UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Privacidade de dados em Blockchain: Um estudo sobre a conformidade regulatória com as regulamentações de proteção de dados do Brasil e da Europa

Dissertação de Mestrado

Tácito Augusto Farias Júnior

São Cristóvão – Sergipe

2024

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Tácito Augusto Farias Júnior

Privacidade de dados em Blockchain: Um estudo sobre a conformidade regulatória com as regulamentações de proteção de dados do Brasil e da Europa

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Sergipe como requisito final para a obtenção do título de mestre em Ciência da Computação.

Orientador(a): Rafael Oliveira Vasconcelos
Coorientador(a): Admilson de Ribamar Lima Ribeiro

São Cristóvão – Sergipe

2024

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

F224p

Farias Júnior, Tácito Augusto.
Privacidade de dados em Blockchain: um estudo sobre a conformidade regulatória com as regulamentações de proteção de dados do Brasil e da Europa / Tácito Augusto Farias Júnior ; orientador Rafael Oliveira Vasconcelos. – São Cristóvão, SE, 2024.
76 f. : il.

Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Sergipe, 2024.

1. Proteção de dados. 2. Blockchains (Base de dados). 3. Privacidade. 4. Compartilhamento de arquivos de computador. 5. Algorítmos. 6. Criptografia de dados (Computação). I. Lei Geral de Proteção de Dados. II. General Data Protection Regulation. III. Vasconcelos, Rafael Oliveira, orient. IV. Título.

CDU 004.6

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
COORDENAÇÃO DE PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Ata da Sessão Solene de Defesa da Dissertação do Curso de Mestrado em Ciência da Computação-UFS.
Candidato: Tácito Augusto Farias Júnior

Em 20 dias do mês de fevereiro do ano de dois mil e vinte quatro, com início às 09hs, realizou-se na Sala de Seminários do PROCC da Universidade Federal de Sergipe, na Cidade Universitária Prof. José Aloísio de Campos, a Sessão Pública de Defesa de Dissertação de Mestrado do candidato **Tácito Augusto Farias Júnior**, que desenvolveu o trabalho intitulado: ***"Privacidade de Dados em Blockchain: Um Estudo Detalhado Sobre a Conformidade Regulatória Com as Regulamentações de Proteção de Dados do Brasil e da Europa"*,** sob a orientação do Prof. Dr. **Rafael Oliveira Vasconcelos e coorientação do prof. Dr. Admilson de Ribamar Lima Ribeiro**. A Sessão foi presidida pelo Prof. Dr. **Rafael Oliveira Vasconcelos** (PROCC/UFS), que após a apresentação da dissertação passou a palavra aos outros membros da Banca Examinadora, o Dr. **Bruno José Olivieri de Souza (**TST**)** , posteriormente o Prof. Dr. **Edward David Moreno Ordonez** (Procc/UFS) e, em seguida, Dr. **Admilson de Ribamar Lima Ribeiro** (PROCC/UFS) . Após as discussões, a Banca Examinadora reuniu-se e considerou o mestrando (a) aprovado "*(aprovado/reprovado)*". Atendidas as exigências da Instrução Normativa 05/2019/PROCC, do Regimento Interno do PROCC (Resolução 67/2014/CONEPE), e da Resolução nº 04/2021/CONEPE que regulamentam a Apresentação e Defesa de Dissertação, e nada mais havendo a tratar, a Banca Examinadora elaborou esta Ata que será assinada pelos seus membros e pelo mestrando.

Cidade Universitária "*Prof. José Aloísio de Campos",* 20 de fevereiro de 2024.

gov.br Documento assinado digitalmente
RAFAEL OLIVEIRA VASCONCELOS
Data: 19/02/2024 17:06:46-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Rafael Oliveira Vasconcelos
(PROCC/UFS)
Presidente

Admilson de Ribamar Lima Ribeiro
Assinado de forma digital por Admilson de Ribamar Lima Ribeiro
DN: cn=Admilson de Ribamar Lima Ribeiro, o, ou, email=secretaria.pos@dcomp.ufs.br, c=BR
Dados: 2024.02.20 13:28:50 -03'00'

Prof. Dr.Admilson de Ribamar Lima Ribeiro
(PROCC/UFS)
Examinador Interno
Coorientador

gov.br Documento assinado digitalmente
EDWARD DAVID MORENO ORDONEZ
Data: 20/02/2024 13:16:11-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Edward David Moreno Ordonez
(PROCC/UFS)
Examinador Interno

gov.br Documento assinado digitalmente
BRUNO JOSE OLIMERI DE SOUZA
Data: 20/02/2024 12:49:48-0300
Verifique em https://validar.iti.gov.br

Dr. Bruno José Olivieri de Souza
(TST)
Examinador Externo

gov.br Documento assinado digitalmente
TACITO AUGUSTO FARIAS JUNIOR
Data: 20/02/2024 13:35:09-0300
Verifique em https://validar.iti.gov.br

Tácito Augusto Farias Júnior
Candidato

Agradecimentos

Inicialmente, agradeço a Deus, pela minha saúde e força para superar todos os desafios que surgiram no decorrer dessa longa jornada.

Aos meus pais, Adenízia e Tácito, e a minha falecida vó, Lindinalva Farias, pela educação, amor, fé, ética, lealdade, humildade e respeito. Pois, são valores que estão presentes no meu perfil pessoal e profissional. Também agradeço às minhas irmãs, Ralitsa e Rebecca, pelo incentivo nessa caminhada.

Um enorme e especial reconhecimento ao meu orientador, Professor Dr. Rafael, e ao meu coorientador Professor Dr. Admilson, por terem compartilhado conteúdos, experiências, conhecimentos e orientações, que foram fundamentais para a conclusão desta dissertação.

Agradeço aos meus colegas de curso, Caio, Samuel, Shexmo e Roberta, pela parceria e apoio em todos os momentos que tivemos juntos. Ao meu grande amigo Sálvio, pelo incentivo nos momentos difíceis e por toda colaboração no decorrer do curso. Um agradecimento especial também para os meus amigos Zanôni, Sampaio, Wilson, Matheus, Noel, Claudenice, Júlia, Karolyne e Allysson pela compreensão e apoio nos momentos conturbados e desafiadores.

Também agradeço a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo financiamento de boa parte do meu curso, pois me possibilitou obter esta grande conquista.

Enfim, sou muito grato a todos os meus amigos, colegas e também aos funcionários do DCOMP/UFS, principalmente a Elaine, que tornou-se uma amiga e conselheira, como também a Wesley, por tudo que vivenciamos juntos.

O homem não teria alcançado o possível se,
repetidas vezes, não tivesse tentado o impossível.
(Max Weber)

Resumo

A privacidade de dados refere-se ao direito fundamental dos indivíduos de controlar suas informações pessoais e a forma como essas informações são coletadas, armazenadas e utilizadas. Isso abrange a proteção dos dados contra vazamentos e acessos não autorizados. Neste contexto, regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a General Data Protection Regulation (GDPR) na Europa foram desenvolvidas para gerenciar a privacidade e o tratamento de dados pessoais. A *Blockchain*, uma tecnologia emergente que utiliza uma cadeia de blocos para registrar transações de maneira imutável, descentralizada e transparente, apresenta desafios de conformidade com essas regulamentações de proteção de dados. Esta dissertação apresenta como objetivo principal uma análise da conformidade regulatória da privacidade de dados existente na *Blockchain* com a LGPD e GDPR. A metodologia deste trabalho consiste num Mapeamento Sistemático da Literatura (MLS) que investiga a conformidade regulatória da *Blockchain* com a LGPD ou GDPR em relação à privacidade de dados. Posteriormente, é realizado um estudo comparativo entre 2 (duas) das principais técnicas de criptografia e privacidade utilizadas em *Blockchain*, *Zero-Knowledge Proof* (ZKP) e *Ring Signatures*, visando conformidade regulatória com a LGPD e GDPR. Por fim, esta dissertação contribui para o entendimento das questões de privacidade de dados em *Blockchain* e fornece insights para empresas, organizações e reguladores sobre a utilização da tecnologia *Blockchain* em conformidade regulatória com as regulamentações de proteção de dados do Brasil e da Europa.

Palavras-chave: Privacidade de Dados. *Blockchain*. Conformidade Regulatória. Lei Geral de Proteção de Dados. General Data Protection Regulation.

Abstract

Data privacy refers to the fundamental right of individuals to control their personal information and the way that information is collected, stored and used. This covers protecting data against leaks and unauthorized access. In this context, regulations such as the General Data Protection Law (LGPD) in Brazil and the General Data Protection Regulation (GDPR) in Europe were developed to manage privacy and the processing of personal data. *Blockchain*, an emerging technology that uses a *Blockchain* to record transactions in an immutable, decentralized and transparent manner, presents compliance challenges with these data protection regulations. This dissertation presents as its main objective an analysis of the data privacy regulatory compliance existing in *Blockchain* with the LGPD and GDPR. The methodology of this work consists of a Systematic Literature Mapping (MLS) that investigates *Blockchain*'s regulatory compliance with the LGPD or GDPR in relation to data privacy. Subsequently, a comparative study is carried out between 2 (two) of the main encryption and privacy techniques used in *Blockchain*, *Zero-Knowledge Proof* (ZKP) and *Ring Signatures*, aiming for regulatory compliance with the LGPD and GDPR. Ultimately, this dissertation contributes to the understanding of data privacy issues in *Blockchain* and provides insights for companies, organizations and regulators on the use of *Blockchain* technology in regulatory compliance with data protection regulations from Brazil and Europe.

Keywords: Data Privacy. *Blockchain*. Regulatory Compliance. General Data Protection Law. General Data Protection Regulation.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ARX	Autoregressive-Exogenous
CNIL	Comissão Nacional de Informática e Liberdades
DCOMP	Departamento de Computação
DeFi	Decentralized Finance
DPoS	Delegated Proof of Stake
DApps	Decentralized Applications
GAF	Framework Analítico de Governança
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IA	Inteligência Artificial
IoT	Internet das Coisas
IPFS	InterPlanetary File System
KYC	Know Your Customer
LGPD	Lei Geral de Proteção de Dados
MSL	Mapeamento Sistemático da Literatura
MPC	Multiparty Computation
NFTs	Non-Fungible Tokens
P2P	Peer-to-Peer
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
PPTD	Privacy-Preserving Truth Discovery
pBFT	Practical Byzantine Fault Tolerance
SGSI	Sistemas de Gestão de Segurança da Informação

SHA	Secure Hash Algorithm
TI	Tecnologia da Informação
UFS	Universidade Federal de Sergipe
ZKP	Zero-Knowledge Proof
zkSNARGs	Zero-Knowledge Succinct Non-Interactive Arguments
zkSNARKs	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
zkSTARKs	Scalable Transparent Argument of Knowledge
zkVPD	Verifiable Polynomial Delegation

Sumário

1 Introdução

O conceito de privacidade de dados é visto como dinâmico e multifacetado, não se limitando apenas a proteção contra o acesso de usuários não autorizados. Também possui um papel fundamental no controle dos dados, de modo que busca o entendimento de como esses tem sido coletados, utilizados e compartilhados (SOLOVE, 2010). Dessa forma, é possível reconhecer o nível de complexidade observado em torno das expectativas da privacidade de dados em diversos contextos.

Trata-se de um direito e prática de gerenciamento da coleta, armazenamento e uso de informações consideradas sensíveis, seja de indivíduos ou organizações. De modo que ambos possuem a autonomia para controlar como os dados coletados e armazenados foram posteriormente utilizados (SOLOVE; SCHWARTZ, 2020). De maneira geral, pode-se afirmar que a privacidade de dados abrange a proteção contra o uso indevido de informações pessoais e organizacionais.

A *Blockchain* é considerada uma tecnologia disruptiva que obteve notoriedade principalmente por conta da sua aplicação nas criptomoedas, como é o caso do Bitcoin. No entanto, as implicações existentes nessa tecnologia vão muito além das moedas digitais. Pois, a *Blockchain* é um registro público descentralizado e distribuído, que pode garantir a segurança, transparência e integridade dos dados sem que haja a necessidade de uma autoridade central ou até mesmo de intermediários (TAPSCOTT; TAPSCOTT, 2016).

A adoção da *Blockchain* vem sendo impulsionada por causa das suas características únicas. Essa tecnologia oferece uma maneira de registrar e compartilhar as informações de forma segura e imutável, de modo que atrai diversas áreas como finanças, saúde, logística e entre outras. A *Blockchain* permite que sejam criados sistemas mais transparentes e confiáveis, onde as transações e os dados podem ser acessados e verificados pelos participantes da rede (MOUGAYAR, 2018).

A criptografia é uma parte essencial da *Blockchain*, que oferece uma maior confiança e

segurança aos sistemas descentralizados. Em *Blockchains*, como a do Bitcoin, é visto o uso da criptografia de chave pública, que permite aos usuários manter o controle sobre as transações e identidades digitais de forma segura (NARAYANAN et al., 2016).

A segurança na *Blockchain* é assegurada através do uso da criptografia, incluindo funções de *hash* para realizar a verificação da integridade dos dados. Além disso, técnicas criptográficas avançadas como *Zero-Knowledge Proof* (ZKP) e Ring Signatures são implementadas para aprimorar a privacidade e o anonimato das transações. Estas técnicas permitem que as transações possam ocorrer de maneira anônima, de modo que preserva a confidencialidade dos usuários (LANTZ; CAWREY, 2020). Quando as transações numa *Blockchain* não necessitam ser anônimas, outras técnicas e configurações (identidades verificáveis, permissões e controles de acesso, bem como transparência seletiva, entre outras) podem ser adotadas para garantir a transparência e rastreabilidade, além da segurança, integridade dos dados e autenticidade das transações.

Atualmente, no Brasil, a relação entre a privacidade e Lei Geral de Proteção de Dados (LGPD), fundamentada nos princípios e diretrizes da General Data Protection Regulation (GDPR), tem sido um tema bastante discutido, pois é através da LGPD que este tema passa a ser compreendido não apenas como um direito, mas considerado uma questão de conformidade corporativa. Essa mudança no paradigma implica a adoção, pelas organizações, de mais medidas efetivas para realizar a proteção de dados, principalmente os pessoais sensíveis, sob o risco de penalizações significativas (LIMA; COSTA; SILVA, 2019).

Nos últimos anos, muita atenção é dada ao conceito de *Blockchain*, principalmente após a popularização da moeda virtual Bitcoin, lançada em 2008 por um desconhecido sob o pseudônimo de Satoshi Nakamoto (NAKAMOTO, 2008). Com a concretização do Bitcoin e os conceitos inovadores que essa ação trouxe ao mercado financeiro, organizações como instituições bancárias, financeiras e órgãos públicos reguladores começaram a discutir explicitamente sobre a importância e adoção dessa nova tecnologia baseada em cadeia de blocos. Por exemplo, o Banco J.P. Morgan Chase criou a "JPM Coin", uma moeda digital baseada em *Blockchain* e que facilita as transações instantâneas entre os clientes institucionais. Além do Santander que foi um dos bancos pioneiros na adoção da *Blockchain* para aprimorar as transferências internacionais de dinheiro através do serviço Santander One Pay FX.

Um dos problemas mais relevantes na tecnologia *Blockchain* está relacionado com a pseudonimidade, que não é considerada equivalente ao anonimato completo. Apesar das identidades dos usuários não serem diretamente visíveis, as transações são públicas na rede e, com a realização de análises avançadas, essas transações podem ser rastreadas até os usuários que as realizaram (MEIKLEJOHN et al., 2013).

1.1 Justificativa

A conformidade regulatória da privacidade de dados presente na *Blockchain* junto às determinações da LGPD e GDPR é vista como um desafio devido à crescente utilização da tecnologia *Blockchain* em diversas áreas e ao aumento na quantidade dos dados pessoais armazenados (ALVES et al., 2020). Como se trata de um sistema descentralizado e baseado em consenso, é possível oferecer níveis mais elevados de segurança e transparência, mas isso também pode representar desafios adicionais quando relacionado com a LGPD e GDPR.

Além disso, a LGPD é uma lei nova no Brasil e há uma necessidade de estudos e análises para aplicar os princípios e exigências às novas tecnologias. Portanto, é importante entender como as tecnologias baseadas em *Blockchain* podem ser utilizadas de forma legal e ética, para que dessa forma seja possível garantir a privacidade e proteção dos dados de maneira adequada (BAIAO, 2020).

