositivos que possibilita o surgimento das mais variadas soluções, desde automação residencial, ao gerenciamento de energia, gerenciamento água em plantações, etc. (ROSE *et al.*, 2015).

Para essa finalidade, são necessários inúmeros sensores, atuadores e outros dispositivos que permitem a comunicação entre eles, ou seja, uma quantidade substancial de dados são coletados e armazenados continuamente a fim de manter a qualidade dos serviços desses aparelhos (SCHWAB, 2016) e uma tecnologia, também emergente, que vem sendo amplamente difundida para atuar nessa movimentação de dados são métodos baseados em blockchain (DON; TAPSCOTT, 2016).

A tecnologia blockchain se diferencia das demais maneiras de armazenamento de dados por ser um método descentralizado de persistência e criptografia e por dificultar significativamente a alteração ou eliminação dos dados da cadeia e, quando unido aos dispositivos IoT, obtém-se uma versão facilitadora de transações, processamento e coordenação de informações entre os dispositivos conectados (PURESWARAN; BRODY, 2015).

Essa junção entre IoT e blockchain, apesar de muito eficiente no que se propõe a realizar, acabam por deixar um questionamento no que diz respeito ao modo como esses dados são tratados no sentido legal do termo.

A legislação que rege a utilização de dados no Brasil é a Lei Geral de Proteção de Dados (LGPD), na qual ficam estabelecidos todos os meios para proteção dos dados armazenados e todos os direitos dos usuários no que diz respeito a privacidade e resguardo de sua informações pessoais, proteção essa que se torna discutível quando voltado a Blockchain aplicados ao IoT, seja pela sua característica descentralizada, pela sua rigidez com a alteração ou exclusão de informações (BRASIL, 2018).

Este trabalho visa trazer uma revisão bibliográfica sobre a perspectiva da LGPD acerca da tecnologia blockchain aplicado à dispositivos IoT e identificar o estado da arte a respeito desse tema.

1.1 Motivação do Trabalho

O principal motivador do atual trabalho foi a divulgação de que no ano de 2023 o Governo Federal passou a contar com o uso tecnologias blockchain com a finalidade de validar dados presentes nos novos Registros de Identidade (RG) emitidos, com o intuito de evitar fraudes e tornar serviços públicos mais eficientes (GUSSON, 2023).

Essa divulgação levou ao questionamento sobre o uso dessas informações em ambientes inteligentes e autônomos que fazem uso de tecnologias IoT e blockchain em seus processos e sobre se a LGPD prevê uso de técnicas como essas.

2 OBJETIVOS

2.1 Objetivo Geral

O objetivo deste trabalho é realizar uma revisão bibliográfica a fim de analisar a possibilidade de integração entre os artigos presentes na LGPD e o caráter das tecnologias IoT, que captura dados variados de modo contínuo e massivo, combinado com tecnologias baseadas em blockchain, que descentraliza o armazenamento de informações e impede a alteração de registros persistidos.

2.2 Objetivo Específico

- Conceituar IoT, blockchain e LGPD
- Identificar os contrapontos entre IoT e LGPD
- Identificar os contrapontos entre blockchain e LGPD
- Identificar os contrapontos entre a composição IoT e blockchain com a LGPD
- Comparar as aplicações que compreendem LGPD, IoT e blockchain presentes na literatura
- Identificar os aspectos em comum que possibilita contornar os contrapontos apresentado

3 FUNDAMENTAÇÃO TEÓRICA

3.1 Internet of Things (IoT)

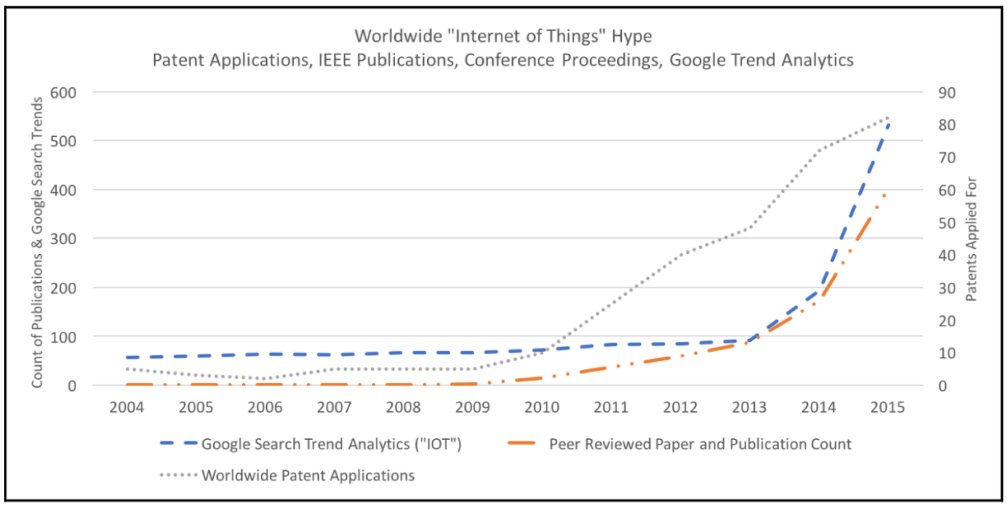
Internet of Things ou Internet das coisas, tem por premissa básica estabelecer conexões onde antes não existia (HIEBERT, 2013), isso é, permitir que dispositivos antes não conectados à rede de Internet passe a ter uma comunicação via rede entre si e entre os usuários do sistema ao qual ele está inserido e, a partir disso, sentir e controlar o mundo físico ao redor tornando objetos inteligentes.

Dadas as diversas utilidades existentes para cada dispositivo, a tecnologia IoT deve ser encarada como uma tecnologia abrangente que envolve diversos conceitos, tecnologias e protocolos dependendo do cenário de aplicação.

Este caráter diverso, portanto, gera inúmeros benefícios como aumento de produtividade e automação de diversos processos e, ao mesmo tempo, gera diversos desafios desde a escalabilidade do contingente de dispositivos até, e principalmente, a grande quantidade de dados a serem processados e armazenados (HANES *et al.*, 2017).

Experimentos visando implementar artefatos conectados à redes de comunicação são realizados desde os anos 70 como demonstrado na Tabela 1 e desde então a popularidade do tema IoT escalou quase que de maneira exponencial desde o surgimento das primeiras pesquisas sobre a tecnologia em 2009 como demonstrado na Figura 1 (LEA, 2018).

Figura 1 – Crescimento do Termo IoT em diferentes Contextos



Fonte: Adaptação de (LEA, 2018)

Tabela 1 – Linha do tempo dos Objetos Conectados à Rede

Ano	**Dispositivo**
1973	Mario W. Cardullo recebe a primeira patente da primeira etiqueta RFID
1982	Máquina de refrigerante conectada à internet na Universidade de Carnegie Mellon
1989	A torradeira conectada à internet apresentada na Interop '89
1991	HP apresenta a HP LaserJet IIISi, a primeira impressora a se conectar à internet
1993	Primeira câmera conectada à internet na cafeteria da Universidade de Cambridge
1996	General Motors lança a OnStar para diagnóstico remoto dos veículos
1998	Formação da SIG para o estudo sobre o Bluetooth
1999	LG lança a Internet Digital DIOS Regrigerator
2000	Primeiro conceito da Cooltown(smartcity) criada pela HP que combinava comunicação e tecnologia entre diferentes dispositivos, locais e pessoas
2001	Lançamento do Primeiro produto contendo conexão Bluetooth, o telefone móvel KDDI
2005	A União Internacional de Telecomunica coes das Nações Unidas prevê a ascensão do IoT pela primeira vez
2008	A aliança IPSO promove a criação de IPs para objetos, primeira aliança voltada à IoT
2010	O conceito de Smart Lightning e formado após o desenvolvimento das primeiras lâmpadas LED
2014	Apple cria o IBeacon, um protocolo para beacons

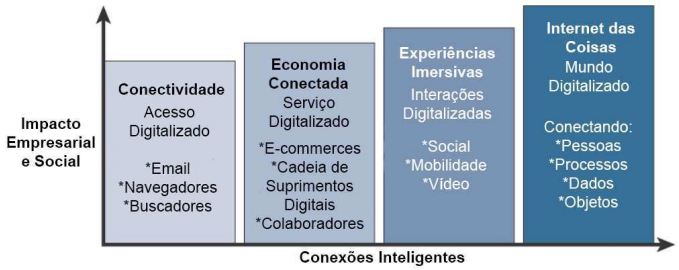
Fonte: Adaptação de (LEA, 2018)

3.1.1 Gênesis do IoT

Apesar do termo ter sido cunhado em 1999 por Kevin Ashton para designar suas ideias acerca de integração entre os suprimentos da empresa que ele trabalhava na época e, durante um tempo ser restrito a tecnologia RFID, o conceito atual de IoT só ganhou significado atual entre os anos de 2008 e 2009, anos esses os quais houveram diversos avanços nas tecnologias de comunicação, bem como o barateamento dessas tecnologias, permitiu que o total de dispositivos conectados a internet ultrapassasse o número de pessoas no planeta (LEA, 2018).