Uma trabalho dessa natureza pode ser considerado de grande relevância para indivíduos, empresas e reguladores que desejam utilizar a tecnologia *Blockchain* para proteger, armazenar e gerenciar os dados, bem como para especialistas em privacidade. De modo que se torna viável fornecer uma percepção do cenário atual e recomendar medidas para garantir a conformidade regulatória com a LGPD e GDPR.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é analisar a conformidade regulatória da privacidade de dados presente na *Blockchain* com a LGPD e GDPR, buscando identificar os desafios existentes na implementação da tecnologia em relação às exigências preestabelecidas pelas regulamentações brasileira e europeia.

1.2.2 Objetivos Específicos

Para alcançar o objetivo geral, outros objetivos específicos precisam ser concluídos, como:

- Discutir as principais características, o funcionamento e os tipos de *Blockchains* existentes na atualidade;
- Identificar os principais desafios enfrentados pela privacidade de dados na *Blockchain* em relação a LGPD ou GDPR;
- Investigar os exemplos das soluções de privacidade de dados que utilizam *Blockchain* visando conformidade regulatória com a LGPD ou GDPR;

1.3 Organização do Trabalho

A presente dissertação está organizada em 5 (cinco) capítulos. O capítulo 1 apresenta tema, motivação, justificativa e os objetivos (geral e específicos). No capítulo 2 é apresentada a fundamentação teórica, em que são abordados conceitos, funcionamentos, composições e limitações da tecnologia *Blockchain*, além de temas complementares como Algoritmos de Consenso, Criptografia, Privacidade de Dados, LGPD, GDPR e NBR ISO/IEC 27001. O capítulo 3 apresenta um mapeamento sistemático das informações coletadas pertinentes ao tema desta dissertação, com uma discussão aprofundada dos trabalhos relacionados. No capítulo 4 foi realizado um estudo comparativo entre *Zero-Knowledge Proof* (ZKP) e *Ring Signatures* em *Blockchain*, visando conformidade regulatória com a LGPD e GDPR. Por fim, o capítulo 5 apresenta as considerações finais e os trabalhos futuros.

2

Fundamentação Teórica

Este capítulo apresenta as definições fundamentais para a dissertação, incluindo *Blockchain*, Algoritmos de Consenso, Criptografia, Privacidade de Dados Lei Geral de Proteção de Dados (LGPD), General Data Protection Regulation (GDPR) e NBR ISO/IEC 27001.

2.1 *Blockchain*

A *Blockchain* é um sistema de registro de transações mantido por uma rede descentralizada de computadores. Ao invés de apenas uma única central de controle, ela utiliza uma estrutura distribuída, tornando-se altamente segura, resistente e tolerante a falhas (NAKAMOTO, 2008).

A tecnologia *Blockchain* possui um livro-razão distribuído que é descrito como um registro digital imutável das transações, sendo considerado uma peça fundamental na *Blockchain*. Este livro-razão permite que haja a criação de um registro permanente e à prova de alterações em todas as transações que foram realizadas numa rede da *Blockchain* (NARAYANAN et al., 2016).

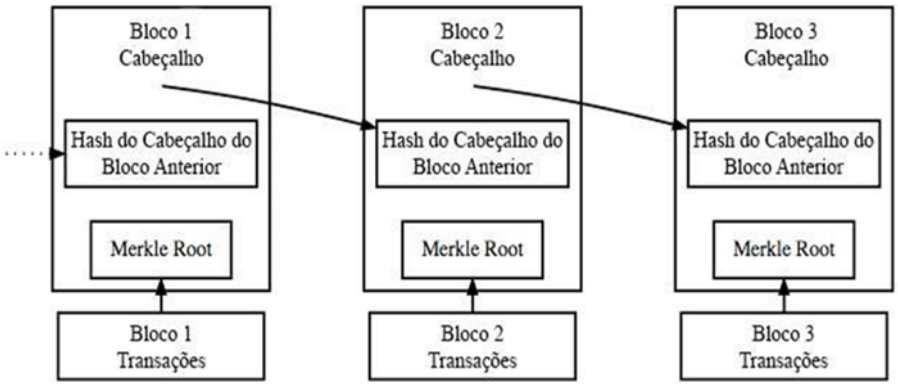
O funcionamento dessa tecnologia é baseado em um mecanismo de consenso. Onde cada bloco contém uma série de transações criptograficamente ligadas ao bloco anterior, formando uma "corrente" de blocos. Uma vez que um bloco é adicionado à cadeia, torna-se quase difícil alterá-lo, graças à função *hash* criptográfica e aos algoritmos de consenso (MAURER; NELMS; SWARTZ, 2013).

Esse sistema obteve o conceito inicial definido no ano de 2008, em "Bitcoin: A Peer-to-Peer Electronic Cash System", artigo escrito por Satoshi Nakamoto, um codinome cuja real identidade nunca foi descoberta. A *Blockchain* foi descrita como sendo a tecnologia do livro-razão do Bitcoin, uma criptomoeda desenvolvida para ser quase inviolável e independente de uma entidade central, permitindo transações entre duas pessoas sem que terceiros possam intervir (NAKAMOTO, 2008).

A arquitetura de uma *Blockchain* é composta por três elementos principais: o bloco, o nó e o protocolo de consenso. Os blocos armazenam os registros de transações, enquanto os nós são os participantes que mantêm a rede. O protocolo de consenso é o mecanismo pelo qual os nós concordam sobre qual bloco deve ser adicionado à cadeia a seguir (MIERS et al., 2013).

A Figura 1 apresenta a arquitetura de uma *Blockchain*, onde cada bloco possui um cabeçalho, o *hash* do cabeçalho do bloco anterior, a raiz de *Merkle Root* e as transações. Segundo Nakamoto (2008), essa arquitetura cria um encadeamento onde a integridade e a sequência dos blocos são mantidas e verificáveis.

Figura 1 – Arquitetura da *Blockchain*



Fonte: Elaborado pelo Autor

Essa arquitetura de dados encadeados de blocos é uma das principais responsáveis por garantir a distribuição e imutabilidade das informações devido ao encadeamento delas através do valor *hash*. As transações salvam do bloco anterior, qualquer alteração que pretenda se fazer em um outro, resultando necessariamente na alteração de todos os imediatamente posteriores a ele, portanto, para manter o encadeamento consistente, seria necessário recalcular todos os valores dos blocos seguintes, tarefa que é extremamente custosa computacionalmente e torna-se cada vez mais difícil com a adição de novos blocos (STALLINGS; BRESSAN; BARBOSA, 2008).

Devido ao triunfo do Bitcoin, entidades como startups, grandes corporações, instituições financeiras e governos, demonstraram interesse na tecnologia, desde então, variantes da *Blockchain* foram desenvolvidas e publicadas com o intuito de melhorar ou de agregar novas funcionalidades a ela, permitindo o uso desta não apenas para transações financeiras, mas também para outras aplicações como votação eletrônica, registros médicos, identidade digital e entre outras (ALI et al., 2016).

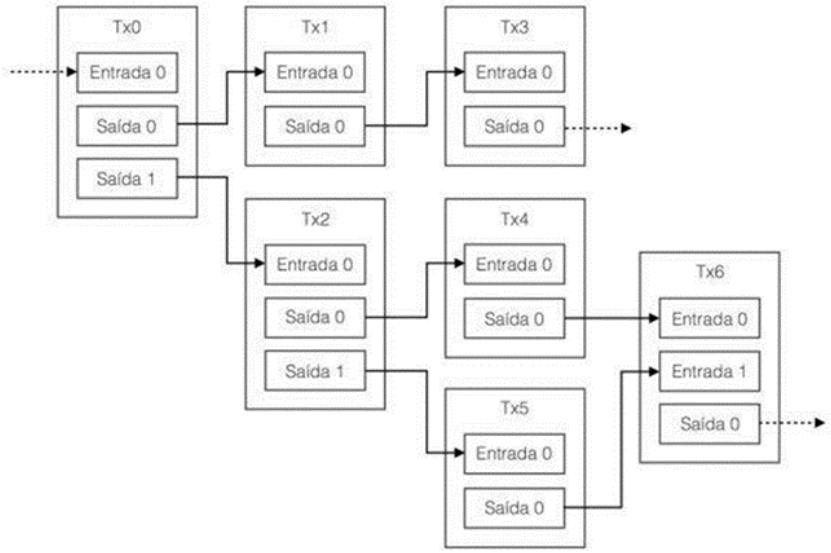
2.1.1 Blocos e Transações

Um bloco é uma estrutura de encapsulamento das transações que serão incluídas no *Blockchain*. Ele é formado por duas partes: o cabeçalho e uma árvore contendo as transações. No cabeçalho, são salvas as informações do bloco, sendo elas: a data e hora que ele foi gerado, o valor compactado realizado, o *hash* do nó raiz da árvore de transações, além das informações de

hash do bloco anterior, permitindo o encadeamento sequencial entre eles. Além do cabeçalho, são salvas também todas as transações do bloco, organizadas por meio de uma árvore *Merkle* (TAPSCOTT; TAPSCOTT, 2016).

As transações também são armazenadas de forma encadeada, através de suas entradas e saídas. Por exemplo, no Bitcoin, cada transação é formada por basicamente 3 conjuntos de informações: os metadados, as entradas e as saídas. Os metadados compõem as informações sobre a transação, são eles: identificação da transação obtida através do cálculo da função *hash* SHA256, tamanho da transação, versão do código e a quantidade de entradas e saídas na transação. Já a parte de entradas é formada por uma lista de transações. Nesse campo, é adicionada também a chave para confirmar que aquela saída pode ser utilizada por essa entrada. No campo de saída, é informada a chave pública da conta que receberá o valor, podendo ser transacionado com a utilização da sua respectiva chave privada (BAMAKAN; MOGHADDAM; MANSHADI, 2021).

Figura 2 – Estrutura de Transações



Fonte: Adaptado de (ANTONOPOULOS, 2014)

A Figura 2 exemplifica como esse encadeamento entre transações ocorre. Ele só é possível de maneira segura devido à utilização de assinatura digital nas transações. Com isso, cada saída possui a chave pública do destinatário, o qual será o único que poderá criar uma transação utilizando essa saída como entrada em uma nova transação.

Um dos principais conceitos envolvidos na garantia de autenticidade e integridade das transações é o de assinatura digital. No *Blockchain*, todas as transações são assinadas digitalmente pelos usuários que as criaram por meio de um par de chaves, contendo uma pública e a outra privada. Esse par de chaves é gerado de maneira aleatória e é irreversível, ficando sob responsabilidade do usuário manter sua chave privada de maneira segura, já que a perda ou vazamento da referida resulta na impossibilidade definitiva de fazer transações no sistema, pois a chave privada é a única forma de garantia de autenticidade para novas transações com recursos

recebidos pela respectiva chave pública (BATISTA et al., 2018).

2.1.2 *Peer-to-Peer* (P2P)

A *Blockchain* é uma tecnologia caracterizada como distribuída visto que, as informações estão replicadas em diferentes nós espalhados pelo mundo por meio de uma rede P2P (CHUEN, 2015). Ademais, ela utiliza esse conceito de rede para manter um livro-razão distribuído, no qual cada nó presente nela é uma cópia do "livro"e trabalha colaborativamente para validar e registrar novas transações. O uso de uma rede P2P ajuda a garantir a descentralização e a segurança da *Blockchain* (NAKAMOTO, 2008).

Esse tipo de rede de computadores é caracterizada por permitir que, cada participante dela (nodo ou peer) possa atuar tanto como cliente quanto como servidor, compartilhando recursos – como espaço em disco e poder de processamento – diretamente uns com os outros sem necessidade de um servidor centralizado (SCHOLLMEIER, 2001). Nessas redes, cada participante consegue compartilhar recursos diretamente com outros nós, sem passar por um intermediário centralizado, de modo que permite essas redes se auto-organizem e sejam tolerantes à falhas, pois não existe apenas um ponto de falha na rede (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004). Seu uso em sistemas de *Blockchain* oferece vários benefícios, incluindo resistência à falhas, aumento da confiabilidade e capacidade de escala além de uma natureza descentralizada de redes P2P que torna os sistemas mais resistentes a ataques e censura (ANTONOPOULOS, 2014).

2.1.3 *Tradeoff*

O conceito de *tradeoff* em *Blockchain* está relacionado ao equilíbrio entre características técnicas e operacionais distintas que necessitam ser gerenciadas ao projetar e operar uma rede *Blockchain*. Esses *tradeoffs* de maneira geral envolvem aspectos como descentralização, segurança e escalabilidade, sendo conhecidos como o "trilema da *Blockchain*". Por exemplo, o aumento da descentralização de uma *Blockchain* pode diminuir a sua velocidade ou escalabilidade, pelo fato de que necessita de mais nós para validar as transações. Da mesma forma, aprimorar a escalabilidade por meio de blocos maiores ou tempos de blocos mais rápidos pode ajudar no comprometimento da segurança ou descentralização, de modo que torna a rede mais suscetível a ataques ou controle por entidades centralizadas (GUDGEON et al., 2020).

Nos últimos anos, a discussão sobre esses *tradeoffs* é vista como central na evolução das tecnologias *Blockchain*. Os pesquisadores e desenvolvedores vem buscando soluções que possam trazer o equilíbrio desses aspectos de maneira eficiente, como a implementação de *sharding*, cadeias laterais, e mecanismos de consenso considerados mais eficientes para aprimorar a escalabilidade sem comprometer de forma significativa a segurança ou descentralização. Essas inovações citadas anteriormente são fundamentais para o desenvolvimento contínuo e a adoção em massa das tecnologias de *Blockchain* (WANG et al., 2019).

2.2 Algoritmos de Consenso

Os algoritmos de consenso são mecanismos considerados fundamentais nos sistemas distribuídos, principalmente em *Blockchain*, para garantir a homogeneidade e confiabilidade das informações entre os nós distintos na rede. Esses algoritmos são projetados para atingir um acordo de confiança sobre um único estado no sistema entre os vários nós, mesmo que haja presença de falhas ou até mesmo nós mal-intencionados mantendo da integridade e segurança dos sistemas descentralizados (CACHIN; KURSAWE; SHOUP, 2000).

Esses algoritmos possuem um funcionamento no qual estabelece as regras e procedimentos para que os nós de uma rede distribuída possam entrar em acordo sobre o estado válido de um sistema. Num ambiente descentralizado, sem a presença de uma autoridade centralizadora, esses algoritmos podem garantir que todos os nós cheguem a um consenso, mesmo que hajam possíveis desacordos ou falhas (REBELLO et al., 2019). Os algoritmos de consenso são considerados fundamentais na resolução do problema de dupla despesa presente nas criptomoedas e para garantir a consistência das informações em bancos de dados distribuídos.

Segundo Zheng et al. (2017), os principais tipos de algoritmos de consenso são o *Proof of Work* (PoW), *Proof of Stake* (PoS), *Delegated Proof of Stake* (DPoS) e *Practical Byzantine Fault Tolerance* (pBFT). O primeiro é conhecido pelo uso no Bitcoin e baseia-se na resolução de problemas complexos de criptografia para realizar a validação das transações e criação de novos blocos. O PoS, é utilizado por criptomoedas como a Ethereum, de modo que depende da participação dos detentores de ativos digitais. O DPoS, é considerado uma variação do anterior, onde permite que ocorra a eleição de representantes para validar as transações. Já o pBFT possui destaque por conta da eficiência em sistemas que necessitam de uma rápida conclusão de transações e baixa latência.

O *Proof of Work* (Pow) é considerado um mecanismo de consenso utilizado em *Blockchain* onde necessita que os participantes da rede façam cálculos computacionais complexos. Esses cálculos, são frequentemente conhecidos como "mineração", visando a resolução de um problema matemático bastante desafiador. O primeiro a resolver o problema possui o direito de incluir um novo bloco ao sistema e adquirir recompensas em criptomoedas (NAKAMOTO, 2008). Este processo consegue garantir a segurança e descentralização da rede, mas também recebe críticas por conta do elevado consumo de energia.

O *Proof of Stake* (PoS) é uma alternativa ao anterior, pois busca superar desafios relacionados ao elevado consumo de energia. Neste algoritmo de consenso, a capacidade do usuário ao adicionar um bloco à *Blockchain*, não depende apenas do trabalho computacional, mas da quantidade de criptomoedas que ele possui e está disposto a "apostar". Quanto maior for o valor da aposta, maior é a probabilidade em ser escolhido para realizar a validação das transações e criação de novos blocos. Essa abordagem provoca uma eficiência energética considerada maior (KING; NADAL, 2012).

O *Practical Byzantine Fault Tolerance* (pBFT) é um algoritmo de consenso que foi projetado para sistemas distribuídos que conseguem tolerar falhas bizantinas. O conceito de falhas bizantinas descreve situações em sistemas distribuídos onde os componentes podem gerar falhas e, de forma complementar, apresentar comportamentos inconsistentes ou maliciosos, de modo que dificulta o estabelecimento de um consenso entre os demais componentes. Este conceito é fundamental para o entendimento da segurança e confiabilidade em sistemas distribuídos, como a *Blockchain*, onde a integridade e a confiança são consideradas essenciais. O mesmo permite que um sistema distribuído continue em funcionamento mesmo com a presença de alguns nós considerados maliciosos ou defeituosos (SOUSA; BESSANI; VUKOLIC, 2018). Este algoritmo é eficiente em relação aos termos de tempo de resposta e também requer uma menor quantidade de recursos computacionais quando comparado ao Pow, sendo assim, escolhido para atuar em sistemas que possuem uma elevada taxa de transações, além da baixa latência.

O *Delegated Proof of Stake* (DPoS) é visto como uma variação do *Proof of Stake* (Pow). Pois, neste algoritmo de consenso, os detentores dos *tokens* não fazem a validação de transações e blocos de forma direta. De outro modo, eles elegem os representantes, ou "delegados", para que realizem essas funções em seu nome. Esse método visa permitir uma maior escalabilidade e eficiência, pelo fato de reduzir o número de participantes que são necessários para atingir o consenso. Além disso, fornece um mecanismo de votação considerado democrático para a governança da rede, de modo que o poder do voto é relativamente proporcional à quantidade de criptomoedas que foram detidas (LARIMER, 2014).

2.3 *Blockchains* Públicas

As *Blockchains* Públicas (não permissionadas) são consideradas estruturas de dados que funcionam de maneira descentralizada e distribuída, onde cada bloco se conecta a outro formando uma espécie de cadeia. Este tipo de *Blockchain* é baseada nos princípios de criptografia visando transparência e imutabilidade. Nelas, qualquer indivíduo pode participar de todo o processo de validação e manutenção da rede (NAKAMOTO, 2008).

Seu funcionamento abrange a criação e verificação dos blocos de transações através de um consenso distribuído. Este processo é realizado por mecanismos de segurança, como: PoW ou PoS, garantindo a integridade e confiabilidade dos dados que foram registrados (ANTONOPOULOS, 2014).

As *Blockchains* Públicas mais notáveis incluem o Bitcoin, sendo a primeira e mais conhecida. A segunda é a Ethereum, pois introduziu os contratos inteligentes, onde esses contratos funcionam sem que haja a utilização de intermediadores. Além da Litecoin, que possui destaque por da rapidez e eficiência em comparação com o Bitcoin, fornecendo transações mais rápidas e menores custos (TASCA; HAYES; LIU, 2018).

2.3.1 Bitcoin

Bitcoin é uma moeda digital descentralizada que permite transações *peer-to-peer* sem a necessidade de intermediários, como bancos ou governos. Foi criada por uma pessoa ou grupo de pessoas sob o pseudônimo de Satoshi Nakamoto e lançada em 2009 como uma forma de permitir transações eletrônicas seguras (NAKAMOTO, 2008).

Essa moeda opera em uma rede descentralizada usando a tecnologia *Blockchain*. As transações são verificadas pelos nós da rede através de um processo chamado "mineração", que envolve a resolução de problemas matemáticos complexos. Uma vez que a transação é verificada, ela é adicionada a um novo "bloco"no sistema. O mecanismo de consenso utilizado é o PoW (ANTONOPOULOS, 2014).

O Bitcoin oferece várias vantagens, incluindo descentralização, resistência à censura, baixos custos de transação e pseudoanonimato. Também facilita pagamentos internacionais e oferece um novo modelo para a inclusão financeira de pessoas sem acesso a sistemas bancários tradicionais (TAPSCOTT; TAPSCOTT, 2016). Nessa criptomoeda, a privacidade de dados não é absoluta, mas sim pseudônima. Isso significa que, embora as transações sejam públicas e qualquer pessoa possa ver o histórico de transações de um endereço específico, a identidade real do proprietário desse endereço não é facilmente determinável (NARAYANAN et al., 2016).

Pelo fato de empregar um sistema de chaves públicas e privadas para facilitar as transações, detalhes como: quantidade de Bitcoins transferida e os endereços do remetente e do destinatário, são registrados publicamente na *Blockchain*. No entanto, esses endereços não estão diretamente ligados à identidade dos usuários, oferecendo um certo nível de privacidade (ANTONOPOULOS, 2014).

Isso oferece, ao Bitcoin, um grau de privacidade que é difícil de alcançar em sistemas financeiros tradicionais. Isto é particularmente útil para pessoas que desejam realizar transações sem a necessidade de intermediários, como bancos, que normalmente requerem informações pessoais detalhadas para cumprir regulamentações como a *Know Your Customer* (KYC) (ZOHAR, 2015).

2.3.2 Ethereum

Ethereum é uma plataforma de computação descentralizada baseada em *Blockchain*, lançada em 2015 por Vitalik Buterin e outros co-fundadores. Diferentemente do Bitcoin, que foi projetado principalmente como uma moeda digital, ele foi criado para servir como uma "máquina virtual"global que permite aos desenvolvedores escrever e implantar contratos inteligentes (WOOD et al., 2014).

Sua operação é feita com uma *Blockchain* que registra transações e estados de contratos inteligentes. Estes são códigos autoexecutáveis que residem na *Blockchain* e são ativados por transações. Ele usa o algoritmo de consenso de PoW similar ao Bitcoin, mas está em transição

para um modelo de PoS chamado Ethereum 2.0 (BUTERIN; GRIFFITH, 2017).

A plataforma oferece uma série de benefícios, incluindo flexibilidade para criar uma ampla variedade de aplicações descentralizadas (DApps), desde finanças descentralizadas (DeFi) até sistemas de identidade digital e mercados de tokens não fungíveis (NFTs). Ela também fornece um ambiente robusto e seguro para a execução de contratos inteligentes, possibilitando a automação de processos e acordos (MAURER; NELMS; SWARTZ, 2013).

O Ethereum opera em um modelo de privacidade pseudônima, no qual as transações e os contratos são visíveis na *Blockchain*, mas as identidades dos participantes não são diretamente reveladas (ZOHAR, 2015). Os endereços usados nas transações não estão necessariamente vinculados às identidades reais dos usuários, proporcionando um certo nível de privacidade. No entanto, uma vez que a plataforma também suporta contratos inteligentes, os dados podem ser armazenados de forma transparente na *Blockchain*, o que pode ser tanto uma vantagem como um desafio para a privacidade (ATZEI; BARTOLETTI; CIMOLI, 2017).

Ao proporcionar um ambiente em que os contratos e os dados podem ser verificados publicamente sem revelar as partes envolvidas – vantajoso em cenários como votações descentralizadas ou na prova de autenticidade de documentos – é essencial observar que a privacidade não é uma garantia absoluta na rede Ethereum e depende muito da implementação específica do contrato inteligente ou da DApp (TAPSCOTT; TAPSCOTT, 2016).

2.3.3 Contratos Inteligentes

Os contratos inteligentes são contratos autoexecutáveis com o código do contrato diretamente escrito em linhas de código. Eles operam em um ambiente de *Blockchain*, tornando as transações transparentes, imutáveis e sem a necessidade de intermediários (SZABO, 1997).

Um contrato inteligente é um programa autoexecutável, livre de interferências, descrito em uma linguagem de programação, onde todos os termos são definidos diretamente em seu código, sem a possibilidade de alteração ou violação das cláusulas executadas como foram descritas (DWYER, 2015).

Esse contrato é acionado por eventos específicos e condições definidas previamente. Quando essas condições são atendidas, o contrato é automaticamente executado. Isso significa que os termos do contrato são autoexecutáveis e autoverificáveis, sem necessidade de terceiros (MAURER; NELMS; SWARTZ, 2013).

Apesar de diversas redes *Blockchains* conseguirem executa-los, a plataforma Ethereum foi a pioneira em permitir a criação de contratos inteligentes sem se limitar a uma finalidade, como, por exemplo, a financeira. Estes contratos conseguem assegurar, de forma autônoma, o cumprimento de suas condições e as consequências descritas para cada situação, de maneira rastreável, irreversível e independente da figura de alguma entidade confiável (STALLINGS; BRESSAN; BARBOSA, 2008; REVOREDO, 2019).

O uso de contratos inteligentes oferece vários benefícios, incluindo a redução de custos, já que elimina a necessidade de intermediários; aumento da eficiência, pois as transações são automatizadas e ocorrem em tempo real; além da maior segurança e transparência, proporcionadas pela tecnologia *Blockchain* (MULLAN, 2018; CHRISTIDIS; DEVETSIKIOTIS, 2016).

Lançado em 2014, por Vitalik Buterin, o Ethereum tem por objetivo levar o conceito de contratos inteligentes para diversos modelos contratuais que possam ter suas cláusulas programadas, tais como transferências financeiras, campanhas de *crowdfunding*, votações, apólices de seguros, registros de direitos autorais, entre outras aplicações (BUTERIN; GRIFFITH, 2017).

2.4 *Blockchains* Privadas

Blockchains privadas (permissionadas) operam em um ambiente fechado e são acessíveis apenas para entidades autorizadas. Essas redes são geralmente mais rápidas e eficientes, mas também são mais centralizadas, o que pode comprometer alguns dos benefícios inerentes à tecnologia blockchain, como imutabilidade e resistência à censura (MENDLING et al., 2018).

Em ambientes fechados, o acesso é restrito a entidades específicas, como membros de uma organização ou partes de uma cadeia de suprimentos. A validação das transações e a criação de novos blocos são feitas por nós predefinidos, e não há necessidade de um mecanismo de consenso baseado em competição, como o PoW ou PoS (CACHIN et al., 2016).

Entre os benefícios das *Blockchains* privadas estão: a eficiência, já que as transações são confirmadas mais rapidamente, e a escalabilidade, devido a menores requisitos computacionais. Além disso, elas oferecem mais controle sobre a governança e a privacidade dos dados, o que pode ser essencial para empresas e organizações (MIERS et al., 2013).

Alguns dos exemplos notáveis de *Blockchains* privadas incluem Hyperledger, uma iniciativa da Linux Foundation para avançar em tecnologias de *Blockchain* multi-indústria; R3's Corda, voltada principalmente para o setor financeiro; e Quorum, que é uma versão empresarial do Ethereum 2.0 (ANDROULAKI et al., 2018).

2.4.1 Hyperledger

Hyperledger é um projeto de *Blockchain* de código aberto hospedado pela Linux Foundation, lançado em 2015. Ele reúne várias partes interessadas, incluindo empresas, desenvolvedores e acadêmicos, para colaborar no desenvolvimento de frameworks e ferramentas *Blockchain* voltadas para soluções empresariais (ANDROULAKI et al., 2018; CACHIN et al., 2016)

Por conta disso, não é uma *Blockchain* única, mas um guarda-chuva de *frameworks* e ferramentas. Hyperledger Fabric, um desses *frameworks*, oferece uma arquitetura modular e *plug-and-play* para criar soluções de *Blockchain*. O consenso nela pode ser alcançado por meio

de uma variedade de algoritmos, permitindo mais flexibilidade em comparação com *Blockchains* públicas como Bitcoin ou Ethereum (VUKOLIĆ, 2016).

Ele oferece várias vantagens para empresas, como a escalabilidade, a eficiência e a privacidade aprimoradas. Essa tecnologia também permite a integração mais fácil com sistemas de Tecnologia da Informação (TI) existentes, além de uma variedade de opções para customização e extensibilidade (MAZIERES, 2015).

O projeto de *Blockchain* empresarial oferece vários *frameworks*, como o modelo Fabric. Esses *frameworks* são projetados para atender a requisitos de privacidade rigorosos que são frequentemente exigidos em cenários empresariais. Por exemplo, apresenta "canais"que permitem a criação de um subconjunto de participantes que podem realizar transações privadas entre si. Além disso, ele fornece várias opções para o armazenamento seguro de dados e permite o controle granular sobre quem pode acessar esses dados (ANDROULAKI et al., 2018; CACHIN et al., 2016).

É importante ressaltar que a privacidade em sistemas como o Hyperledger é ajustável de acordo com as necessidades específicas da organização ou do consórcio que o utiliza. O modelo de governança e as políticas de acesso podem ser personalizados para garantir que apenas partes autorizadas possam ver ou interagir com as informações na *Blockchain* (CROSBY et al., 2016; MAZIERES, 2015).

Além dos benefícios já mencionados, também há a possibilidade de integrar soluções de privacidade como o uso de ZKP para validações que não requerem a divulgação de informações sensíveis (KOSBA et al., 2016). Essa tecnologia continua a evoluir, com a comunidade de desenvolvimento ativamente trabalhando em melhorias que podem reforçar ainda mais a privacidade e a segurança dos dados.

Novos módulos e características, como os oráculos para interação com fontes de dados externas, também estão em desenvolvimento, o que poderia oferecer novas formas de garantir a privacidade dos dados (TAPSCOTT; TAPSCOTT, 2016; MAZIERES, 2015).

2.5 *Blockchains* Híbridas

Blockchains híbridas combinam elementos de *Blockchains* públicas e privadas. Elas oferecem um modelo flexível e personalizável para atender a necessidades específicas, como permitir transações públicas em um ambiente geralmente restrito ou fornecer diferentes níveis de permissão para diferentes tipos de usuários (TAPSCOTT; TAPSCOTT, 2016).

Não só isso, como também as *Blockchains* híbridas oferecem uma combinação de transparência e privacidade, além de permitir uma escalabilidade e eficiência superiores em comparação com as puramente públicas. Elas são especialmente úteis para organizações que precisam realizar transações tanto públicas quanto privadas, permitindo uma maior flexibilidade

operacional (ZHENG et al., 2018).

Nas *Blockchains* híbridas algumas das transações ou dados podem ser privados, de modo que são acessíveis somente aos participantes que foram autorizados, enquanto que as outras partes da *Blockchain* conseguem ter exposição ao público. Dessa forma permite que as organizações possam manter a confidencialidade das informações sensíveis, além de se beneficiarem com a transparência e segurança inerentes às *Blockchains* públicas. A flexibilidade da *Blockchain* híbrida é vista como atraente para as empresas que precisam de uma solução personalizada, que seja capaz de atender aos requisitos específicos de privacidade e abertura (ZHENG et al., 2017).

Dragonchain e Kadena são exemplos de *Blockchains* híbridas que procuram fornecer a segurança e a transparência de uma *Blockchain* pública com a eficiência e a privacidade de uma *Blockchain* privada. A R3 Corda também tem capacidades híbridas, permitindo uma variedade de casos de uso no setor financeiro e além (BROWN et al., 2016).

2.6 *Blockchains* de Consórcio

Blockchains de consórcio são definidas como semi-privada, sendo adequadas para ambientes de negócios que possuem a necessidade de um certo nível de privacidade e controle, possibilitando a manutenção de alguns dos benefícios das tecnologias de *Blockchain*, como é o caso da imutabilidade e transparência (TAPSCOTT; TAPSCOTT, 2016).

Diferentemente das *Blockchains* públicas que frequentemente utilizam o PoW ou PoS, as *Blockchains* de consórcio de maneira geral empregam mecanismos de consenso considerados mais eficientes e menos intensivos tratando-se do consumo de energia, como é o caso do PoA ou então dos algoritmos de consenso que são baseados em votação (BUTERIN et al., 2014).

Nas *Blockchains* de consórcio o controle da rede é compartilhado entre os membros do consórcio, pois são eles que determinam quem pode participar da rede e em quais condições. Isso é visto como ideal para situações onde a colaboração entre várias organizações é considerada essencial, de modo que permite a criação de um sistema de registros compartilhado com as regras de governança que foram definidas coletivamente (PETERS; PANAYI, 2016).

Parte das *Blockchains* de consórcio são construídas e utilizadas em setores específicos, como finanças, saúde ou até mesmo cadeias de suprimentos, onde os participantes possuem interesses que estão alinhados e necessitam do compartilhamento de dados (CROSBY et al., 2016). Existem também *Blockchains* de consórcio que são usadas com base na localização geográfica, principalmente em casos que envolvem as regulamentações locais ou então necessidades específicas de dados regionais (SWAN, 2015).