Dispositivos IoT serão responsáveis por impactos significativos em muitos aspectos da vida das pessoas ao redor do mundo (KOON, 2019), ademais é considerado um importante etapa na evolução da internet como demonstrado na Figura 2.

Figura 2 – Fases da Evolução da Internet



Fonte: Adaptação de (HANES *et al.*, 2017)

Tabela 2 – Fases da Evolução da Internet

Fase da Internet	**Definição**
Conectividade	Essa fase houve conexão de pessoas via email, serviços e pesquisa na web, então a informação se tornou de mais fácil acesso
Economia Conectada	Essa fase possibilitou o surgimento de e-commerce e o entrelaçamento de processos colaborativos e o aumento na eficiência dos negócios
Experiência Imersiva	Essa fase estendeu a Internet ao cotidiano das pessoas através da abrangência de vídeos e mídias sociais em tecnologias móveis. Mais e mais aplicações são realizadas na tecnologia Cloud
Objetos Conectados	Essa fase adiciona conectividade a objetos e máquinas no mundo ao redor e possibilita novos serviços e experiências com o mundo antes desconectado

Fonte: Adaptação de (HANES *et al.*, 2017)

Cada fase é uma evolução direta da fase anterior e para cada uma delas é dada sua devida importância às realizações geradas por eles em seus períodos.

A primeira fase retrata o começo da conectividade, principalmente em universidades, corporações e meios militares com os primeiros e-mails enviados e os primeiros buscadores desenvolvidos. A segunda fase possibilitou a primeira grande disruptura econômica na era digital com o surgimento da Economia em Rede e dos primeiros *e-commerce*, houve uma maior interconectividade entre compradores vendedores e distribuidores e o surgimento de grandes empresas de tecnologias mundo a fora.

A terceira fase gerou uma maior integração dos meios digitais com o dia a dia dos usuário, integração essa provocada principalmente pelo surgimento de redes sociais e de dispositivos moveis que possibilitou o acesso a diversos meios e canais de comunicação em massa.

Por fim, a última fase, a qual está apenas em seu início, retrata a possibilidade de conexão entre dispositivos, objetos e usuários, a fim de tornar mais eficientes os diversos setores da sociedade e, a longo prazo, tornando os dispositivos IoT agentes modificadores do mundo assim como as demais tecnologias desenvolvidas nas fases da Internet (HANES *et al.*, 2017).

3.1.2 Arquitetura dos dispositivos IoT

A arquitetura de sistemas é amplamente discutida quando se trata de tecnologia ligadas ao Information Technology (IT) e quanto ao Operational Technology (OT) e durante muito tempo foram utilizadas arquiteturas voltadas a esses sistemas para tratar acerca de sistemas IoT.

Contudo, diferente de sistemas IT e OT, em que o objetivo é voltado à disponibilidade de suporte contínuo para aplicações de negócios ou de maquinários, os sistemas IoT se destinam a recolher diversos dados gerados por sensores e utilizar esses dados como convém para aplicação e, portanto, a arquitetura de sistemas IoT passou a envolver tema como o transporte, coleta, análise e ações através das informações capturadas pelos dispositivos.

Em 2017, o The Iot World Forum (IoTWF) estabeleceu uma padronização de arquitetura de aplicações IoT baseado em sete camada ilustrado na Figura 3.

Figura 3 – Arquitetura IoT

Fonte: Adaptação de (MODEL, 2017)

A seguir será pontuado, brevemente, cada uma das camadas de acordo com (MODEL, 2017):

- **Camada Física:** Consiste nos diversos equipamentos que serão aplicados no sistema - sensores, câmeras, atuadores, etc, - Podendo os tamanhos desses dispositivos variar desde equipamentos nanométricos à gigantes maquinas. A principal função dessa camada é gerar

os dados a serem utilizados no processo.

- **Camada de Conectividade:** Responsável pela disponibilidade e velocidade na transmissão dos dados em trânsito. Nessa camada são incorporados os elementos de rede computacional - roteamento, gateway, switch, comunicação entre protocolos, etc.
- **Camada Computação de Borda:** Responsável pela redução e na conversão do fluxo de dados em informação útil, permitindo geral alertas e notificações acerca das informações obtidas. Além disso, cuida da formatação e dos processamentos para a camada seguinte.
- **Camada de Acúmulo de Dados:** Armazena os dados processados para utilização em aplicações quando necessário e converte dados baseado em eventos para processamento baseado em consulta.
- **Camada de Abstração de Dados:** Concilia diversos formatos de dados e garante a consistência das diversas fontes desses dados. Confirmar se o conjunto de dados necessário para a aplicação está completo e consolida a informação via virtualização.
- **Camada de Aplicação:** Interpreta os dados a partir de aplicações de softwares. A aplicação pode reportar, monitorar e controlar os processos de acordo com a análise dos dados.
- **Camada de Colaboração:** Consumo e compartilhamento da informação da aplicação. Útil para melhorias nas etapas de negócios - eficiência de processos, segurança, experiência do usuário, redução de custos, etc.

Apesar de ser um modelo de referência dentre outros existentes, o modelo proposto pelo IoTWF se torna bastante útil para resolver alguns problemas na etapa de desenvolvimento como dividir os problemas envolvendo IoT em pequenas partes, identificar as tecnologias necessárias para cada etapa, definir os sistemas e os fornecedores de cada camada, definição dos processos e interfaces e o estabelecimento de modelos de segurança entre os níveis.

3.1.3 Desafios das Tecnologias IoT

Alguns obstáculos ainda impedem as tecnologias IoT de se tornarem onipresentes no dia a dia dos usuários e das indústrias. A Tabela 3 descreve alguns desafios que o sistema IoT ainda enfrenta.

Tabela 3 – Desafios da Tecnologia IoT

Desafio	**Descrição**
Escala	Enquanto a escala das redes IT podem abranger uma certa largura, a escala dos dispositivos IoT podem abranger magnitudes de largura. Os sistemas IT ainda utilizam o sistema de IP IPv4 enquanto que para conseguir abarcar todos os componentes conectados em um sistema IoT é necessário o sistema IPv6 que possibilita a conexão e identificação de milhões de dispositivos
Big Data e Análise de Dados	Com o grande número de sensores presentes nos sistemas IoT, o grande desafio passa a ser como determinar o valor desses dados e como processa-los da maneira mais eficiente levando em consideração as diversas fontes e a frequência de captura desses dados
Interoperabilidade	Como toda e qualquer tecnologia emergente, existem vários protocolos e arquiteturas que permeiam o mercado de IoT. Alguns desses protocolos e arquiteturas são elementos proprietários e outros são abertos para o publico em geral. Apesar de já existirem algumas arquiteturas propostas que ajudam a reduzir esse problema
Segurança	Com mais "coisas" conectadas e mais pessoas envolvidas nos processos, mais cresce a complexidade da segurança em sistemas IoT, ou seja, uma superfície de ataque maior e, caso seja invadido, as consequências tende a ser mais desastrosas dado a sua concatividade
Proteção dos Dados	Como os sensores se tornaram comuns no cotidiano, muitos dados específicos são capturados continuamente. Esses dados podem abranger desde informações sobre saúde ate padrões de consumo e transações. Para empresas, esses dados possuem valor monetário e muito se discute sobre a propriedade, o controle e o compartilhamento desses dados

Fonte: Adaptação de (HANES *et al.*, 2017)

Em outro estudo, Rob Van Kranenburg e Alex Bassi (KRANENBURG; BASSI, 2012), apresentam como desafio para as tecnologias IoT a falta de cooperação global, a desconfiança nos modelos de negócio atuais, problemas éticos no que se refere aos dados, os desafios tecnológicos e o equilíbrio entre inovação e planejamento. Invariavelmente, ambos os estudos apresentam, de modo semelhante, problemas relacionadas ao tratamento de dados, o que demonstraria que em diversos cenários esse é um problema que ainda impede significativamente o desenvolvimento e aplicação das tecnologias IoT (KRANENBURG; BASSI, 2012).

3.2 Blockchain

O protocolo blockchain teve seu início focado em transferências financeiras digitais e, pouco a pouco, foi sendo aplicado em setores como gerenciamento de dados de saúde, gerenciamento de cadeia de suprimentos, monitoramento do mercado financeiro, gerenciamento inteligente de energia e proteção de direitos autorais (XU *et al.*, 2019).

Dada essa expansão houve o crescente número de estudos que buscavam aplicar blockchain a outras áreas como a de conexão peer-to-peer, criptografia, contratos inteligentes, algoritmo de consenso e armazenamento de dados distribuídos (XU *et al.*, 2019).

3.2.1 Gênesis do BlockChain

Em meio ao recesso econômico de 2008, Satoshi Nakamoto, uma pessoa anônima ou um grupo de pessoas, criou um protocolo para uma criptomoeda chamada Bitcoin. Batizado de blockchain, o protocolo em questão permitia realizar transações sem a necessidade de um terceiro agente fiscalizador, pois sua modelagem garantiria a integridade das transações (VYAS *et al.*, 2019).

Em 2013, a criação do *ETHEREUM* promove uma nova etapa na evolução do blockchain com o surgimento dos contratos inteligentes, que são contratos que executam todos os seus estágios automaticamente, tornando o protocolo naquilo que ele é conhecido atualmente (POPOVSKI; SOUSSOU, 2018).

Apesar de ser muito atribuído à instituições financeiras, dado seu papel na redução de custos e no aprimoramento da eficiência dos processos contábeis, o blockchain vem sendo adaptado para outro serviços como gerenciamento da cadeia de suprimentos da empresa e armazenamento de dados, os chamados sistemas baseados em blockchain (KSHETRI, 2018).

3.2.2 Funcionamento da tecnologia BlockChain

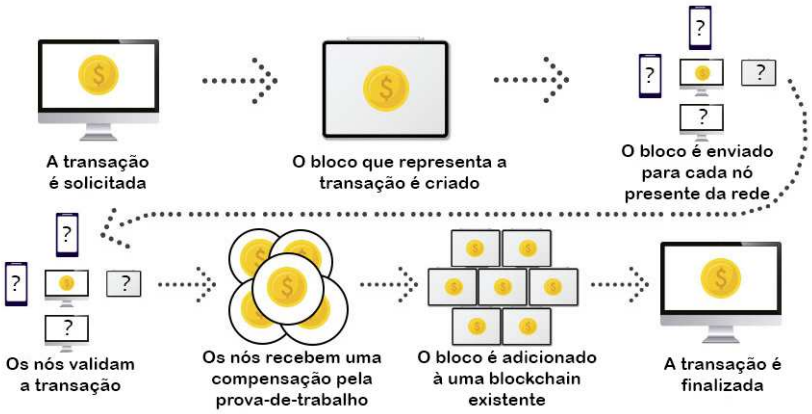
O blockchain funciona como um banco de dados distribuído e partilhado via peer-to-peer, atuando como uma sequência de blocos com os registros de data e hora guardados por uma criptografia de chave pública, podendo ser aferido por qualquer usuário envolvido dado que, a partir do momento que um bloco novo entra na sequência ele não pode ser modificado (SEEBACHER; SCHüRITZ, 2017).

Ao preencher um bloco é necessário realizar sua validação e para isso utiliza-se

a *Proof-of-Work* que consiste na verificação da etapa de mineração, em que se busca resolver uma operação matemática de um determinado problema que é difícil de se obter a resposta, mas um vez obtida essa resposta se torna fácil verificar se a resposta é correta (SEEBACHER; SCHüRITZ, 2017).

A verificação se determinado bloco faz parte ou não da sequência se dá via criptografia de chave pública-privada, na qual os participantes assinam as informações compartilhadas com as chaves privadas e compartilham a chave pública para que outros possam realizar essa verificação e, como cada movimentação na corrente se registra também um código hash referente a movimentação anterior e a seguinte, é impossível alterar as informações sem que esses códigos hash sejam alterados juntos tornando as informações carregadas pelos blocos inalteradas enquanto a corrente existir (ZHAO *et al.*, 2016).

Figura 4 – Funcionamento da Tecnologia Blockchain



Fonte: Adaptação de (UJJWAL, 2023)

Por conta desses mecanismos a tecnologia blockchain apresenta suas três principais características como apresentadas na tabela 4 adaptada de (HACKIUS; PETERSEN, 2017).

Tabela 4 – Propriedades da BlockChain

Propriedade	**Descrição**
Transparência	Livro-razão distribuído: uma versão digital de um livro-razão para acompanhar e seguir dados
Descentralizado	Conceito de Peer-to peer: Trocas são realizadas diretamente entre quem envia e quem recebe, sem intermediários
Segurança	Criptografia: No momento que a transação é aprovada, os dados constroem um bloco que será incluído na blockchain e jamais ser alterado

Fonte: Adaptação de (HACKIUS; PETERSEN, 2017)

3.2.3 Armazenamento distribuído baseado em blockchain

Os sistemas de armazenamentos centralizados se caracterizam pela presença de servidores que realizam o estoque de dados que pode ser acessado a depender das regras determinadas pelo gerente do banco de dados e, para um funcionamento eficaz do mesmo, é necessário que apresente uma alta performance, uma alta disponibilidade e uma alta segurança (FOXBIT, 2019).

Com o advento das aplicações de larga escala e a crescente rede de dados gerada por aplicações recentes, os sistemas centralizados vem sendo gradualmente substituídos por métodos de armazenamento de dados distribuídos, isso é, sistemas que distribuem dados através de múltiplos servidores que permite a segurança e eficiência necessária para as novas aplicações (RAWAT *et al.*, 2016).

Apesar de ser uma solução eficiente para os problemas de armazenamento padrão, os sistemas distribuídos enfrentam três tipos de problemas, como apresentado na Tabela 5.

Tabela 5 – Problemas dos Sistemas de Armazenamento Distribuídos

Problema	**Descrição**
Segurança de Dados	Quando um dos equipamentos servidores falha ou ocorre um problema da rede algum dado importante pode ser perdido, além disso existe a possibilidade de ataques maliciosos aos dados
Gerenciamento de Dados	Como os dados são depositados em equipamentos diferentes, podem ocorrer inconsistências ente os tipos de dados, além de diferentes versões de sistemas entre os equipamentos conflitarem entre si
Problemas de Desempenho	Problemas decorrentes de possibilidade de expansão ou de otimização de rede

Fonte: Adaptação de (WANG *et al.*, 2021)

A combinação de blockchain a esses sistemas de estoque distribuídos surge para resolver esses problemas e prover a segurança necessária para a aplicação dessa tecnologia em diversas áreas com as *smart grids*, *smart homes* e *Internet of Vehicles* (WANG *et al.*, 2021).

3.2.4 IoT e Blockchain

Entendendo os desafios das tecnologias IoT, é possível entender o porquê da combinação entre elas e o blockchain é tão eficaz. As tecnologias blockchain podem ofertar diversos

benefícios. A necessidades ao entorno da segurança de dados continua a crescer constantemente, principalmente dado a quantidade de dados coletados pelos sensores dos dispositivos IoT (CHAKRABORTY *et al.*, 2023).