2.7 Redes Permissionadas e Não Permissionadas

As redes permissionadas possuem o acesso restrito e controlado por uma entidade ou grupo de entidades. Nestas redes, os participantes necessitam de autorização para juntar-se e realizar interações diretamente com a *Blockchain* (VUKOLIĆ, 2016).

Nas redes permissionadas, o processo de validação das transações ocorre sendo gerenciado por nós confiáveis, escolhidos pelo administrador da rede. Dessa forma, pode resultar numa maior eficiência e escalabilidade, embora exija uma menor descentralização (CACHIN; VUKOLIĆ, 2017).

Existem diversos tipos de redes permissionadas, como é o caso das *Blockchains* de consórcio, onde várias organizações gerenciam a rede, e *Blockchains* privadas, que são gerenciadas por uma única organização (ANDROULAKI et al., 2018).

Enquanto que as redes não permissionadas são abertas, e permitem que qualquer um indivíduo participe sem que haja necessidade de autorização prévia. Essas redes são consideradas tipicamente descentralizadas, e possuem um elevado grau de transparência (NARAYANAN et al., 2016).

Nas redes não permissionadas, qualquer pessoa pode tornar-se um nó validador, participando do processo de consenso, como acontece na mineração no Bitcoin. Podendo oferecer um elevado grau de segurança e imutabilidade, mas também resultando em desafios de escalabilidade (FILIPPI; LOVELUCK, 2016).

2.8 Criptografia

A criptografia é um mecanismo utilizado para a proteção da privacidade e também para a segurança de dados confidenciais de um usuário, transformando-os em informações ininteligíveis, que só podem ser lidas por quem possui a chave de descriptografia. Ela é crucial por permitir que esses dados sejam protegidos seguramente, tendo em vista que, no mundo atual, quase todas as informações são passadas por um sistema de computadores *online* (TEIXEIRA, 2022).

Ao criar uma transação, o usuário calcula um valor *hash* derivado dos dados da transação e assina com sua chave privada antes de realizar o envio, garantindo que aquela transação foi realizada por ele. Juntamente com o envio da transação, é enviada também a respectiva chave pública, a qual permite a verificação da autenticidade e integridade dos dados recebidos (ZHENG et al., 2018).

A criptografia em regra, utilizada na *Blockchain*, é nomeada como *Secure Hash Algorithm* (Algoritmo de Dispersão Seguro) sendo o *SHA256* um algoritmos de *hash* que protege dados não importando o tamanho. Em uma cadeia, sempre haverá 32 *bytes* (256 *bits* / 8 *bits* por *byte* = *32 bytes*) de extensão devido à especificação do próprio algoritmo. Diante disto, o *SHA256* é o

algoritmo de *hash* mais atuante no cotidiano. A criptografia gera duas informações fundamentais para quem deseja transitar dados sem risco de ser quebrado, são elas: as chaves pública e privada (ALI et al., 2016).

A criptografia de chave assimétrica é considerada um dos pilares da *Blockchain*. A mesma usa um par de chaves, uma pública e uma privada, para que seja possível garantir as transações de maneira segura. A chave pública é utilizada para criptografar a transação, enquanto a chave privada é utilizada para descriptografá-la. Este método é visto como essencial para assegurar que apenas o destinatário que foi pretendido consiga ter o acesso aos dados que foram transmitidos (NARAYANAN et al., 2016).

Além disso, os algoritmos de *hash*, como *SHA-256* no Bitcoin, são utilizados para gerar um resumo único para cada transação e bloco. Estes *hashes* são considerados cruciais para que seja possível manter a integridade e também a ordem cronológica dos blocos na *Blockchain*. Tendo em vista que um bloco é adicionado à cadeia, alterá-lo torna-se uma tarefa computacionalmente impraticável por conta da necessidade de *rehash* em todos os blocos posteriores (ANTONOPOULOS, 2014).

Outro algoritmo considerado importante é o PoW, utilizado em várias *Blockchains* para validar as transações e adicionar os novos blocos à cadeia. O PoW necessita que os participantes da rede, que são conhecidos como mineradores, consigam resolver problemas matemáticos complexos, de modo que ajuda na proteção da rede contra possíveis ataques e manipulações (SWAN, 2015).

Tabela 1 – Tipos de Criptografias

Chaves simétricas	São chaves que possuem o mesmo código de acesso para o emissor e para o receptor da informação, ou seja, a mesma chave é utilizada para cifrar e descriptografar as informações. Não é recomendada para a proteção de dados extremamente sigilosos, visto que dá acesso para ambas as partes.
Chaves assimétricas	É um método de codificação que utiliza duas chaves diferentes: uma chave pública, compartilhada com o público, para criptografar a mensagem, e uma chave privada, mantida em segredo, para descriptografá-la, sendo possível usar a primeira para criptografar algo destinado a alguém sem correr o risco da privacidade ser comprometida, pois somente a pessoa com a última poderá descriptografá-la.

Fonte: Elaborado pelo Autor

Sendo assim, a encriptação da mensagem ocorre com a utilização da chave pública a quem for destinada à mensagem e para decriptar utiliza-se a chave privada e se alguém interferir na comunicação e captar a informação que for transmitida ela não conseguirá ler, pois estará embaralhada pelo algoritmo. Vale ressaltar que uma chave privada gera novamente uma chave pública, mas uma chave pública nunca gera uma chave privada (ALI et al., 2016).

2.9 Privacidade de Dados

A privacidade de dados refere-se ao direito dos indivíduos de controlar como suas informações pessoais são coletadas, armazenadas e utilizadas. Além da abrangência de proteção dos dados contra os vazamentos e acessos não autorizados (SOLOVE, 2005).

O conceito de privacidade de dados está em constante evolução por conta do avanço da tecnologia, onde a coleta, o processamento e a disseminação de dados pessoais tornaram-se práticas muito comuns, fazendo uma ampliação dos desafios inerentes à proteção da privacidade (BYGRAVE, 2014).

A privacidade de dados está profundamente relacionada com a noção do consentimento informado, onde os indivíduos possuem o direito de serem informados de como suas informações estão sendo utilizadas e de aprovar esta prática de maneira explícita. Este aspecto é crucial para proporcionar uma relação de confiança entre indivíduos e entidades que realizam o processamento dos dados (HARTZOG, 2018).

Na *Blockchain*, a privacidade de dados é geralmente mantida por meio de técnicas de criptografia que protegem tanto a identidade dos usuários quanto o conteúdo das transações. Alguns sistemas, como o *Zerocoin* (atual *Zcash*) e *Monero*, incorporam tecnologias como *Zero-Knowledge Proof* (ZKP) e *Ring Signatures*, respectivamente, para garantir um elevado grau de privacidade (BEN-SASSON et al., 2014).

Os benefícios desta incluem a garantia de transações seguras e privadas, resistência à censura e a capacidade de controlar o acesso às informações pessoais. O caráter imutável e transparente da *Blockchain* também facilita a auditoria e aumenta a confiança no sistema (NARAYANAN et al., 2016).

Esta é uma área em constante evolução que oferece um conjunto diversificado de técnicas e mecanismos, dependendo do tipo de *Blockchain* (pública, privada ou híbrida) e das necessidades específicas dos usuários e organizações (ZOHAR, 2015).

2.10 Lei Geral de Proteção de Dados (LGPD)

A partir do surgimento da LGPD, que passou a ser vigente em 18 de setembro de 2020, as sanções administrativas passaram a valer a desde o dia 01 de agosto de 2021, onde os riscos de vazamento de dados nas empresas podem gerar prejuízos financeiros, atingindo até 2% do faturamento anual ou 50 milhões de reais, vale o maior, além da possibilidade de perda do faturamento em decorrência da falta de operação ou danos à imagem e também a reputação podendo reter valores considerados inestimáveis.

A LGPD é considerada um marco legislativo brasileiro importante, onde altera de forma relevante o recente modelo de coleta e tratamento indiscriminado dos dados pessoais para um

novo modelo em que a coleta e o tratamento é apenas referente ao necessário. A regulamentação brasileira aporta em si mesma os fundamentos que ressaltam a proteção dos direitos e garantias da pessoa natural, por exemplo: o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da intimidade, ao desenvolvimento econômico e tecnológico, como também da livre iniciativa e respeito aos direitos humanos (STELZER et al., 2019 apud BRASIL, 2018).

A LGPD enumera os direitos específicos que devem ser exercidos por qualquer pessoa natural que seja titular dos dados pessoais, com ressalva para casos previstos pela lei. De todo modo, o controlador, o qual toma as decisões referentes ao tratamento dos dados pessoais, precisa obter todas as permissões geradas pelo titular dos dados, sem ignorá-las (MALDONADO; BLUM, 2019). A implementação de padrões, como é o caso da NBR 27001 (2013), pode ser vista como um exemplo de boa estratégia para as empresas se adequarem às exigências da LGPD.

A NBR 27001 (2013) solicita a adoção de uma perspectiva de gestão de risco para segurança da informação, exigindo que as organizações realizem a identificação, avaliação e o tratamento dos riscos relacionados a segurança da informação. Essa norma não especifica de maneira exata quais são os controles que precisam ser implementados, porém oferece um conjunto amplo de melhores práticas através da sua anexação à (NBR ISO/IEC 27002, 2013), que faz orientação sobre os controles de segurança da informação que as organizações conseguem escolher ou implementar (CHAPPLE; STEWART; GIBSON, 2018).

O consentimento informado, previsto na LGPD, é considerado uma manifestação livre, informada e inequívoca na qual o titular aceita o tratamento dos dados pessoais para uma finalidade específica (BRASIL, 2018). Para que o consentimento seja válido, o mesmo precisa ser dado de forma clara e específica para as finalidades legítimas, explícitas e informadas ao titular, de modo que possa assegurar a autonomia e o controle sobre os dados pessoais.

O direito de ser esquecido, conforme explícito no contexto da LGPD, refere-se à possibilidade do indivíduo em realizar uma solicitação de remoção dos dados pessoais de um determinado banco de dados ou serviço (VALIM, 2022). Esse direito é bastante significativo em casos onde os dados não são mais considerados necessários para a finalidade na qual foram coletados, ou então quando o consentimento para uso foi revogado.

A anonimização de dados, segundo a LGPD, é o processo onde um dado pessoal não possui a possibilidade de associação, direta ou indireta, a um indivíduo. Ocorre de maneira que o dado não consiga ser utilizado para identificação do indivíduo (BRASIL, 2018). A anonimização é considerada uma ferramenta fundamental na proteção da privacidade, pelo fato de permitir o uso de dados em pesquisas e análises sem que haja o comprometimento da identidade dos indivíduos.

2.11 General Data Protection Regulation (GDPR)

A General Data Protection Regulation (GDPR), implementada na Europa em 2018, é considerada uma das regulamentações mais rigorosas de privacidade de dados em todo o mundo. A GDPR não somente eleva as exigências para todas as organizações no tratamento dos dados pessoais, como também revigora os direitos dos indivíduos, proporcionando-lhes um maior controle sobre as informações pessoais. Esta regulamentação vem influenciando as políticas de privacidade no mundo e estabelecendo um moderno modelo de forma global para a proteção de dados (KUNER; BYGRAVE; DOCKSEY, 2020).

A relevância dessa regulamentação refere-se à capacidade de equilíbrio nos interesses econômicos e tecnológicos em se tratando dos direitos de privacidade dos indivíduos, demonstrando um reconhecimento progressivo sobre a importância e necessidade de governança e proteção de dados dos cidadãos evitando o uso não autorizado das informações pessoais (SCHWARTZ; PEIFER, 2020).

O consentimento informado explícito na GDPR é uma forma de indicação da vontade livre, específica, informada e inequívoca, pela qual os indivíduos aceitam o processamento dos seus dados pessoais. O consentimento deve ser realizado através de uma declaração clara ou então por uma ação afirmativa clara. Sendo assim, significa dizer que a inatividade, caixas de seleção pré-marcadas ou omissão não fazem parte do consentimento válido previsto pela GDPR. Além disso, precisa ser fácil retirar o consentimento na mesma proporção que o mesmo for dado (REGULATION, 2018).

O direito de ser esquecido, exposto na GDPR, é mais conhecido como "direito ao apagamento". O mesmo permite que os indivíduos façam a solicitação de remoção dos seus dados pessoais de sistemas e bancos de dados de organizações, perante algumas condições. Este direito é aplicável, por exemplo, quando os dados pessoais não são considerados necessários para os fins pelos quais foram coletados, ou então quando o consentimento para o processamento foi retirado e não existe mais outro fundamento legal para que ocorra tal processamento (FEILER; FORGÓ; WEIGL, 2018).

A anonimização dos dados, conforme previsto pela GDPR, envolve o processamento de dados pessoais de maneira que os dados não possam mais estar atribuídos a um indivíduo em específico sem que ocorra o uso de informações adicionais. Visto que os dados foram efetivamente anonimizados, eles não vão se enquadrar mais perante o âmbito da GDPR, pois os mesmos não constituem os dados pessoais. A anonimização é considerada uma ferramenta muito poderosa que pode aprimorar a privacidade enquanto a mesma permite a análise e o utilização de vários conjuntos de dados (REGULATION, 2018).

2.12 NBR ISO/IEC 27001

A NBR 27001 (2013) é uma norma brasileira com foco em Sistemas de Gestão de Segurança da Informação (SGSI). Ela apresenta um modelo que: estabelece, opera, monitora, revisa, mantém e aprimora a segurança da informação. A mesma é reconhecida globalmente e utilizada por diversas organizações que procuram realizar o gerenciamento de maneira segura dos ativos de informação, como é o caso dos dados financeiros, da propriedade intelectual e também de informações confidenciais dos colaboradores e clientes.

Esta norma é uma ferramenta de implementação que diz o que precisa ser feito na segurança da informação, com objetivo da integridade, confidencialidade e a disponibilidade da informação. Principalmente com a finalidade de mitigar o risco como apresenta SKYPRO (2018), "é a maneira mais eficiente de mitigação do risco de sofrer uma violação de informações de dados". Desta forma, ela é importante para identificar os possíveis empecilhos ao fiscalizar as ameaças ou buscar resposta para os perigos previstos. Este gerenciamento de segurança da informação é estabelecido pela própria organização com finalidade de obter certificado por meio de auditoria.

O funcionamento da NBR 27001 (2013) é feito através da implementação de um SGSI, que faz a inclusão de uma avaliação sistemática dos riscos relacionados a segurança da informação, sempre considerando as ameaças, vulnerabilidades e impactos existentes. Esta norma exige das organizações que desenvolvam e implementem um conjunto extensivo de controles em segurança da informação, além de outros tipos de medidas voltadas ao gerenciamento de riscos para o enfrentamento destes considerados inadmissíveis. Também demanda um processo contínuo, que abrange o monitoramento e a revisão frequente do sistema de gestão, tal como um processo de melhoria contínua (HONAN, 2017).

A norma técnica possui uma relação considerada significativa quando se trata de privacidade de dados, pois oferece um *framework* para proteção das informações pessoais contra o acesso de indivíduos não autorizados, o que é considerado essencialmente relevante no contexto de aumento das regulamentações globais de proteção de dados. Ao implementar a NBR 27001 (2013), as organizações auxiliam no cumprimento com as regulamentações de proteção de dados, diminuindo os riscos de violações dos dados e aprimorando a gestão da privacidade (CHAPPLE; STEWART; GIBSON, 2013).

3

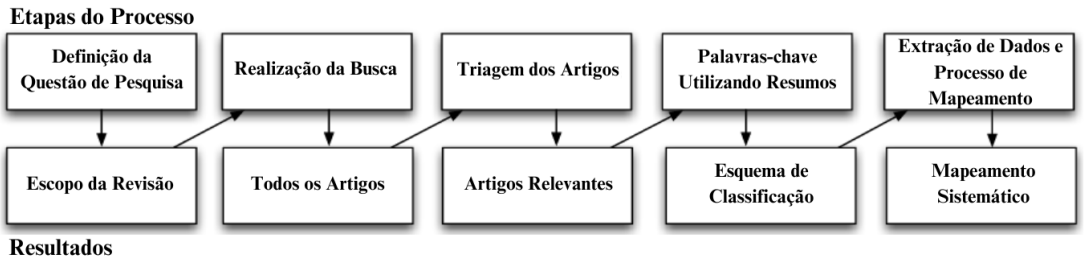
Mapeamento Sistemático

Este capítulo apresenta a metodologia baseada em uma abordagem qualitativa e quantitativa, com o objetivo de investigar a conformidade regulatória da *Blockchain* com a Lei Geral de Proteção de Dados (LGPD) ou General Data Protection Regulation (GDPR) em relação ao conceito de privacidade de dados.