A integração entre IoT e blockchain confere as seguintes características ao sistema ao qual serão implementados (REYNA *et al.*, 2018):

- **descentralização e escalabilidade**: remove problemas que podem existir decorrentes a um servidor central e problemas de gargalo. Além de reduzir os silos IoT e contribui para a escalabilidade do IoT;
- **Identidade**: cada participante de uma cadeia blockchain pode identificar os dispositivos presente na cadeia e com isso pode ter a certeza que o sistema é confiável;
- **Autonomia**: com blockchain os dispositivos podem interagir sem a necessidade de um servidor central permitindo o surgimento de aplicações desacopladas;
- **Confiabilidade**: as informações dentro da blockchain são imutáveis e todos os participantes podem autentificar cada dado vinculado a ela;
- **Segurança**: os dados sensíveis persistidos são protegidos pelo uso de criptografias eficientes;
- **Serviços de Mercado**: blockchain pode acelerar serviços e dados de *marketplaces*, onde transações podem ser realizadas sem uma autorização externa;
- **Implantação de código seguro**: tomar as características imutáveis de armazenamento de dados do blockchain pode prover mais segurança para os dispositivos conectados em rede.

Ambos, tanto o IoT quanto as tecnologias blockchain tornam possível o surgimento de diversas aplicações que concatenam o benefício das duas tecnologias e o papel mais proeminente da blockchain em meio aos controladores do dispositivos IoT é armazenar os dados de maneira descentralizada (SACHDEVA; ALI, 2021).

3.3 Leis Para Proteção de Dados

3.3.1 Primeiras Leis Sobre Informações Pessoais no Brasil

A proteção de informações pessoais no Brasil já é algo estabelecido na Constituição desde sua implantação em 1988 no qual o art. 5º descreve o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas (BRASIL, 1988).

Já em 1993 o Código de Defesa do Consumidor (CDC) estabelece que todo con-

sumidor tem o direito de acesso e de correção de dados cadastrados por empresas (BRASIL, 1990).

Em 1996 é aprovado a Lei 9.296 a qual descreve como inviolável o sigilo das correspondências e das comunicações telegráficas, salvo por ordem judicial (BRASIL, 1996).

3.3.2 Lei Carolina Dieckmann ou Lei de Crime Cibernéticos

Apenas em 2012 que as comunicações digitais e via internet entraram no radar das legislações brasileiras com a Lei nº 12.737, conhecida como "Lei Carolina Dieckmann", aprovada mediante um acontecimento marcante no âmbito nacional. A atriz Carolina Dieckimann teve seu computador pessoal invadido e suas informações pessoais e fotos íntimas expostas na rede, causando um constrangimento para a triz e tal fato levou a rápida aprovação da lei em questão.(BRITO, 2020).

A "Lei Carolina Dieckmann"ou Lei de Crime Cibernéticos descreve que invasões à dispositivos alheios conectados ou não a rede, violando mecanismos de segurança, visando obter, adulterar ou destruir dados sem autorização do titular passam a ser considerados crime puníveis com prisão (BRASIL, 2012).

3.3.3 Marco Civil da Internet

Em meio ao crescente número de aplicações digitais e com a expansão da internet em todos os cenários no Brasil em 2014, observou-se alguns aspectos que até então não se havia discutido. Dentre esses aspectos cabe citar a proteção de registros, os dados pessoais em comunicações privadas, a neutralidade da rede, a responsabilidade civil de provedores de conexão e aplicação e as questões judiciais acerca desses registros (TEFFé; MORAES, 2017).

Os princípios que regem a Lei do Marco Civil(LEI Nº 12.965, DE 23 DE ABRIL DE 2014) são garantir a liberdade de expressão, proteger a privacidade, proteção de dados pessoais, preservação da neutralidade da rede, preservar a estabilidade da rede, responsabilizar agentes de acordo com a sua atividade, preservar a participação da rede e prover a liberdade aos modelos de negócios promovidos na internet (BRASIL, 2014).

3.3.4 Cenário Pré-Lei Geral de Proteção de Dados

Em 2015, ano anterior às eleições Americanas que consagraram o candidato Republicano Donald Trump como o 45º presidente do país, a empresa de consultoria política *Cambridge Analytica* se viu em um escândalo envolvendo a utilização indevida dos dados de oitenta e sete milhões de eleitores americanos a fim de identificar seus interesses e comportamentos e assim contribuir para a campanha presidencial de Trump (ISAAK; HANNA, 2018).

Esse vazamento de informações pessoais por parte da empresa levou ao surgimento de debates que resultaram na a aprovação da lei europeia de proteção de dados, a chamada General Data Protection Regulation (GDPR) que passou a reger toda a segurança de dados em território europeu e inspirou o surgimento da LGPD no Brasil (RAPôSO *et al.*, 2019).

3.3.5 Lei Geral de Proteção de Dados (LGPD)

Sancionada em agosto de 2018 pelo então presidente da República Michel Temer, a Lei Nº 13.709 ou LGPD tem por objetivo proteger as informações pessoais e a transparência no tratamento e armazenamento dos dados. Para isso, possui 65 artigos que visam detalhar os métodos de utilização dos dados privados de terceiros (AGOSTINELLI, 2018).

A lista abaixo traz o resumo dos artigos mais importantes que compõem a (BRASIL, 2018):

- Artigo 1 trata do objetivo da LGPD;
- Artigo 2 apresenta a Fundamentação para essa proteção;
- Artigos 3 e 4 tratam dos destinatários dessa lei, quando ela deve ser aplicada e sua excussões;
- Artigo 5 apresenta as definições de alguns termos importantes para entender a lei;
- Artigo 6 define os princípios a serem observados pelas entidades que tratarão dos dados;
- Artigo 7 trata a respeito da liberdade de concessão do uso dos dados do usuário;
- Artigo 8 trata como o consentimento para captura e uso de dados deverá ser estabelecido;
- Artigos 9 e 10 tratam dos direitos do titular e os limites do controlador;
- Artigo 11 estabelece a possibilidade de uso de dados sensíveis;
- Artigos 12 e 13 detalham cerca dos dados anônimos e os utilizados na saúde pública;
- Artigo 14 traz como devem ser tratados os dados de crianças e adolescentes;
- Artigos 15 e 16 tratam do prazo de tratamento dos dados

- Artigos do 17 ao 22 apresentam os direitos dos titulares;
- Artigos do 23 ao 30 tratam do uso de dados pessoais pelo poder público;
- Artigos do 33 ao 36 tratam da transferência internacional de dados;
- Artigos 42 e 43 tratam do ressarcimento de dados causados pelo controlador dos dados e quando serão responsabilizados;
- Artigos do 46 ao 51 tratam das posturas e boas práticas a serem tomadas para com os dados e do estimulo à adoção de padrões técnicos;
- Artigos 48 e 49 trata da ocorrência de incidentes de segurança;
- Artigos 52 e 53 tratam sobre as sanções contra agentes de tratamento de dados em caso de infrações;
- Artigos do 60 ao 65 tratam da integração dessa lei às demais já existentes como a lei do Marco Civil (Lei Nº 12.965).

4 METODOLOGIA

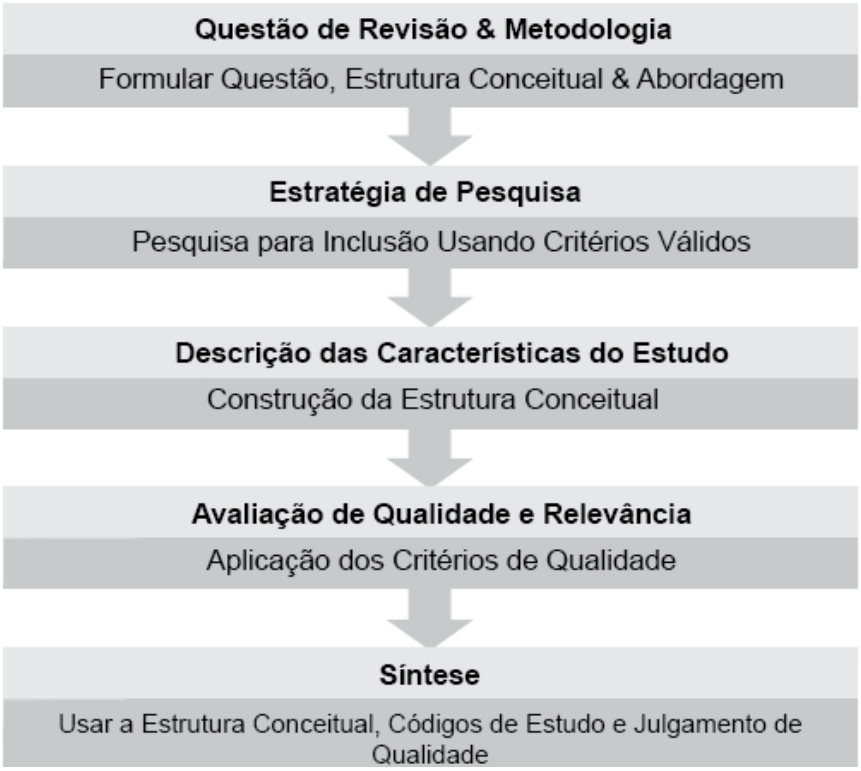
4.1 Revisão Bibliográfica Sistemática

O trabalho em questão visa apresentar uma Revisão Bibliográfica Sistemática (RBS) que, segundo (BOLAND *et al.*, 2014) é projetada visando localizar, avaliar e sintetizar as melhores evidências disponíveis relativa à uma pergunta de pesquisa. Além disso, tem o objetivo de fornecer informações baseadas em evidências seguindo etapas bem definidas e transparentes e que podem ser definidas de diversas maneiras, mas todas elas visam obter uma conclusão relevante.

4.2 Estágios da RBS

Para esse trabalho usar-se-á as etapas definidas por (GOUGH *et al.*, 2012, p. 8) que descrevem cada passo a ser trilhado para a obtenção de uma RBS completa e estão apresentados na Figura 5.

Figura 5 – Etapas de uma RBS



Fonte: Adaptação de (GOUGH *et al.*, 2012)

4.2.1 Pergunta de Revisão e Metodologia

Esta etapa diz respeito a parte de identificar a pergunta que se deseja responder já que, como citado anteriormente, toda RBS visa apresentar a resposta para uma determinada pergunta. Aqui especifica-se a pergunta em questão e reúne-se os interessados para projetar o que de fato se deseja obter com a RBS em questão. Além disso, esta parte também se propõe descrever os métodos e estratégias que serão seguidas para se obter a resposta dessa pergunta (GOUGH *et al.*, 2012, p. 74).

No trabalho em questão a pergunta que se deseja responder é:

"Existe algum tipo de contradição ou incompatibilidade entre as normas determinadas pela LGPD e tecnologias baseadas em blockchain aplicados a dispositivos IoT?"

Para responder essa questão serão utilizados artigos e pesquisas acadêmicas obtidas através de pesquisa no sítio *Google Schoolar* que lista diversos materiais acadêmicos relacionados a termos-chave.

4.2.2 Estratégia de Pesquisa

Nesse passo são estabelecidos os métodos de realização da pesquisa em questão (GOUGH *et al.*, 2012, p. 110).

No caso da RBS em foco, a estratégia se refere aos termos utilizados para realização das pesquisas, que serão um combinação entre os argumentos "LGPD", "IoT", "Blockchain", "Regulação no uso de dados", "regulação do uso de dados", "GDPR". Esses termos foram aplicados a barra de pesquisa de maneira que todos os artigos devam conter obrigatória o/os termo(s) apresentados, ou seja, utilizando a estratégia de colocar os termos entre aspas (“ ”) que, no mecanismo de busca da Google, induz os resultados da pesquisa a conter os termos em questão obrigatoriamente.

A Tabela 6 apresenta o número aproximado de resultados totais na busca de cada termo pesquisado. Os valores apresentados são das pesquisas realizadas entre os dias 15 de setembro 2023 à 25 de setembro de 2023.

Tabela 6 – Número Aproximado de Artigos Referentes à Cada Busca em Ordem Crescente

Termo Pesquisado	**Número de Artigos Encontrados**
"Blockchain"AND "Regulação no uso de dados"	5
"IoT"AND "Regulação no uso de dados"	9
"IoT"AND "Blockchain"AND "LGPD"	510
"LGPD"AND "Blockchain"	1.270
"LGPD"AND "IoT"	1.560
"LGPD"	16.100
"Blockchain"AND "GDPR"	21.800
"IoT"AND "GDPR"	28.000
"IoT"AND "Blockchain"	279.000
"Blockchain"	610.000
"IoT"	1.960.000
TOTAL	2.667.154

Fonte: Autor

4.2.3 Descrição das Características do Estudo

Nesse passo deve-se estabelecer os critérios de avaliação dos estudos, dado que são diversos textos aprestados pela ferramenta de busca e para que o estudo se torne viável é necessário estabelecer parâmetros sobre quantos e quais serão utilizados (GOUGH *et al.*, 2012, p. 137).

No trabalho em questão serão utilizados artigos de livre acesso, em inglês ou português e que esteja completo que se relacionem com o objetivo do estudo, qualquer artigo que não cumpram com esses parâmetros serão desconsiderados.

Serão avaliados nesses critérios até os 100 primeiros artigos apresentados por busca, os demais artigos serão desconsiderados a fim de manter o trabalho possível.

Dos trabalhos artigos apresentados na Tabela 6 foram aplicados os critérios anteriormente citados e como resultado temos os números de artigo obtidos para esse trabalho na Tabela

Tabela 7 – Número de Artigos Referentes à Cada Busca ao Aplicar os Critérios de Características de Estudo em Ordem Crescente

Termo Pesquisado	**Número de Artigos Aceitos**
"Blockchain"AND "Regulação no uso de dados"	2
"IoT"AND "Regulação no uso de dados"	6
"IoT"AND "Blockchain"	32
"IoT"	37
"Blockchain"	38
"IoT"AND "Blockchain"AND "LGPD"	38
"IoT"AND "GDPR"	43
"Blockchain"AND "GDPR"	47
"LGPD"	70
"LGPD"AND "IoT"	72
"LGPD"AND "Blockchain"	85
TOTAL	470

Fonte: Autor

4.2.4 Avaliação de Qualidade e Relevância

Nesse passo, tendo obtido todos os estudos que se relacionam com o tema, deve-se estabelecer um método de avaliação para determinar se o texto em questão tem sentido e relevância para ser incluso na etapa de síntese (GOUGH *et al.*, 2012, p. 156).

No trabalho em foco, os artigos selecionados poderão passar pelas etapas de avaliação apresentadas na Tabela 8, a depender o grau de relevância da obra avaliada:

Tabela 8 – Etapas da Leituras

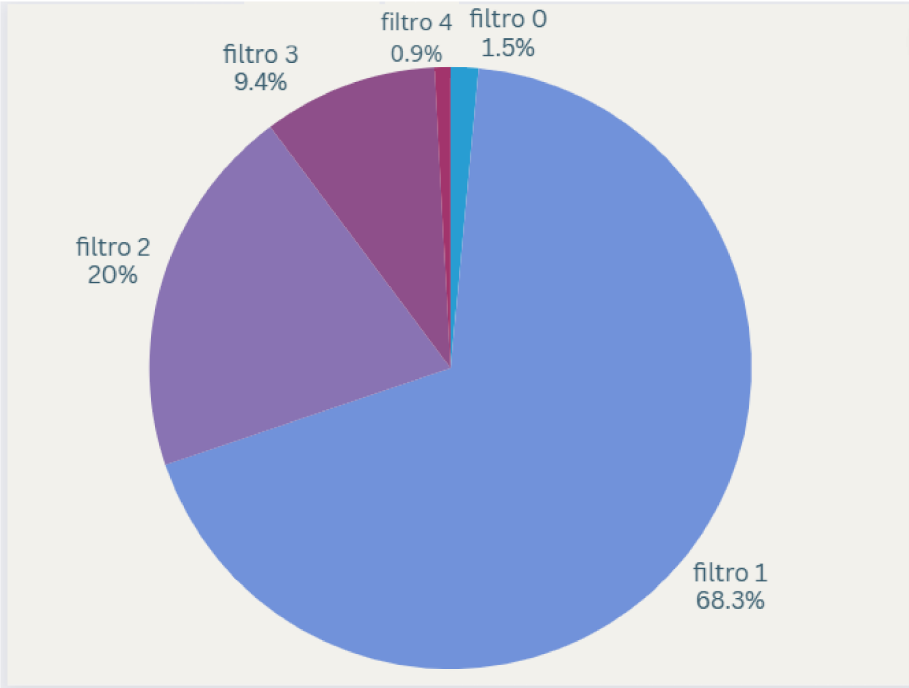
Etapa	**Tipo de Relevância**
Ignorado (0)	Duplicatas ou artigos não passíveis de avaliação
Leitura do Titulo (1)	Todos os textos passarão por essa etapa independente da relevância
Leitura do Resumo (2)	Os textos que possuem aspectos importantes sobre os termos utilizados
Leitura da Conclusão (3)	Os textos que possuem relação direta entre termos de maneira relevantes
Leitura do Material Completo (4)	Os textos que possuem total relação com a pergunta chave da pesquisa e englobem todos os termos necessários para respondê-la

Fonte: Autor

Aplicados os 470 artigos obtidos após aplicação dos critérios da seção 4.2.3 na etapa avaliativa especificada pela Tabela 8 obteve-se as porcentagens apresentadas no gráfico presente

na Figura 6.