3.1 Metodologia

O Mapeamento Sistemático da Literatura (MSL), conforme dito por Petersen (2015), é uma metodologia de pesquisa utilizada para categorização e sintetização da literatura existente sobre um determinado tema. Esta abordagem é geralmente usada no campo da engenharia de software, ainda que também possa ser aplicada em áreas diversas. Essa metodologia de pesquisa possui várias etapas-chave, conforme visto na Figura 3.

Figura 3 – Etapas de um Mapeamento Sistemático da Literatura



Fonte: Adaptado de (PETERSEN, 2015)

3.2 Questões de Pesquisa

O objetivo deste MSL é mapear os artigos publicados nos últimos 5 (cinco) anos completos, compreendendo o período de janeiro de 2018 à dezembro de 2023, que abordem

sobre privacidade de dados em *Blockchain*, visando a conformidade regulatória com a LGPD ou GDPR. A pesquisa leva em consideração os termos e conceitos similares entre as duas regulamentações de proteção de dados, como por exemplo: anonimização, pseudonimização, direito de ser esquecido e consentimento informado. Dessa forma, foi definida a seguinte questão de pesquisa principal que conduz o estudo: "Quais mecanismos e técnicas de privacidade de dados em *Blockchain* possuem conformidade regulatória com a LGPD ou GDPR?". Para que fosse possível responder a está questão, foi necessário extrair outras 4 (quatro) questões de pesquisa apresentadas a seguir: **QP1)** Quais as principais preocupações discutidas a respeito da privacidade de dados em *Blockchain*? **QP2)** Quais os desafios enfrentados em relação à privacidade de dados em *Blockchain*? **QP3)** Quais as soluções propostas para lidar com as questões de privacidade de dados em *Blockchain*? **QP4)** Qual o método de pesquisa utilizado?

3.3 Estratégia de Busca

Esta subseção apresenta uma *string* de busca automática que foi utilizada para realizar a busca dos artigos científicos na plataforma Periódicos CAPES e nas seguintes bases científicas: *Web of Science*, *SpringerLink* e *IEEE Xplore*. A Tabela 2 representa a *string* de busca genérica que foi utilizada na pesquisa, podendo sofrer alterações em cada uma das bases de forma específica.

Tabela 2 – *String* de Busca

***String* de Busca**
((”Blockchain” AND (”Privacidade de Dados” OR ”Data Privacy’) AND (”Lei Geral de Proteção de Dados” OR ”General Data Protection Regulation”))

Fonte: Elaborado pelo Autor

3.4 Critérios de Seleção

A partir disso, foram definidos critérios de inclusão e exclusão para realizar a filtragem dos trabalhos acadêmicos que possuíam relação direta com a pesquisa. Os critérios de inclusão contém: **CI-1)** Artigos completos em português ou inglês. **CI-2)** Artigos publicados em conferências ou periódicos entre os anos de 2018 e 2023. **CI-3)** Artigos que possuíam os assuntos *Blockchain*, Privacidade de Dados, LGPD ou GDPR. Enquanto que os critérios de exclusão contém: **CE-1)** Artigos sem o texto completo disponível. **CE-2)** Artigos incorretos ou que não possuíam relação com o tema. **CE-3)** Artigos duplicados.

3.5 Análise dos Resultados

Dos trabalhos que foram retornados após a utilização da *string* de busca apresentada na Tabela 2, foi obtido um total 7.630 trabalhos inclusos nessas 3 (três) bases de dados acadêmicas,

conforme visto na Tabela 3.

Tabela 3 – Resultados da *String* de Busca

Bases de Dados	**Número de Artigos**
Web of Science	5.341
SpringerLink	1754
IEEE Xplore	535
Total	**7.630**

Fonte: Elaborado pelo Autor

Dentre os 7.630 trabalhos encontrados, após aplicação dos critérios de inclusão, verificou-se que 4.197 não atendiam aos critérios estabelecidos ou eram duplicados. Ao retirá-los da lista, restaram 3.433 trabalhos, os quais tiveram os critérios de exclusão aplicados por meio da leitura do título, caso o título não tivesse nenhuma relação com o tema, foi lido o resumo ou *abstract* de cada um. Dessa forma, foi possível identificar quais os trabalhos que trariam algum tipo de contribuição de fato para esta pesquisa. Após aplicação dos critérios de exclusão, os artigos relacionados com a pesquisa capazes de responder as questões pertinentes ao estudo foram lidos por completo. Foram selecionados um total de 25 artigos condizentes com o tema e questões de pesquisa, conforme visto na Tabela 4.

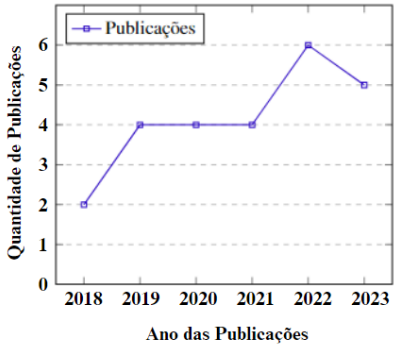
Tabela 4 – Apoś Critérios de Inclusão e Exclusão

Bases de Dados	**Número de Artigos**
Web of Science	12
SpringerLink	5
IEEE Xplore	8
Total	**25**

Fonte: Elaborado pelo Autor

Na Figura 4, é possível observar a quantidade de publicações por ano, entre os anos de 2018 e 2023, referente aos trabalhos selecionados conforme os critérios que foram estabelecidos.

Figura 4 – Publicações por Ano



Fonte: Elaborado pelo Autor

3.6 Trabalhos Selecionados

Na Tabela 5 estão listados os 25 (vinte e cinco) trabalhos selecionados, a partir dos critérios de inclusão e exclusão descritos.

Tabela 5 – Trabalhos Selecionados

Autores	**Principal Área de Aplicação**	**Base**
Han e Park (2022)	Gerenciamento de Informações Pessoalmente Identificáveis (PII)	IEEE Xplore
Arbabi et al. (2023)	Gestão de Dados da Saúde	IEEE Xplore
Roman-Martinez et al. (2023)	Gestão de Consentimentos, Controle de Acesso e Auditoria	IEEE Xplore
Politou et al. (2021)	Conformidade Jurídica	IEEE Xplore
Haque et al. (2021)	Conformidade Jurídica	IEEE Xplore
Al-Zaben et al. (2018)	Gerenciamento de Informações Pessoalmente Identificáveis (PII)	IEEE Xplore
Lee et al. (2022)	Gestão de Ativos Digitais	IEEE Xplore
Schaefer e Edman (2019)	Conformidade Jurídica	IEEE Xplore
Wylde et al. (2022)	Gestão da Segurança da Informação	SpringerLink
Ma, Cao e Xiong (2020)	Gestão de Consentimentos, Controle de Acesso e Auditoria	SpringerLink
Boulos, Wilson e Clauson (2018)	Gestão de Dados da Saúde	SpringerLink
Upadrista, Nazir e Tianfield (2023)	Gestão da Segurança da Informação	SpringerLink
Ahmed et al. (2020)	Conformidade Jurídica	SpringerLink
Rantos et al. (2019)	Gestão de Consentimentos, Controle de Acesso e Auditoria	Web of Science
Merlec et al. (2021)	Gestão de Consentimentos, Controle de Acesso e Auditoria	Web of Science
Kakarlapudi e Mahmoud (2021)	Gestão de Consentimentos, Controle de Acesso e Auditoria	Web of Science
Xu et al. (2022)	Conformidade Jurídica	Web of Science
Reegu et al. (2023)	Gestão de Dados da Saúde	Web of Science
Chiarini e Compagnucci (2022)	Conformidade Jurídica	Web of Science
Haro-Olmo, Varela-Vaca e Álvarez-Bermejo (2020)	Gestão da Segurança da Informação	Web of Science
Dick e Praktiknjo (2019)	Gestão da Segurança da Informação	Web of Science
Kassem et al. (2019)	Gerenciamento de Informações Pessoalmente Identificáveis (PII)	Web of Science

Autores	**Principal Área de Aplicação**	**Base**
Bai et al. (2022)	Gestão de Dados da Saúde	Web of Science
Alves et al. (2020)	Conformidade Jurídica	Web of Science
Fekete e Kiss (2023)	Conformidade Jurídica	Web of Science

Fonte: Elaborado pelo Autor

O trabalho de Han e Park (2022) discute os desafios da privacidade e proteção de dados em *Blockchain*, focando principalmente nos conceitos de imutabilidade e transparência. É apontada a dificuldade na alteração ou exclusão dos dados pessoais, de modo que desafia o "direito de ser esquecido", enquanto a transparência pode revelar as informações sensíveis, conflitando com as regulamentações de proteção de dados, como GDPR na Europa. Para enfrentar os desafios existentes, os autores propuseram o uso de criptografia e pseudonimização na proteção dos dados pessoais, visando garantir o acesso apenas para partes autorizadas e manutenção da confidencialidade. Além disso, foi sugerida a anonimização dos dados para que fosse possível desvincular as informações de identidade dos usuários. Ademais, recomenda-se a utilização dos contratos inteligentes, pois permite aos usuários o controle de uso dos dados pessoais, possibilitando que as preferências de privacidade possam ser respeitadas e aplicadas de maneira automatizada. As soluções propostas buscam equilibrar o funcionamento da *Blockchain* com as exigências previstas na GDPR.

O trabalho de Arbabi et al. (2023) aborda as implicações do uso da *Blockchain* na área da saúde, com foco nas questões de privacidade de dados. Destaca-se que a transparência e imutabilidade presentes nessa tecnologia pode ocasionar a exposição dos dados sensíveis, gerando preocupações de privacidade e confidencialidade. Ao expor esses dados, pode-se resultar em violações e impactos negativos para os pacientes. Em algumas das implementações de *Blockchain*, é possível realizar o rastreamento da identificação dos participantes, de modo que ameaça a privacidade, principalmente na saúde. A conformidade regulatória com as regulamentações de privacidade, como a GDPR na Europa e Health Insurance Portability and Accountability Act (HIPAA) nos EUA, é fundamental. O principal desafio é com relação à garantia de anonimato dos dados da saúde, propiciando a integridade e transparência da rede. Os desafios complementares englobam estabelecer o consentimento informado e a conformidade regulatória com as regulamentações de privacidade. Para que seja possível superar esses desafios, é proposta a utilização de técnicas de criptografia e identidades digitais descentralizadas para realizar a proteção da privacidade e criação dos mecanismos de consentimento atribuível.

O trabalho de Roman-Martinez et al. (2023) explora as preocupações existentes na privacidade em ambientes de *Blockchain*, com destaque aos desafios relacionados à imutabilidade e transparência dos dados. Salienta-se que, embora a imutabilidade possa garantir a integridade das informações, a mesma pode resultar na exposição inevitável dos dados confidenciais, criando desafios para a proteção da privacidade. Principalmente nos setores regulamentados como ocorre na saúde, a transparência nas *Blockchains* públicas eleva o risco do acesso não autorizado

aos dados sensíveis. Isso implica na conformidade regulatória com as regulamentações de privacidade como a GDPR na Europa e HIPAA nos EUA. Para que seja possível enfrentar os desafios existentes, são propostas soluções como criptografia e utilização das *Blockchains* privadas para gerar a restrição do acesso aos dados. Os contratos inteligentes também são sugeridos para o controle do acesso aos dados, enquanto que, as técnicas de anonimização buscam a preservação da confidencialidade nas transações. Essas abordagens visam proteger a privacidade dos dados nos ambientes de *Blockchain*, propiciando a conformidade regulatória com as regulamentações de privacidade e garantindo a integridade e confidencialidade das informações.

O trabalho de Politou et al. (2021) analisa quais os desafios da privacidade em *Blockchains* que são baseadas na transparência completa, de modo que as transações encontram-se visíveis a todos os participantes, mesmo com a utilização dos *hashes* e da criptografia. É destacado que, embora o anonimato potencial em *Blockchains* permissionadas, ainda existem os riscos que são consideráveis à privacidade dos dados. Mesmo com pseudônimos, os usuários conseguem ser relacionados e identificados. A natureza imutável e transparente da *Blockchain* realiza a exposição dos dados pessoais e permite que ocorra a recuperação das informações sensíveis. Como solução, é sugerido o uso de *Blockchains Permissioned*, na quais as políticas de controle do acesso auxiliam na preservação da privacidade e confidencialidade. Todavia, mesmo com estas medidas, o anonimato completo é visto como desafiador. A utilização de técnicas criptográficas é proposta para realizar a proteção dos dados em *Blockchain*, de modo que permite a criptografia e o processamento dos dados sem que o conteúdo seja revelado. Contudo, a implementação eficiente dessas técnicas ainda é considerada um desafio em execução, com a pesquisa sendo conduzida em busca de soluções criptográficas mais eficientes e práticas para privacidade dos dados nas *Blockchains*.

O trabalho de Haque et al. (2021) aborda as preocupações de privacidade de dados na *Blockchain*, com foco na conformidade regulatória com a GDPR. Os autores apontam que a natureza distribuída e imutável da *Blockchain* pode ser problemática para o cumprimento dos requisitos presentes na GDPR, como a exclusão e retificação dos dados pessoais. O estudo destaca o desafio relacionado ao gerenciamento de consentimento dos titulares de dados na *Blockchain*, conciliando a transparência da tecnologia com a proteção da privacidade. Para solucionar essas questões, propuseram a anonimização e pseudonimização dos dados pessoais na *Blockchain* para proteger a identidade dos usuários. Além disso, recomendam armazenar os dados sensíveis fora da cadeia (*off-chain*) e utilizar os contratos inteligentes para gerenciar o consentimento de maneira automatizada e transparente. Ademais, é sugerida a aplicação dos princípios de *Privacy by Design* no desenvolvimento das soluções de *Blockchain*, assegurando que a privacidade seja integrada desde o início. Por fim, exploram o uso de técnicas de criptografia como o ZKP, para obter a proteção da privacidade dos dados na *Blockchain*, permitindo operações com dados criptografados sem ocasionar a exposição das informações sensíveis.

O trabalho de Al-Zaben et al. (2018) discute os desafios de privacidade associados à *Blockchain*, concentrando-se na visibilidade pública de todas as transações e na ausência de uma autoridade central para controlar o acesso. Os autores destacam que isso pode comprometer a privacidade de dados pessoais identificáveis (PII), e a imutabilidade da *Blockchain* é problemática quando se trata de atualizar ou remover informações pessoais. Para superar esses desafios, os autores sugerem várias soluções. Uma delas é o armazenamento *off-chain* combinado com a verificação de *hash* na *Blockchain*, proporcionando privacidade dos dados pessoais enquanto mantém a transparência e segurança da tecnologia. Outra solução é o uso do *Multiparty Computation* (MPC) e *hyperledger* para armazenar informações sensíveis de forma segura, útil em setores como o da saúde. O estudo também propõe a separação física de PII e dados não-PII, uma abordagem usada por empresas de grande volume de dados, como as de mídia social, para manter as informações pessoais privadas e, ao mesmo tempo, preservar a transparência e segurança da *Blockchain*. Além disso, é recomendado o uso de ontologias para definição das regras de privacidade de dados, garantindo armazenamento e compartilhamento seguros e privados das informações pessoais, prática comum em empresas que realizam a análise dos dados.

O trabalho de Lee et al. (2022) investiga as questões de privacidade na *Blockchain*, focando na maneira como a transparência e imutabilidade podem expor as informações confidenciais para indivíduos não autorizados. Os autores apontam que a facilidade do acesso a *Blockchain* pode levar à revelação dos dados sensíveis, incluindo detalhes de transações financeiras e informações pessoais. A implementação da GDPR na Europa em 2018 destacou a importância de proteger os dados dos usuários, desafiando alguns dos princípios presentes na *Blockchain*, como a persistência dos dados e o direito ao esquecimento. O estudo identifica os desafios como a necessidade de manutenção da transparência e segurança na *Blockchain* enquanto se observa regulamentações de privacidade como a GDPR, e a limitação dos contratos inteligentes às funções básicas. Para superar esses desafios, os autores propuseram o uso do *framework* SPChain, um modelo seguro e privado para *Blockchain* que integra Inteligência Artificial (IA). Este modelo visa elevar a diversidade dos contratos inteligentes, além de incluir as avaliações práticas de desempenho e análises detalhadas da GDPR para assegurar a privacidade e segurança dos dados. Além disso, são apresentadas estratégias de privacidade, como criptografia e anonimização dos dados, e sugerido a utilização de modelos explicativos de IA para garantir a transparência e responsabilidade nos sistemas baseados em *Blockchain*.

O trabalho de Schaefer e Edman (2019) analisa os desafios relacionados à privacidade de dados em *Blockchain*, dando ênfase à natureza pública e imutável dessa tecnologia. Os autores indicam que, embora a imutabilidade seja considerada uma característica fundamental da *Blockchain*, ela pode gerar conflitos com regulamentações de privacidade e proteção de dados como a GDPR na Europa, principalmente quando aborda sobre o "direito ao esquecimento"e à possibilidade de apagamento dos dados pessoais. A integridade dos dados é essencial para prevenção de manipulações indevidas ou até mesmo não autorizadas, podendo afetar diretamente

a privacidade e segurança das informações. Em *Blockchain*, o cumprimento das exigências da GDPR é visto como desafiador por conta da imutabilidade presente nesta tecnologia. O estudo enfatiza sobre a necessidade de garantir com que os dados sejam acessíveis somente por partes autorizadas e quando forem circunstâncias apropriadas. Como soluções viáveis, propuseram a utilização de *Blockchains* privadas para o armazenamento de dados pessoais e sensíveis, com limitações de acesso às partes autorizadas. Além disso, recomendam a utilização da tecnologia de proveniência de dados para realizar o rastreamento da origem e do histórico dos dados, visando assegurar a integridade e transparência. É sugerida a utilização dos contratos inteligentes, como também dos mecanismos de permissão para possuir o controle de acesso às informações. Por fim, é ressaltada a importância da transparência e auditoria, sendo proposto como sugestão o registro transparente das transações e atividades numa *Blockchain* para garantir a conformidade regulatória com as regulamentações de privacidade de dados e elevar a confiança dos usuários nas empresas que fazem o gerenciamento desses dados.

O trabalho de Wylde et al. (2022) aborda os desafios existentes da privacidade em *Blockchain*, destacando que, apesar das vantagens em termos de segurança e imutabilidade, essa tecnologia enfrenta questões relevantes que estão diretamente relacionadas à privacidade dos dados. Um problema central é com relação a transparência imutável da *Blockchain*, pois torna todas as transações visíveis para os demais participantes da rede, de maneira que compromete a privacidade dos dados sensíveis devido à exposição ocorrida. A segurança das chaves privadas é considerado outro aspecto crítico, mesmo com a criptografia dos dados, a segurança está inteiramente associada à segurança dessas chaves, caso sejam comprometidas, os dados criptografados também correm o risco. A vulnerabilidade da *Blockchain* aos ataques de reorganização, que podem realizar alterações nas transações anteriores, é outro fato que preocupa, de modo que afeta a integridade e a possibilidade de manipular os dados que foram armazenados. Em relação à conformidade regulatória com as regulamentações de privacidade como a GDPR na Europa, a natureza descentralizada e transparente da *Blockchain* apresenta alguns desafios na proteção e no controle do processamento e armazenamento dos dados pessoais. Para contornar os desafios, os autores propuseram o uso de técnicas de criptografia, que permitem o processamento dos dados sem que ocorra a exposição do conteúdo original, protegendo a privacidade no decorrer das operações em dados criptografados. Além disso, é sugerida a implementação de *Blockchains* privadas, restringindo o acesso aos dados para um grupo selecionado de participantes, como uma forma de mitigar as preocupações com privacidade. Por fim, ressaltam sobre a importância das políticas de privacidade de forma clara e a conformidade regulatória com as regulamentações de privacidade como medidas essenciais para garantir a proteção dos dados em *Blockchain*.

O trabalho de Ma, Cao e Xiong (2020) explora as questões da privacidade em *Blockchain*, principalmente em contextos sensíveis como é o caso do compartilhamento de dados. Os autores indicam que a transparência e imutabilidade da *Blockchain* pode ocasionar a exposição das informações sensíveis para todos os participantes da rede. A falta de controle sobre quem realiza o acesso aos dados que foram registrados na *Blockchain* é uma preocupação relevante,

principalmente em relação à GDPR, que solicita o consentimento dos titulares e prestação de contas. A possibilidade do rastreamento de todas as transações também pode comprometer a privacidade dos usuários, gerando questões sobre a rastreabilidade em excesso. Para enfrentar os desafios citados, o estudo sugere algumas soluções. Uma delas está relacionada à divisão do *ledger* em diferentes canais, de modo que permite o compartilhamento seletivo entre os subconjuntos de usuários, além da criação de canais privados para os registros sensíveis. É sugerido também o uso de técnicas como *Multiparty Computation* (MPC) e ZKP para realizar a proteção da privacidade dos dados que foram registrados na *Blockchain*. A gestão do consentimento dos titulares através dos contratos inteligentes é outra abordagem para obtenção de conformidade regulatória com as regulamentações de privacidade.

O trabalho de Boulos, Wilson e Clauson (2018) investiga as preocupações e os desafios atrelados à privacidade de dados em *Blockchain*, focando na área da saúde. Os autores enfatizam que a natureza aberta e distribuída da *Blockchain* pode proporcionar questões relacionadas à privacidade de dados, principalmente nos dados médicos considerados sensíveis, por conta da sua transparência inerente. A segurança dos dados e a interoperabilidade entre distintos sistemas são vistas como preocupações complementares, salientando sobre a necessidade em compartilhar os dados da saúde de forma segura e com restrição de acesso para as partes autorizadas. Após a implementação das regulamentações de proteção de dados como a GDPR, emerge uma complexidade adicional em assegurar a conformidade regulatória na privacidade de dados utilizando *Blockchain* na área da saúde. Mesmo com a segurança inerente ao funcionamento da *Blockchain*, são vistos desafios como os "ataques de 51%", onde uma entidade consegue obter o controle da maioria do poder de processamento da rede, de modo que torna-se uma ameaça à segurança dos dados que foram armazenados. Para que seja possível superar esses desafios, propuseram o uso de mecanismos de segurança, junto a implementação dos protocolos de segurança avançados e também da vigilância constante contra quaisquer vulnerabilidade. Além disso, ressaltam sobre a importância de atender à conformidade regulatória na privacidade e proteção de dados, criando soluções que venham a permitir a exclusão dos dados pessoais sempre que for necessário, sem que haja o comprometimento da integridade e segurança na *Blockchain*.

O trabalho de Upadrista, Nazir e Tianfield (2023) analisa sobre as preocupações relacionadas à privacidade de dados na área da saúde em *Blockchain*, com destaque para os desafios resultantes das ameaças cibernéticas, da falta de interoperabilidade entre bancos de dados distintos e também as limitações existentes no compartilhamento colaborativo dos dados nessa área. Os autores reconhecem que, apesar da *Blockchain* oferecer os conceitos de segurança e privacidade, ainda existem barreiras que precisam ser superadas para que haja um compartilhamento mais eficiente e seguro desses dados. Os desafios abordados englobam a garantia dos princípios de confidencialidade, autenticidade, integridade e disponibilidade dos dados da saúde para os pacientes, protegendo-os das possíveis ameaças cibernéticas e visando assegurar a precisão e acessibilidade. É discutida a importância da escalabilidade em *Blockchain* e gestão das grandes

quantidades de dados na saúde, principalmente nos sistemas de monitoramento remoto. Para aprimorar a escalabilidade, é recomendada a utilização de técnicas *on-chain* e *off-chain*, como também o uso de algoritmos simétricos leves, como é o caso do *Autoregressive-Exogenous* (ARX), para garantir a confidencialidade dos dados e sustentar a autenticação por meio da assinatura digital. Propuseram o uso dos contratos inteligentes para que fosse possível analisar os dados da saúde dos pacientes e realizar a emissão de alertas em casos de leituras consideradas anormais, relatando sobre as vulnerabilidades em privacidade e segurança no monitoramento remoto. Além disso, o estudo destaca a necessidade de investigação da confiabilidade dos oráculos presentes na *Blockchain*, os quais são componentes *off-chain* vistos como críticos para que haja a integridade do sistema.

O trabalho de Ahmed et al. (2020) discute sobre os desafios atrelados à privacidade de dados em *Blockchain*, principalmente no contexto da conformidade regulatória com a GDPR. É vista como principal preocupação a imutabilidade dos dados que foram armazenados na *Blockchain*, conflitando com o direito ao esquecimento previsto na GDPR. Este direito permite que os indivíduos peçam a exclusão dos seus dados pessoais, porém a natureza imutável da *Blockchain* conflita com a remoção efetiva desses dados. É abordado também sobre a identificação do controlador dos dados, como da atribuição das responsabilidades, desafiadas pela natureza descentralizada presente na *Blockchain*, que torna complexa a determinação de quem é considerado responsável pelas transações ou operações em específico. Para tratar esses desafios, são sugeridas algumas soluções, onde uma delas é a pseudonimização dos dados, de modo que substitui as informações identificáveis por identificadores artificiais para proporcionar o anonimato dos dados, mantendo-os sob a proteção da GDPR. Outra solução que foi proposta é a criptografia dos dados para obter a proteção da privacidade dos usuários, assegurando que somente partes autorizadas possam ter acesso aos dados pessoais. A transparência, é vista como um elemento crucial da *Blockchain*, podendo ser aproveitada para garantia da conformidade regulatória com a GDPR, oferecendo clareza na coleta, processamento e compartilhamento das informações pessoais. Além disso, o rastreamento e registro de todas as transações na *Blockchain* pode auxiliar a garantir as práticas de processamento dos dados visando a conformidade regulatória com as regulamentações de privacidade de dados.

O trabalho de Rantos et al. (2019) explora as preocupações da privacidade em *Blockchain*, dando ênfase a importância da proteção dos dados pessoais num ambiente descentralizado e transparente. A tecnologia *Blockchain*, possui como características principais a transparência e a imutabilidade, podendo ocasionar desafios para a privacidade de dados, pois todas as transações são registradas de maneira permanente e mantêm-se visíveis para os demais participantes da rede. A conformidade regulatória com as regulamentações de proteção de dados, como a GDPR, que propicia restrições consideradas rigorosas sobre o processamento e a proteção das informações pessoais, representa um desafio complementar para aplicações de *Blockchain*. Existe uma necessidade em buscar a conciliação da transparência e imutabilidade da rede com a proteção da privacidade e conformidade regulatória. Para superar esses desafios, os autores propõem algumas

soluções, onde uma delas é a utilização de mecanismos de controle de acesso, permitindo definir as permissões detalhadas para o acesso aos dados, assegurando que somente as partes autorizadas possam ter acesso às informações específicas, além de proteger a privacidade dos usuários. O uso das técnicas de criptografia e anonimização dos dados também foi sugerida visando o controle de acesso das informações. Outra abordagem proposta está relacionada à implementação das infraestruturas de *Blockchains* de consórcio, que fornecem um maior controle sobre a governança e privacidade dos dados quando comparada com as redes de *Blockchains* públicas. Essas infraestruturas permitem que um grupo em específico de entidades ou organizações possam manter e validar a rede, propiciando um nível mais elevado de controle sobre a privacidade e conformidade regulatória com as regulamentações de privacidade e proteção de dados.

O trabalho de Merlec et al. (2021) aborda sobre as complexidades em privacidade de dados na *Blockchain*, com foco na conformidade regulatória junto a GDPR e também na proteção de direitos dos usuários. A natureza imutável da *Blockchain* é considerada uma das principais preocupações, por conta da dificuldade de excluir ou modificar os dados, desafiando o "direito de ser esquecido"previsto na GDPR. A transparência da *Blockchain*, possui benefícios em alguns aspectos, podendo exibir as informações confidenciais dos usuários a terceiros, ocasionando questões de privacidade dos dados. Entre os desafios atrelados à privacidade, um dos mais relevantes é com relação a busca pelo equilíbrio entre transparência e privacidade, principalmente quando se trata dos dados sensíveis. Outro desafio é garantir que os dados possam ser armazenados de maneira segura e sejam acessíveis somente para as partes autorizadas. Os autores sugeriram como uma das soluções a utilização de técnicas de criptografia e implementação de mecanismos de controle de acesso. Além disso, é essencial que os usuários possuam controle sobre os seus dados e tenham poder de decisão sobre quem pode ou não acessá-los e de qual forma serão utilizados. A utilização de criptografia para proteção dos dados armazenados na *Blockchain*, pode incluir o uso de chaves privadas para que seja possível criptografar as informações, assegurando que apenas indivíduos autorizados tenham acesso. Os contratos inteligentes também podem ser úteis na definição das condições de disponibilidade das informações pessoais, proporcionando aos indivíduos controle total sobre os seus dados e com permissão para decidir quem pode ou não ter o acesso e como esses dados devem ser utilizados.

O trabalho de Kakarlapudi e Mahmoud (2021) investiga os desafios existentes na privacidade de dados em *Blockchain*, principalmente nos contextos que envolvem os dados sensíveis. Os autores enfatizam que a imutabilidade da *Blockchain*, embora seja uma característica essencial para a segurança e integridade dos dados, simboliza um desafio relativo à privacidade de dados. Visto que os dados foram registrados na *Blockchain*, tornam-se permanentes e não podem mais ser alterados ou excluídos, o que é problema em relação à conformidade regulatória com as regulamentações de privacidade como a GDPR, sobretudo quando se trata dos dados pessoais incorretos ou obsoletos. Outro desafio está atrelado a natureza pública da *Blockchain*, que, apesar de permitir o acesso universal às informações registradas, também pode realizar a exposição dos dados sensíveis a partes não autorizadas. Isso é considerado preocupante nas áreas financeira e da

saúde, onde a confidencialidade é fundamental. A ausência de uma autoridade centralizadora para garantia da conformidade com as regulamentações de privacidade dos dados complementa mais uma camada de complexidade. Para superar esses desafios, os autores propuseram a utilização de técnicas de criptografia para proteção dos dados que foram registrados na *Blockchain*, além da criptografia de dados em repouso, que visa a manutenção dos princípios de confidencialidade e integridade dos dados num ambiente descentralizado. O uso dos contratos inteligentes é sugerido para oferecer uma camada complementar de segurança e privacidade, que permite a definição automatizada e segura das regras de acesso e compartilhamento dos dados. Além disso, é ressaltada a importância de introduzir políticas de privacidade de forma específicas para utilização da *Blockchain* em contextos com dados sensíveis para estabelecer diretrizes no armazenamento e compartilhamento dos dados, assegurando a conformidade regulatória com as regulamentações de privacidade e proteção de dados.

O trabalho de Xu et al. (2022) explora as preocupações, desafios e soluções que estão relacionadas à privacidade de dados em *Blockchain*. Os autores enfatizam que a transparência inerente da *Blockchain*, embora seja vantajosa para a integridade e confiança, é possível comprometer a privacidade dos usuários, visto que todas as transações são visíveis a todos os participantes da rede. A proteção eficiente dos dados pessoais e sensíveis na *Blockchain* é fundamental, principalmente em relação às regulamentações de privacidade como a GDPR na Europa e às recorrentes preocupações com a segurança dos usuários. O estudo também aborda sobre a dificuldade em buscar um equilíbrio entre o anonimato e a identificação, pois, por mais que a *Blockchain* forneça um certo nível de anonimato, é possível associar transações com as identidades reais, sendo considerado um desafio para a privacidade dos usuários. Para superar os desafios existentes, foram propostas soluções como o *Privacy-Preserving Truth Discovery* (PPTD), que implementa sistemas de descoberta da verdade visando preservar a privacidade, assegurando precisão e integridade dos dados que foram coletados por *crowdsourcing*. Além disso, recomendam a utilização dos contratos inteligentes para execução de forma transparente e descentralizada das regras de transação, trazendo segurança às informações. A aplicação das técnicas de criptografia e anonimização também é sugerida para a proteção da privacidade dos usuários. É destacada a importância dos sistemas de reputação baseados em *Blockchain*, que podem colaborar para confiança e privacidade na coleta de dados em *crowdsourcing*. Pois, a reputação dos participantes é fundamental para garantia da qualidade e integridade das informações que foram coletadas, gerando confiança e transparência no processo de *crowdsourcing*.