Figura 6 – Porcentagem dos Artigos em Cada Nível de Filtro.



Fonte: Autor

O Apêndice A apresenta a tabela modelo usada para categorização de cada trabalho avaliado, nela estão contidos um numero de identificação para o artigo, título da obra, autores, o termo que foi utilizado para sua localização no Google Scholar, o objetivo do artigo e por fim, qual filtro ele pertence. [1] [2]

4.2.5 Síntese

Etapa de construção de conhecimento e entendimento do estado da arte acerca da pergunta que abre o processo de construção da RBS, nessa etapa deve-se conseguir uma resposta e uma justificativa válida para a pergunta chave utilizando os artigos avaliados na etapa anterior (GOUGH *et al.*, 2012, p. 180).

O presente trabalho apresenta no capítulo 5 o resultado constando como síntese um relatório detalhado contendo os textos aferidos e os métodos de verificação desse texto a fim de possibilitar a replicação responder a questão de abertura do trabalho.

---

[1] O link para o acesso dos trabalhos avaliados na secção 4.2.3: https://1drv.ms/f/c/034e0e8320be30d7/Eh8yVIRzVlVHv9FB4mVmmwkBP9zFjTkC8KTWC0Fy-LP2Fg?e=M687IG

[2] O link para o acesso à filtragem dos dados avaliados na secção 4.2.4: https://docs.google.com/spreadsheets/d/1D937289RQtjnoy5w7WxO4XTnAcDgQNzy4QPstQ2Hn7k/edit?usp=sharing

5 RESULTADOS E SÍNTESE

Munido com os artigos filtrados e realizando a análise deles é possível responder os itens restantes esperados nos objetivos desse trabalho.

5.1 Contrapontos entre IoT e LGPD

Como citado na seção de desenvolvimento desse trabalho, a LGPD apresenta em seu texto, mais especificamente dos parágrafos 46 ao 51, práticas e condutas que os desenvolvedores devem levar em consideração no momento da construção de dispositivos tecnológicos que utilizam dados pessoais e à essas práticas incluírem a preservação da segurança dos dados e a manutenção da privacidade dos usuários cujos dados foram coletados.

Um ensaio tratando os aspectos de segurança dos dispositivos IoT frente à LGPD, (OLIVEIRA *et al.*, 2019) apresentou 3 pontos que devem ser levados em consideração ao conceber um sistema constituído de dispositivos IoT, pontos esses que ao serem implementados produzem uma elevação de custos no desenvolvimento e, em alguns cenários, dificultam a implementação do sistema em questão, pontos apresentados na listagem abaixo.

- **Coleta:** Tratar da obtenção dos dados a partir do consentimento e da transparência para com os usuários, apresentando quais dados devem ser coletados e quais os princípios dos mesmos; Solicitar de algum modo o consentimento para a coleta desses dados; Aplicar interfaces gráfica que permitam o usuário compreender o funcionamento do dispositivo; Em caso de obtenção de imagens por meios de sensoreamento também se deve ter o consentimento para o uso comercial dessas imagens ou para a persistência das mesmas em bases de dados .
- **Transmissão:** Dado que a camada de transmissão possui um grande conjunto de intermediários é inevitável que essa camada seja a que mais sofre com ataques de terceiros, para cada um desses intermediários e cada dispositivo vinculado a ele vinculado, deve-se estabelecer parâmetro de segurança que garantam a integridade desses dados.
- **Armazenamento:** A integridade desse ponto é o aspecto mais importante a se levar em consideração e, junto a ele, temos outro pontos que cabem citar, tais como: O aspecto da exclusão, onde dados não podem ser mantidos por tempo indeterminado, sendo necessário estabelecer métodos e parâmetro para que eles possam ser apagados; O aspecto do registro, onde toda manipulação, leitura, gravação e edição desses dados devem ser registradas; O

aspecto de consulta, onde os dados devem ser facilmente acessíveis por parte dos usuários de modo eficiente; O aspecto de criptografia, o qual aumenta a segurança dos dados coletados, gerando, contudo, alteração no desempenho do sistema (OLIVEIRA *et al.*, 2019).

5.2 Contrapontos entre blockchain e LGPD

A utilização do termo 'contraponto' no objetivo desse trabalho teve por razão a possibilidade de analisar aspectos não só de oposição, como de complemento. Esse é o caso dos artefatos blockchain e LGPD, dado que boa parte dos artigos avaliados apresentam uma visão positiva acerca da tecnologia quando se refere a legislação.

O contraste mais substancial apresentado entre LGPD e blockchain é referente a falta de destaque na legislação acerca de entidade descentralizadas, que é, por princípio, a filosofia que norteia o funcionamento do protocolo blockchain (MEWES, 2021).

Ao se tratar das convergências que permeiam ambos os termos, tem-se que a tecnologia blockchain, atualmente, ainda é tida como uma das mais seguro método de processamento de dados, haja vista que evita a intrusão de dados desconhecidos e torna imutável seu registros. Esta última, por vezes, considerada como algo que contradiz a lei, quando na verdade, segundo a própria LGPD, não se caracteriza como algo que prejudique o usuário (MEWES, 2021).

Dada essa observação, diversos são os artigos que apresentam técnicas com o protocolo blockchain para sistemas de coleta de dados seguros que suportam a legislação vigente não somente no Brasil como também na Europa onde vigora a GDPR, lei que originou a LGPD (BAIãO, 2023).

5.3 Contrapontos entre a composição IoT, Blockchain e LGPD

Ao longo da pesquisa por materiais para a realização dessa RBS foi possível perceber o baixo número de pesquisas envolvendo a composição desses três conceitos. O fato dessas tecnologias serem significativamente recentes e o fato de ainda estarem sendo realizados estudos que relacionem IoT e blockchain são, possivelmente, os principais causadores dessa escassez.

Ao fim da filtragem dos artigo observados nesta RBS, quatro trabalhos foram selecionados como inteiramente relacionado com os três objetos avaliados -IoT, Blockchain e LGPD- e apresentam como ponto convergente a utilização de técnicas baseadas em blockchain para

resolver os problemas causados por tecnologias IoT que são contrários às resoluções propostas na redação da LGPD.

Segundo o artigo de Sarah Gomes Sakamoto (SAKAMOTO, 2020), o blockchain, por ser uma rede peer-to-peer distribuída e por promover uma segurança de dados transparente e descentralizada possibilita a implementação de sistemas IoT em conformidade à LGPD. Além disso, ela lista estudos que apresentam essas soluções com as mais diferentes técnicas para utilização de tecnologias blockchain atuando como processador de informações e que facilmente poderiam ser adaptados a um cenário de tecnologias IoT.

O estudo conduzido pelo grupo encabeçado por Maria Amália Arruda Câmara (CAMARA *et al.*, 2021) apresenta que a tecnologia blockchain vem sendo alvo de discussões a respeito de sua utilização em aplicações na área da saúde, mais especificamente em dispositivos IoT presentes em ambientes clínicos. Além disso, o grupo de pesquisa destaca que a tecnologia blockchain quando aplicada a dispositivos IoT pode oferecer aos usuários a consciência total dos dados coletados, gerenciar os consentimentos e estabelecer os parâmetros de compartilhamento sem a atuação de um autoridade central. Porém existe a possibilidade de haver problemas na implementação quando levado em consideração a Lei do esquecimento.