O trabalho de Reegu et al. (2023) aborda sobre a necessidade de proteger as informações sensíveis dos pacientes na área da saúde, com destaque para a importância dos princípios de confidencialidade e integridade dos dados. Os autores indicam quais os desafios enfrentados pela área da saúde na implementação da *Blockchain*, sendo estes problemas a escalabilidade, privacidade e conformidade regulatória. A transparência da tecnologia *Blockchain*, apesar de crucial, exige a proteção eficiente das informações sensíveis dos pacientes, onde a conformidade regulatória com as regulamentações como a GDPR é vista como fundamental para as organizações

da saúde que pretendem adotar a *Blockchain*. Outro desafio é com relação ao gerenciamento do consentimento dos pacientes para que haja o compartilhamento de dados, isso envolve questões éticas e legais. Para superar os desafios citados, é sugerida a implementação de sistemas de permissão para que seja possível controlar o acesso às informações, havendo limitação às partes autorizadas. Além disso, propuseram o uso de técnicas de criptografia para proteger a privacidade dos dados, assegurando que as informações sensíveis possam ser armazenadas e compartilhadas de maneira segura, e prevenir o acesso não autorizado. A adoção de padrões de segurança e conformidade é proposta para garantir a proteção dos dados dos pacientes, com a implementação de medidas de segurança que estejam alinhadas com as regulamentações em vigor. Ademais, é discutida a utilização dos contratos inteligentes e mecanismos de consenso para que seja possível automatizar e assegurar o cumprimento dos acordos que estão relacionados ao compartilhamento das informações. Esses contratos podem garantir a execução segura e transparente das transações, de modo que atendem às necessidades específicas da privacidade e segurança na área da saúde.

O trabalho de Chiarini e Compagnucci (2022) investiga os desafios da privacidade de dados na *Blockchain*, com foco nas dificuldades de conformidade com as regulamentações de proteção de dados, por conta da natureza imutável, descentralizada e transparente da tecnologia *Blockchain*. Os autores enfatizam sobre a importância do armazenamento dos dados de maneira segura e acessível somente para indivíduos autorizados, mantendo o controle dos usuários com os dados e assegurando os direitos de proteção de dados, como acesso, alteração e exclusão. Para superar os desafios existentes, foram propostas algumas soluções. É recomendado o armazenamento dos dados pessoais na *Blockchain*, utilizando técnicas de ofuscação, criptografia e agregação de dados para fazer a anonimização dos dados, enquanto que a coleta vai ocorrer *off-chain*. Outra solução é a utilização das redes privadas e permissionadas para realizar o armazenamento dos dados pessoais, fornecendo mais proteção em comparação com as redes públicas. É importante ser transparente com os usuários sobre o uso dos seus dados, garantindo que esses usuários estejam informados e possam ter controle sobre os dados. A Comissão Nacional de Informática e Liberdades (CNIL) da França e também o Observatório da União Europeia salientam a necessidade de uma abordagem colaborativa para que seja possível garantir a conformidade regulatória da *Blockchain* com regulamentações de proteção de dados como a GDPR na Europa, recomendando que a Comissão Europeia e os tribunais possam adotar uma posição clara e compartilhada sobre a conformidade regulatória da tecnologia com essas regulamentações *Blockchain*.

O trabalho de Haro-Olmo, Varela-Vaca e Álvarez-Bermejo (2020) discute a privacidade de dados na *Blockchain*, com abordagem para aspectos como a necessidade de garantia da privacidade e anonimato, em conformidade regulatória com regulamentações como a GDPR na Europa. Os autores identificam que a transparência e imutabilidade inerentes à *Blockchain* são consideradas desafiadoras para a proteção da privacidade e anonimato, por conta da natureza pública e imutável da rede pode acabar expondo as informações sensíveis. Além disso, a estrutura distribuída da *Blockchain* fornece oportunidades únicas, porém cria novos desafios de segurança,

principalmente em setores sensíveis como é o caso da saúde e Internet das Coisas (IoT). Quanto às soluções, é enfatizada a importância para desenvolver mecanismos que possam permitir aos usuários ser proprietários do seus dados, visando assegurar o acesso exclusivo a eles e impedir a vinculação entre a identidade real e os dados derivados. Foi sugerido investigar o uso da *Blockchain* para reduzir o risco de comprometimento ou manipulação dos dispositivos IoT, buscando garantir a segurança e privacidade dos dados nestes dispositivos e desenvolver soluções de segurança sofisticadas e lucrativas sendo baseadas em *Blockchain* para IoT. Ademais, enfatizam a necessidade de avanços na proteção dos dados, sugerindo uma cobertura internacional para as regulamentações, incluindo a conformidade regulatória da *Blockchain* com a GDPR.

O trabalho de Dick e Praktiknjo (2019) analisa sobre os desafios que estão relacionados à privacidade de dados na *Blockchain*, com foco nos setores regulados como é o caso do mercado de energia. Os autores apontam para a proteção de dados pessoais como uma preocupação relevante, principalmente quando se diz respeito à conformidade regulatória com a GDPR, que garante aos cidadãos europeus o direito ao esquecimento. Este direito vem sendo desafiado pela natureza imutável da *Blockchain*, que impede a alteração ou exclusão dos registros. A criptografia na *Blockchain* auxilia na pseudonimização, porém não garante a anonimização total, gerando questões sobre a efetiva proteção da identidade e privacidade dos indivíduos nas transações de energia que podem possuir dados sensíveis. Outro desafio destacado é a acessibilidade a níveis distintos de dados na *Blockchain* e identificação de quem pode fazer a visualização das informações específicas, o que pode complicar após adicionar mais dados a uma transação. Esses desafios visam encontrar um equilíbrio entre a transparência e privacidade, pois existe a dificuldade na exclusão das informações pessoais, falta clareza sobre a responsabilidade pelos erros nos registros imutáveis, e necessidade de assegurar estruturas apropriadas para que as empresas ofereçam os seus serviços. Para superar os desafios citados, é proposta a implementação de técnicas de criptografia para processamento de dados sem que haja a exposição e criação das camadas de privacidade que tornem somente partes selecionadas do livro-razão acessíveis aos usuários permitidos. Além disso, enfatizam a importância de regulamentações claras e específicas para a *Blockchain*, buscando facilitar a conformidade regulatória nas empresas com as regulamentações de dados vigentes e oferecendo aos usuários um maior controle sobre as suas informações pessoais.

O trabalho de Kassem et al. (2019) investiga as preocupações com a privacidade de dados na *Blockchain*, com foco na proteção de dados pessoais que foram armazenados numa cadeia *on-chain* e também na preservação da privacidade dos usuários. Os autores apontam que, embora a *Blockchain* ofereça segurança e imutabilidade, a estrutura distribuída e transparente dessa tecnologia representa um desafio relevante para a privacidade dos dados. As transações e informações que são registradas tornam-se visíveis para todos os participantes da rede, ocasionando preocupações em relação a dados pessoais sensíveis. Além disso, a dificuldade de associação das atividades na rede com as identidades reais, por conta do caráter pseudônimo das transações, pode gerar o comprometimento da privacidade dos usuários. Para superar os

desafios citados, é discutida a utilização de técnicas de criptografia para a proteção dos dados na *Blockchain*, de modo que permite que somente partes autorizadas acessem as informações sensíveis. Dessa forma pode ser incluído o uso da criptografia homomórfica, que permite as operações em dados criptografados sem que haja a necessidade de descriptografá-los. De forma adicional, a implementação de mecanismos de controle de acesso e gerenciamento de identidade busca a restrição do acesso aos dados específicos na rede, mitigando as preocupações relacionadas à transparência e a identificação dos usuários. Essas estratégias visam o equilíbrio da tecnologia *Blockchain* com a conformidade regulatória junto às regulamentações de proteção de dados pessoais, dando importância à confidencialidade e ao controle dos usuários sobre as suas informações.

O trabalho de Bai et al. (2022) explora as preocupações com a privacidade de dados na *Blockchain*, salientando sobre a necessidade da conformidade regulatória com as regulamentações de proteção de dados como a GDPR e a importância de garantir a confidencialidade e privacidade dos dados pessoais. Os autores dão ênfase à relevância de permissão aos proprietários de dados para controlar as suas informações e assegurar os conceitos de visibilidade, transparência e rastreabilidade dos dados que foram armazenados e compartilhados na *Blockchain*. Os desafios incluem proteger as informações sensíveis, como é o caso dos dados pessoais da saúde (PHI) e das informações de identificação pessoal (PII), contra o acesso não autorizado, e a necessidade de armazenamento e compartilhamento desses dados de maneira segura, visando manter a conformidade regulatória com as regulamentações de proteção de dados. Para superar esses desafios, foram propostas soluções como o armazenamento *off-chain* dos dados sensíveis, com sistemas como o *InterPlanetary File System* (IPFS), buscando aprimorar a privacidade e oferecer o controle de exclusão aos usuários. Dessa forma permite armazenar os dados de maneira segura e privada, enquanto que os metadados e as transações relacionadas estão sendo registrados na *Blockchain* para que obtenha a rastreabilidade. Outra solução é a utilização dos contratos inteligentes para o compartilhamento de dados criptografados de forma segura, de modo que seja permitido o acesso somente aos participantes autorizados. Além disso, a implementação do *Privacy by Design* possui importante destaque, incorporando os princípios de privacidade desde o início de design do sistema. Essa abordagem está incluindo o cumprimento do direito ao esquecimento e garantindo a exclusão dos dados pessoais depois do cumprimento de propósito da coleta.

O trabalho de Alves et al. (2020) analisa sobre a importância crítica da privacidade e proteção de dados no decorrer das pandemias como foi o caso da *COVID-19*, onde a coleta e uso dos dados pessoais e sensíveis são cruciais para controlar e reduzir os riscos de infecções e mortes. Embora haja a necessidade desses dados, são destacados os desafios relacionados à privacidade e proteção de dados envolvidos, com ênfase para a importância de processá-los e posteriormente armazená-los de forma segura e transparente, em conformidade regulatória com as regulamentações de proteção de dados. Os autores também apontam a necessidade de oferecer aos indivíduos o controle sobre o compartilhamento e uso das suas informações. Para

superar os desafios visto anteriormente, foi proposta a implementação de uma segunda camada de governança de dados nos sistemas de *Blockchain* permissionadas, através dos princípios do *Framework* Analítico de Governança (GAF), onde essa camada permite aos usuários a verificação dos dados que foram processados de acordo com as políticas de privacidade, responsabilizando os envolvidos no processamento. O estudo também destaca que a tecnologia *Blockchain* deve facilitar a reconstrução das concessões dos sujeitos de dados no decorrer do tempo.

O trabalho de Fekete e Kiss (2023) investiga as preocupações e os desafios relacionados à privacidade de dados nos sistemas educacionais baseados em *Blockchain*, dando destaque a falta do anonimato completo como uma questão chave. Por conta da natureza pública e transparente da *Blockchain*, o histórico completo dos registros e das transações pode ser rastreado por qualquer indivíduo, de modo que representa uma ameaça à privacidade dos usuários. A imutabilidade dos dados presente na *Blockchain* também impede a proteção efetiva dos dados na cadeia *on-chain*, devido às limitações nas operações do usuário e à falta de proteção de privacidade implementada. Além disso, a conformidade com as regulamentações de privacidade de dados, como a GDPR, é vista como desafiadora. Para superar esses desafios, foram propostas soluções específicas, onde uma delas envolve o armazenamento em *off-chain* dos dados pessoais que necessitam de privacidade, buscando manter somente o *hash* correspondente *on-chain*. Dessa forma permite que sejam cumpridos os requisitos de privacidade visando a manutenção da integridade das informações. Outra abordagem é com relação à implementação das soluções de escalonamento na *Blockchain*, elevando a capacidade da rede para atender de maneira eficiente um grande volume de acessos pelos usuários, o que é considerado como fundamental para aplicativos com dados sensíveis, como é o caso dos sistemas educacionais superiores que são baseados em *Blockchain*.

3.7 Discussão dos Principais Trabalhos Selecionados

Os trabalhos desta subseção foram escolhidos de acordo com os diferentes cenários que foram apresentados anteriormente, com o intuito de obter a conformidade regulatória e trazer como solução para o anonimato de forma específica, as técnicas de ZKP ou Ring Signatures, técnicas essas que serão abordadas no capítulo 4.

Os trabalhos de Han e Park (2022) e Haque et al. (2021) abordam a dificuldade existente na conciliação entre a imutabilidade e transparência presentes na *Blockchain* em relação as regulamentações de proteção de dados. Ambos propõem soluções que incluem a utilização de mecanismos de controle de acesso, técnicas de criptografia e anonimização dos dados para que seja possível garantir a privacidade e segurança dos dados em ambientes que são baseados na tecnologia *Blockchain*. Ademais, é proposto por eles o uso de contratos inteligentes para realizar o gerenciamento do consentimento de maneira automatizada e transparente. Han e Park (2022) propuseram como uma alternativa a utilização do *Zero-Knowledge Proof* (ZKP), visando garantir inacessibilidade aos dados subjacentes, oferecendo apenas respostas binárias, como *true* ou *false*.

Enquanto Haque et al. (2021) sugerem que o ZKP seja utilizado para tornar os dados anônimos. Ambos enfatizam sobre o uso do ZKP como uma forma de obter conformidade regulatória com a GDPR.

Os trabalhos de Ma, Cao e Xiong (2020) e Wylde et al. (2022) investigam sobre a compatibilidade da *Blockchain* com a General Data Protection Regulation (GDPR) e analisam a eficácia do registro e consulta para auditoria de acesso aos conjuntos de dados entre os sistemas baseados na tecnologia *Blockchain*. É enfatizada a importância da privacidade e segurança dos dados, e são propostas soluções para a garantia da conformidade regulatória com as regulamentações de proteção de dados, além de abordarem sobre a necessidade da busca por soluções eficazes para o gerenciamento do consentimento em ambientes que são baseados em *Blockchain*. Os autores propuseram como uma dessas soluções a utilização do *Zero-Knowledge Proof* (ZKP) para realizar a confirmação sobre determinadas ações ou consultas feitas por um usuário, sem revelar quais foram de fato as ações ou consultas feitas por aquele usuário, dessa forma mantendo o anonimato. Enquanto Wylde et al. (2022) afirmam que o ZKP podem oferecer validade, anonimato e transparência nas operações. Ambos enfatizam que a utilização do ZKP é vista como uma forma de possibilitar a conformidade regulatória com a GDPR.

O trabalho de Politou et al. (2021) analisa quais são os desafios da privacidade em *Blockchains* baseadas na transparência por completo, de modo que as transações encontram-se visíveis para todos os participantes, mesmo com a utilização dos *hashes* e da criptografia. É destacado pelo autor que, apesar do anonimato potencial nas *Blockchains* permissionadas, ainda existem riscos consideráveis à privacidade dos dados. Politou et al. (2021) abordam que o ZKP é visto como uma solução que permite a realização de cálculos específicos que são capazes de serem feitos sem revelar as entradas e saídas desses cálculos.

Os trabalhos de Ahmed et al. (2020) e Xu et al. (2022) discutem sobre os desafios existentes que estão diretamente relacionados as questões de privacidade de dados na tecnologia *Blockchain*. Ahmed et al. (2020) propuseram que a utilização de técnicas de privacidade como *Zero-Knowledge Proof* (ZKP) e Ring Signatures são capazes de anonimizar as chaves públicas para obter conformidade regulatória com a General Data Protection Regulation (GDPR). Enquanto Xu et al. (2022) afirmam que o ZKP suporta os serviços de agregação de dados, podendo garantir de forma completa a exatidão da agregação de dados, privacidade diferencial, confidencialidade e robustez.

3.8 Resposta às Questões de Pesquisa

Esta subseção apresenta os resultados obtidos a partir dos artigos selecionados e das questões de pesquisa.

QP1) Quais as principais preocupações discutidas a respeito da privacidade de dados em *Blockchain*?

Os artigos selecionados indicam que as principais preocupações em relação à privacidade de dados na *Blockchain* são a transparência e a imutabilidade. Como a *Blockchain* é uma tecnologia que proporciona a criação de registros transparentes e imutáveis, existem preocupações relacionadas à exposição e exclusão das informações sensíveis, visando a conformidade regulatória prevista pela LGPD ou GDPR. O direito ao esquecimento poderia entrar como uma dessas preocupações, principalmente no Brasil, pois implica na proteção da privacidade das informações.