Outros dois estudos realizados por um grupo de estudo liderado por Konstantinos Rantos(RANTOS *et al.*, 2019) e o grupo de estudo liderado por George Drosatos (DROSATOS *et al.*, 2019) apresentam um *framework* que busca aplicar nos ecossistemas IoT os requerimentos exigidos pela GDPR e, dado que a GDPR é a originadora da LGPD, pode facilmente transpor essa solução para o cenário nacional. Além disso, esse sistema tem como base justamente a tecnologia blockchain na forma de *smart contracts* cujo propósito é gerir a parte do consentimento no uso de dados pessoais dos usuários.

5.4 Comparação entre as soluções propostas nos artigos selecionados

A partir dos 4 artigos observados, obteve-se 3 soluções semelhantes, porém com características diferentes, o estudo de Sakamoto apresenta uma lista de aplicações que podem tornar o protocolo Blockchain fundamental para a conformidade de sistemas IoT às normas da LGPD. O artigo publicado pelo grupo comandado pela Câmara apresenta uma solução para o problema de dados coletados por IoT no sistema de saúde e, por fim, os grupos chefiados por Rantos e Drosantos apresentam um *framework* que viabiliza a implementação 'orientada a privacidade e segurança' de um ecossistema IoT que gerencia o consentimento do uso de dados

dos usuários.

A Tabela 9 apresenta uma comparação entre as soluções propostas no conjunto de artigos observados.[1]

Tabela 9 – Lista de Artigos que Propõem Blockchain com Agente de Resolução de Problemas de Segurança Envolvendo IoT

Artigo	**Problema**	**Solução**
(NOVO, 2018) *	Gerenciamento de acesso aos dados.	Utilizar uma blockchain pública e um contrato inteligente para gerenciar o acesso aos dados.
(RIFI *et al.*, 2017) *	Gerenciamento de acesso aos dados.	Utilizar uma blockchain pública e múltiplos contratos inteligentes para gerenciar o acesso aos dados.
(ALPHAND *et al.*, 2018) *	Gerenciamento de acesso aos dados.	Utilizar uma blockchain pública não permissionada gerenciada pelo próprio usuário.
(DORRI *et al.*, 2017) *	Otimização da segurança em IoT.	Implementar um algoritmo de consentimento mais eficiente e aplicar um método de confiança distribuído que reduz o tempo de validação a cada validação realizada.
(PINNO *et al.*, 2017) *	Gerenciamento de acesso aos dados.	Implementar quatro blockchains, três para gerenciar o controle de acesso e uma para armazenar os registros de acesso.
(HAMMI *et al.*, 2018) *	Gerenciamento de acesso aos dados.	Implementar uma blockchain publica sobre o *Etherium* criando regiões virtuais de acesso seguro aos usuários.
(CAMARA *et al.*, 2021)	Gerenciamento dos dados da saúde pública obtidos via IoT.	Propor a solução através de um gerenciamento convencional utilizando banco de dados para a quantidade massiva de dados ou utilizar blockchain para realizar essa persistência levando em consideração as normas presentes na LGPD.
(RANTOS *et al.*, 2019) e (DROSATOS *et al.*, 2019)	Gerenciamento de consentimento do uso de dados no ecossistema IoT.	Uma plataforma que gerencia o consentimento obtidos do usuário e através de blockchain gerenciar os dados para os agentes que processam e utilizam esses dados levando em consideração a GDPR.

Fonte: Autor

[1] * artigo citados pelo artigo da (SAKAMOTO, 2020).

5.5 Conclusão e Considerações Finais

As tecnologias inseridas no paradigma de Internet das Coisas vem cada vez mais ganhando espaço no cotidiano das pessoas, indústrias e cidades e com ela surge o problema referente à privacidade de dados pessoais que possam ser capturadas pelos mais diversos tipos de sensores.

Tecnologias baseadas em blockchain vem sendo utilizadas amplamente para gestão de dados e, por apresentarem aspectos de segurança avançado e altamente eficiente, passam a ser uma solução para o problema apresentado pelos dispositivos IoT.

Levando em consideração a legislação que rege a manipulação de dados no Brasil, uma das soluções que podem ser aplicadas no desenvolvimento dessas aplicações envolvendo blockchain e IoT é o paradigma de construção denominado *'Privacy -by-Design'*.

'Privacy -by-Design' tem por premissa a preocupação com a privacidade dos usuário desde a concepção do projeto a ser implementado, ou seja, a partir do momento que se estabelece a intensão de projetar um dispositivos IoT, deve-se já ser considerado os meios de preservação da privacidade dos indivíduos que irão manipula-lo (KARASSAWA *et al.*, 2021). Essa pratica é prevista nos artigos 46 e 52 da LGPD e, para realizar essa implementação, pode-se estabelecer Blockchains como gestores dos dados, dos registros de manipulação desses dados e dos consentimentos ofertados a esses dispositivos levando em consideração as boas praticas apontadas pela LGPD e com isso manter a integridade do novo sistema projetado.

Ademais, ao se observar as comparações acerca das soluções propostas pelos autores dos artigos selecionados nota-se a significativa utilidade que as tecnologias baseadas em blockchain tem considerando a sua aplicação nos aspectos de segurança em dispositivos IoT.

A adoção de uma arquitetura, na qual, os dispositivos IoT tem por responsabilidade a coletar dados e do consentimento do uso dessas informações e no qual o sistema blockchain passa a tratar a movimentação desses dados utilizando *smart contracts* que é uma estratégia apresentadas nos artigos (RANTOS *et al.*, 2019) e (DROSATOS *et al.*, 2019) e se demonstra bastante eficiente para essa implementação em uma diversidades de cenários de dispositivos IoT orientados à LGPD.

Por fim, pode-se responder a pergunta problema em aberto levando em consideração que tecnologias baseadas em Blockchain quando aplicadas a dispositivos IoT tendem a formata-lo justamente aos moldes esperados pela LGPD e, por tanto, apresentam mais vantagens do que desvantagens na sua aplicação, sendo as contradições limitadas a aspectos que o protocolo

Blockchain possui e que ainda não foram discutidas em meio político.

REFERÊNCIAS

AGOSTINELLI, J. A importância da lei geral de proteção de dados pessoais no ambiente online. ETIC - Encontro de Iniciação Científica, ISSN 21-76-8494, 2018.

ALPHAND, O.; AMORETTI, M.; CLAEYS, T.; DALL'ASTA, S.; DUDA, A.; FERRARI, G.; ROUSSEAU, F.; TOURANCHEAU, B.; VELTRI, L.; ZANICHELLI, F. Iotchain: A blockchain security architecture for the internet of things. IEEE Internet of things journal, 2018.

BAIãO, R. B. S. M. **Afinal, blockchain é incompatível com a LGPD?** 2023. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/blockchain-lgpd-dados-pessoais-brasil>. Acesso em: 20 nov. 2023.

BOLAND, A.; CHERRY, M. G.; DICKSON, R. **Doing a Systematic Review**: A student's guide. [S.l.]: SAGE Publications, 2014.

BRASIL. ConstituiÇÃo da repÚblica federativa do brasil de 1988. Brasília, DF: Diário Oficial da União, 1988.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. código de defesa do consumidor. Brasília, DF: Diário Oficial da União, 1990.

BRASIL. Lei federal 9.296, de 1996. Brasília, DF: Diário Oficial da União, 1996.

BRASIL. Lei nº 12.737, de 30 de novembro de 2020. lei carolina dieckmann. lei de crimes cibernéticos. Brasília, DF: Diário Oficial da União, 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. lei do marco civil da internet. Brasília, DF: Diário Oficial da União, 2014.

BRASIL. Presidência da república. lei n.13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Diário Oficial da União, 2018.

BRITO, M. M. Crimes cibernéticos e a recepção da lei no 12.737/2012 no brasil. Universidade Católica do Salvador, 2020.

CAMARA, M. A. A.; LINS, G. H. A.; OLIVEIRA, F. H. C. de; CAMELO, E. M. A.; MEDEIROS, N. R. F. C. de. Internet das coisas e blockchain no sistema Único de saúde: a proteção dos dados sensíveis diante da lei geral de proteção de dados. Cadernos Ibero-Americanos de Direito Sanitário, 2021.

CHAKRABORTY, R.; GHOSH, A.; BALAS, V. E.; ELNGAR, A. A. **BLockChain**: Principles and applications in iot. [S.l.]: CRC Press, 2023.

DON; TAPSCOTT, A. **Blockchain Revolution**: How the technology behind bitcoin is changing money, business, and the world. [S.l.]: Penguin Random House LLC, 2016.

DORRI, A.; KANHERE, S. S.; JURDAK, R.; GAURAVARAM, P. Lsb: A lightweight scalable blockchain for iot security and privacy. Elsevier BV, 2017.

DROSATOS, G.; RANTOS, K.; KRITSAS, A.; ILIOUDIS, C.; FILIPPIDIS, A. P.; PAPANIKOLAOU, A. A blockchain-based platform for consent management of personal data processing in the iot ecosystem. Security and Communication Networks, 2019.

FOXBIT. **O que são bases de dados centralizadas, descentralizadas e distribuídas?** 2019. Disponível em: <https://foxbit.com.br/blog/diferenca-entre-as-bases-de-dados-blockchain/>. Acesso em: 25 out. 2023.

GOUGH, D.; OLIVER, S.; THOMAS, J. **An Introduction to Systematic Reviews**. [S.l.]: SAGE Publications, 2012.

GUSSON, C. **Governo anuncia nova versão do RG que agora usa blockchain e token de identificação para todos os brasileiros.** 2023. Disponível em: <https://br.cointelegraph.com/news/government-announces-new-version-of-rg-that-now-uses-blockchain-and-already-has-1-million-documents Acesso em: 30 ago. 2023.

HACKIUS, N.; PETERSEN, M. **Blockcahin in Logistics and Supply Chain: Trick or Treat?** 2017. Disponível em: <https://tore.tuhh.de/bitstream/11420/1447/1/petersen_hackius_blockchain_in_scm_and_logistics_hicl_2017.pdf>. Acesso em: 15 jun. 2023.

HAMMI, M. T.; HAMMI, B.; BELLOT, P.; SERHROUCHNI, A. Bubbles of trust: A decentralized blockchain-based authentication system for iot. Computers Security, 2018.

HANES, D.; SALGUEIRO, G.; GROSSETETE, P.; BARTON, R.; HENRY, J. **IoT Fundamentals**: Networking technologies, protocols, and use cases for the internet of things. [S.l.]: Cisco Press, 2017.

HIEBERT, L. **Public Safety Blog Series-Connecting the Unconnected in Public Safety Response**. 2013. Disponível em: <https://blogs.cisco.com/government/connecting-the-unconnected-in-public-safety-response>. Acesso em: 20 jun. 2023.

ISAAK, J.; HANNA, M. J. User data privacy: Facebook, cambridge analytica, and privacy protection. IEEE, Computer 51(8), pp. 56-139, 2018.

KARASSAWA, G.; ALENCAR, A. C. de; ALMEIDA, A. R. B. G. de; LIMA, C. C. C.; BUENO, G.; VIEIRA, G. N. G. G. G.; LANDIM, H. D. P.; PEDROSA, H. R. V.; MORAES, H. F.; COSTA, M.; PREVITALI, M. B.; GUEDES, M. E. A.; BRUNO, M. G. da S.; BLUM, R. O.; VAINZOF, R.; FURTADO, T. N. Dpo (encarregado) gestão dos programas de privacidade e proteção de dados. Opice Blum, 2021.

KOON, J. **How IoT Will Change Our Lives**. 2019. Disponível em: <https://www.engineering.com/story/how-iot-will-change-our-lives>. Acesso em: 20 jun. 2023.

KRANENBURG, R. V.; BASSI, A. Iot challenges. Communications in Mobile Computing: a SpringerOpen Journal, 2012.

KSHETRI, N. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management 39,80-89, 2018.

LEA, P. **Internet of Things for Architects**: Architecting iot solutions by implementing sensors, communication infrastructure, edge computing, analytics and security. [S.l.]: Packt Publishing, 2018.

MEWES, L. H. Blockchain e exclusÃo de dados: A compatibilidade entre a tecnologia e a lei geral de proteÇÃo de dados pessoais (lgpd). Repositório Universitário de Ânima, 2021.

MODEL, T. I. W. F. R. **IoT World Forum Reference Model**. 2017.

NOVO, O. Blockchain meets iot: An architecture for scalable access management in iot. IEEE Internet of things journal, 2018.

OLIVEIRA, N. S. de; GOMES, M. A.; LOPES, R.; NOBRE, J. C. Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd). Revista Eletrônica de Iniciação Científica em Computação da UFRGS, 2019.

PINNO, O. J. A.; GREGIO, A. R. A.; BONA, L. C. E. D. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. IEEE Global Communications Conference, 2017.

POPOVSKI, L.; SOUSSOU, G. A brief history of blockchain. ALM Publication, 2018.

PURESWARAN, V.; BRODY, P. **Device Democracy:** saving the future of th internet of things. IBM Corporation, 2015.

RANTOS, K.; DROSATOS, G.; DEMERTZIS, K.; ILIOUDIS, C.; PAPANIKOLAOU, A. Blockchain-based consents management for personal data processing in the iot ecosystem. Security and Communication Networks, 2019.

RAPôSO, C. F. L.; JUNIOR, H. M. de Lima an Waldecy Ferreira de O.; SILVA, P. A. F.; BARROS, E. de S. Lgpd-lei geral de proteÇÃo de dados pessoais em tecnologia da informaÇÃo: Revisão sistemática. RACE - Revista de Administração do Cesmac, 2019.

RAWAT; SINGH, A.; PAPAILIOPOULOS; S., D.; DIMAKIS; G., A.; VISHWANATH, S. Locality and availability in distributed storage. IEEE Transactions on Information Theory, 2016.

REYNA, A.; MARTíN, C.; CHEN, J.; SOLER, E.; DíAZ, M. On blockchain and its integration with iot. challenges and opportunities. Future Generation Computer Systems, 2018.

RIFI, N.; RACHKIDI, E.; AGOULMINE, N.; TAHER, N. C. Towards using blockchain technology for iot data access protection. IEEE Internet of things journal, 2017.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. **The Internet of Things: An Overview**: Understanding the issues and challenges of a more connected world. [S.l.]: Internet Society, 2015.

SACHDEVA, S.; ALI, A. A hybrid approach using digital forensics for attack detection in a clund network environmet. International Journal of Future Generation Communication and Networking, 2021.

SAKAMOTO, S. G. SeguranÇa, privacidade e blockchain no contexto de internet das coisas. Repositório Institucional da Universidade Tecnológica Federal do Paraná, 2020.

SCHWAB, K. **The Fourth Industrial Revolution**. [S.l.]: World Economic Forum, 2016.

SEEBACHER, S.; SCHüRITZ, R. Blockchain technology as an enabler of service systems: A structured literature review. Exploring Services Science, 2017.

TEFFé, C. S. de; MORAES, M. C. B. de. Redes sociais virtuais: privacidade e responsabilidade civil. análise a partir do marco civil da internet. Pensar - Revista de Ciências Jurídicas, 2017.

UJJWAL, A. **How Does the Blockchain Work?** 2023. Disponível em: <https://www.geeksforgeeks.org/how-does-the-blockchain-work/>. Acesso em: 26 out. 2023.

VYAS, N.; BEIJE, A.; KRISHNAMACHARI, B. **BlockChain and the Supply Chain**: Concepts, strategies and pratical applications. [S.l.]: KoganPage, 2019.

WANG, J.; HAN, C.; YU, X.; REN, Y.; SHERRATT, R. S. Distributed secure storage scheme based on sharding blockchain. Tech Science Press: Computers, Materials Continua, 2021.

XU, M.; XEN, X.; KOU, G. A systematic review of blockchain. Financial Innovation Journal, 2019.

ZHAO, J. L.; FAN, S.; YAN, J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2016.

APÊNDICE A – CLASSIFICAÇÃO DOS ARTIGOS SELECIONADOS

Tabela 10 – Filtragem dos Artigos

Nº	**Título**	**Autores**	**Termo de Localização**	**Objetivo**	**Filtro**

Fonte: Autor