QP2) Quais os desafios enfrentados em relação à privacidade de dados em *Blockchain*?

Os artigos selecionados apontam que os desafios enfrentados em relação à privacidade de dados na *Blockchain* estão ligados diretamente à transparência e à imutabilidade. Por conta da dificuldade de encontrar soluções viáveis que possam de fato corresponder com a conformidade regulatória estabelecida pela LGPD ou GDPR.

QP3) Quais as soluções propostas para lidar com as questões de privacidade de dados em *Blockchain*?

Os artigos selecionados apresentam algumas propostas de solução para lidar com as questões de privacidade de dados na *Blockchain* em conformidade regulatória com a LGPD ou GDPR. Sendo as principais delas a utilização de técnicas de criptografia e pseudonimização, uso de mecanismos de controle de acesso e implementação de contratos inteligentes.

Para obter conformidade com a LGPD ou GDPR, a criptografia e a pseudonimização precisariam ser utilizadas para proteger os dados pessoais contra o acesso não autorizado e para garantir que os dados consigam ser acessados apenas pelos indivíduos ou sistemas que detém permissão. Por exemplo, antes de realizar o armazenamento dos dados pessoais na *Blockchain*, uma organização pode pseudonimizar esses dados, de modo que substitui os identificadores diretos por pseudônimos. Além disso, a criptografia pode ser utilizada para proteger os dados no decorrer do processo de transmissão e o armazenamento, assegurando que mesmo que os dados possam ser acessados, os dados não podem ser interpretados sem que haja a chave de descriptografia correspondente.

As organizações precisam realizar as avaliações periódicas de acesso e ajustes das permissões conforme seja necessário para garantir que o acesso aos dados pessoais seja considerado restrito aos indivíduos necessários para a finalidade que foi definida. A implementação dos registros de acesso e auditoria através do uso dos contratos inteligentes pode auxiliar a demonstrar conformidade com as regulamentações de proteção de dados.

O controle de acesso necessita ser implementado estrategicamente para que seja possível garantir que apenas usuários autorizados consigam acessar ou processar os dados pessoais, conforme necessário. Isso está alinhado ao princípio da minimização dos dados e limitação de finalidade da LGPD ou GDPR. Os mecanismos de controle de acesso em *Blockchain* podem ser configurados no decorrer da fase de design da solução com a utilização dos contratos inteligentes para definir e executar as políticas de acesso sendo baseadas em funções ou atributos.

Os contratos inteligentes podem ser programados para automatizar o cumprimento das políticas de privacidade, como é o caso da gestão de consentimentos, dos direitos de acesso a dados (como acesso, retificação, exclusão), e da execução dos processos de verificação de identidade. Esses contratos devem facilitar a transparência e a automação do processamento de dados pessoais, assegurando que as ações possam ser executadas apenas após condições que foram pré-determinadas serem de fato atendidas, o que é visto como uma exigência do princípio da legalidade sob a LGPD ou GDPR.

Para aplicar contratos inteligentes na gestão de consentimento, por exemplo, uma organização pode desenvolver um contrato inteligente que registre o consentimento do usuário de forma verificável e permita que o usuário retire seu consentimento a qualquer momento. Isso não só proporciona uma base legal clara para o processamento de dados pessoais, mas também facilita a gestão de consentimentos em grande escala.

QP4) Qual o método de pesquisa utilizado?

Os artigos selecionados para esta pesquisa adotaram diferentes métodos, incluindo análise documental, survey, experimento e estudo de caso.

Na Tabela 6 é possível observar cada uma das respostas dos artigos selecionados as questões de pesquisas que foram propostas nesse estudo.

Tabela 6 – Questões de Pesquisa

Autores	**QP1**	**QP2**	**QP3**	**QP4**
Han e Park (2022)	Imutabilidade e transparência	Imutabilidade e transparência	Técnicas de criptografia e pseudonimização, mecanismos de anonimização e contratos inteligentes	Análise documental
Arbabi et al. (2023)	Imutabilidade e transparência	Imutabilidade e transparência	Técnicas de criptografia, identidades digitais descentralizadas e mecanismos de consentimento	Survey
Roman-Martinez et al. (2023)	Imutabilidade e transparência	Imutabilidade e transparência	Técnicas de criptografia e anonimização, mecanismos de consentimento e contratos inteligentes	Experimento
Politou et al. (2021)	Imutabilidade e transparência	Imutabilidade e transparência	Técnicas de criptografia e mecanismos de consentimento	Análise documental
Haque et al. (2021)	Imutabilidade e transparência	Imutabilidade e transparência	Mecanismos de anonimização e pseudonimização, *off-chain*, contratos inteligentes e mecanismos de consentimento	Análise documental
Al-Zaben et al. (2018)	Imutabilidade e transparência	Imutabilidade e transparência	*Off-chain*, *Multiparty Computation* e mecanismos de consentimento	Experimento
Lee et al. (2022)	Imutabilidade e transparência	Imutabilidade e transparência	*Framework* SPChain e modelos de explicação de Inteligência Artificial	Experimento
Schaefer e Edman (2019)	Imutabilidade e transparência	Imutabilidade e transparência	Proveniência de dados e contratos inteligentes	Estudo de caso
Wylde et al. (2022)	Transparência e chaves privadas	Transparência e vulnerabilidade a ataques de reorganização	Técnicas de criptografia e políticas de privacidade claras	Análise documental
Ma, Cao e Xiong (2020)	Imutabilidade e transparência	Transparência e falta de mecanismos de controle de acesso	Divisão do *ledger*, técnicas de criptografia e contratos inteligentes	Survey

Autores	**QP1**	**QP2**	**QP3**	**QP4**
Boulos, Wilson e Clauson (2018)	Transparência e interoperabilidade	Transparência e ataques de 51%	Mecanismos de privacidade e segurança	Estudo de caso
Upadrista, Nazir e Tianfield (2023)	Vulnerabilidade, interoperabilidade e compartilhamento colaborativo	Confidencialidade, autenticidade e integridade	Técnicas on-chain e off-chain, algoritmos simétricos e contratos inteligentes	Análise documental
Ahmed et al. (2020)	Imutabilidade	Imutabilidade e descentralização	Técnicas de criptografia e pseudonimização	Análise documental
Rantos et al. (2019)	Descentralização e transparência	Descentralização e transparência	Mecanismos de controle de acesso, técnicas de criptografia e anonimização	Experimento
Merlec et al. (2021)	Imutabilidade e transparência	Transparência e Armazenamento	Técnicas de criptografia e contratos inteligentes	Experimento
Kakarlapudi e Mahmoud (2021)	Imutabilidade, transparência e descentralização	Imutabilidade, transparência e descentralização	Técnicas de criptografia, contratos inteligentes e políticas de privacidade	Análise documental
Xu et al. (2022)	Transparência e anonimato	Transparência e anonimato	*Privacidade-Preservando Truth Discovery*, contratos inteligentes e técnicas de criptografia	Análise documental
Reegu et al. (2023)	Confidencialidade e integridade	Escalabilidade	Mecanismos de controle de acesso, técnicas de criptografia e adoção de padrões de segurança	Experimento
Chiarini e Compagnucci (2022)	Imutabilidade, transparência e descentralização	Armazenamento e controle de acesso	Técnicas de criptografia e redes privadas e permissionadas	Análise documental
Haro-Olmo, Varela-Vaca e Álvarez-Bermejo (2020)	Imutabilidade e transparência	Imutabilidade e transparência	Mecanismos de privacidade e anonimização	Análise documental
Dick e Praktiknjo (2019)	Imutabilidade, segurança e acessibilidade	Imutabilidade transparência	Técnicas de criptografia e regulamentações claras	Survey
Kassem et al. (2019)	Imutabilidade e transparência	Imutabilidade e transparência	Técnicas de criptografia e mecanismos de controle de acesso	Experimento

Autores	**QP1**	**QP2**	**QP3**	**QP4**
Bai et al. (2022)	Visibilidade, transparência e rastreabilidade	Segurança, escalabilidade, armazenamento e desempenho	*Off-chain*, contratos inteligentes e *Privacy by Design*	Experimento
Alves et al. (2020)	Segurança	Segurança e transparência	*Framework Analítico de Governança*	Experimento
Fekete e Kiss (2023)	Imutabilidade e transparência	Imutabilidade e transparência	*Off-chain* e implementação de escalonamento	Análise documental

Fonte: Elaborado pelo Autor

3.9 Considerações Finais do Mapeamento Sistemático

Em relação às questões de pesquisa, os resultados que foram obtidos indicam que a transparência e imutabilidade são vistas como as principais preocupações e desafios existentes em relação à privacidade de dados na *Blockchain*. A partir disso, a utilização de técnicas de criptografia, o uso de mecanismos de consenso, a implementação de políticas de privacidade, a adoção de padrões de segurança e entre outras soluções, são consideradas estratégias importantes para que seja possível garantir a conformidade regulatória em *Blockchain* com as regulamentações de proteção de dados.

Na *Blockchain*, as técnicas de criptografia são usadas para garantir a confidencialidade e a integridade dos dados. Onde, a criptografia de chave pública, por exemplo, permite que os dados sejam criptografados através da chave pública de um receptor, de maneira que somente a chave privada correspondente consiga descriptografar esses dados.

Com relação aos mecanismos como PoW e PoS, os mesmos são fundamentais para manutenção da integridade e a veracidade das informações na *Blockchain*. Esses mecanismos asseguram que todas as transações que foram adicionadas ao bloco possam ser verificadas e aceitas pela maioria dos nós participantes, de modo que auxilia na prevenção de fraudes e garantia da transparência.

A implementação de políticas de privacidade rigorosas é essencial para conformidade regulatória em *Blockchains* que armazenam dados pessoais. Pois, essas políticas devem definir de maneira clara como os dados são coletados, utilizados e protegidos, além de obter conformidade com as regulamentações de proteção de dados, como a LGPD e GDPR, onde ambas impõem regras específicas sobre o processamento de dados pessoais.

A Adoção de padrões de segurança reconhecidos nacionalmente, como NBR ISO/IEC 27001, auxilia a estabelecer um modelo de *framework* de segurança que visa a proteção dos dados contra ameaças e vulnerabilidades. Esses padrões citados incluem medidas de segurança física, administrativa e técnica.

Por fim, o uso de tecnologias como os contratos inteligentes podem ser utilizados para aumentar a segurança e a conformidade regulatória. Pois, os contratos inteligentes permitem que haja a execução automática dos termos contratuais.

4

Estudo Comparativo

Este capítulo apresenta um estudo comparativo baseado na literatura acadêmica entre 2 (duas) das principais técnicas de privacidade de dados em *Blockchain*, além da conformidade regulatória dessas técnicas com a LGPD e GDPR.

4.1 *Zero-Knowledge Proof (ZKP)*

O conceito de ZKP está atrelado diretamente a um método de privacidade de dados onde uma parte (o provador) pode provar para outra parte (o verificador) que sabe um determinado valor "x", sem revelar qualquer tipo de informação relevante sobre esse valor (GOLDWASSER; MICALI; RACKOFF, 1989). É utilizado de forma ampla em criptomoedas como *Zerocoin* (atual *Zcash*) para garantir a privacidade, e também nos sistemas de identidade digital para realizar a autenticação sem revelar as informações de maneira excessiva (BEN-SASSON et al., 2014).

Quando comparado aos métodos tradicionais de autenticação, o ZKP fornece um maior nível de privacidade e segurança, pois não revela as informações secretas no decorrer do processo de verificação. Desse modo, reduz significativamente o risco contra os ataques de *phishing* ou engenharia social (GOLDWASSER; MICALI; RACKOFF, 1989).

As soluções que são baseadas nesta forma de autenticação podem ser consideradas altamente escaláveis e eficientes, de modo que se tornam adequadas para sistemas com maior nível de complexidade, como as redes de *Blockchain* (públicas, privadas, híbridas e de consórcio), tornando-se fundamentais para a garantia da viabilidade dos sistemas descentralizados em grande escala (BEN-SASSON et al., 2013).

O ZKP é visto como aplicável numa diversidade de cenários, desde a verificação de identidade até mesmo a realização de transações financeiras de forma segura, fornecendo um mecanismo considerado flexível e robusto para que seja possível garantir a integridade das operações (CAMENISCH; STADLER, 1997).

4.1.1 Funcionamento do *Zero-Knowledge Proof* (ZKP)

O funcionamento básico do ZKP possui 2 (duas) partes principais: o provador (à esquerda) e o verificador (à direita). Este utiliza um padrão onde o provador tenta convencer o verificador de que sabe uma determinada informação considerada confidencial, como uma chave secreta (*secret key*), sem revelar o conteúdo presente naquela informação (GOLDWASSER; MICALI; RACKOFF, 1989).

O ZKP é estruturado em torno de 3 (três) propriedades fundamentais: completude, onde se o provador é considerado honesto, o verificador será convencido da verdade daquela afirmação; solidez, onde um provador considerado desonesto não consegue convencer o verificador de uma afirmação falsa possuindo uma probabilidade relevante; e o conhecimento zero, de forma que o verificador não consegue apreender nada além do fato daquela afirmação ser verdadeira (GOLDREICH, 2004).

Figura 5 – Funcionamento do ZKP

Fonte: Elaborado pelo Autor

A Figura 5 apresenta uma sequência de passos de maneira ilustrativa que pode ser descrita da seguinte forma:

Autenticação: O provador realiza a comunicação inicial com o verificador, manifestando a intenção de provar o conhecimento de uma informação considerada secreta.

Troca de Provas: Uma série de interações acontece, onde o provador encaminha "provas"ao verificador. Estas provas são produzidas de modo que elas possam ser verificadas sem que a informação considerada secreta tenha sido revelada.

Verificação: O verificador realiza uma análise das "provas". Caso elas cumpram com os critérios que foram estabelecidos, que foram informados anteriormente, ele deve confirmar que o provador obtém o conhecimento da informação considerada secreta. No entanto, não é necessário que o verificador possua qualquer tipo de conhecimento sobre aquela informação de fato.

Conclusão: Se todas as provas apresentadas forem consideradas satisfatórias, o verificador faz aceitação da "prova"do provedor. Este processo pode garantir que a informação secreta possa permanecer segura e que o verificador não consiga realizar a replicação do processo ou então examinar a informação secreta.

Figura 6 – Exemplo Prático do ZKP em *Python*

```python
import random
import hashlib

def hash_string(input_string):
    # A função utiliza o SHA-256 para criação de um hash da string de entrada
    return hashlib.sha256(input_string.encode()).hexdigest()

def provador(nome_secreto):
    # A função permite a representação da informação secreta vinda do provador
    return hash_string(nome_secreto)

def gerar_prova(nome_secreto):
    # O provador vai gerar uma prova sem revelar a informação secreta
    multiplicador_aleatorio = random.randint(1, 100)
    # O "comprometimento" é feito com o hash do nome ao invés de revelar o nome em si
    comprometimento = hash_string(nome_secreto + str(multiplicador_aleatorio))
    return comprometimento, multiplicador_aleatorio

def verificar_prova(comprometimento, multiplicador_aleatorio, hash_publico):
    # O verificador confirma a prova, sem conhecer o nome secreto
    # Depois gera o hash novamente com o multiplicador e compara com o comprometimento
    return comprometimento == hash_string(nome_secreto + str(multiplicador_aleatorio))

nome_secreto = 'Tácito'  # O nome secreto que o provador conhece
hash_publico = provador(nome_secreto)  # O provador compartilha publicamente o hash do nome secreto

# O provador gera a prova
comprometimento, multiplicador_aleatorio = gerar_prova(nome_secreto)

# O verificador verifica a prova
prova_valida = verificar_prova(comprometimento, multiplicador_aleatorio, hash_publico)
# O verificador realiza a aceitação da prova
print(f"A prova é válida: {prova_valida}")
```

Fonte: Adaptado pelo Autor

A Figura 6 representa um exemplo prático em *Python* da utilização do ZKP realizando os passos apresentados anteriormente, desde a fase de autenticação até a conclusão, sem que o provador revele ao verificador a informação secreta.

Inicialmente é feita a importação dos módulos ***random*** (gerar números aleatórios) e ***hashlib*** (criptografar informações utilizando *hash*). Posteriormente, são implementadas as seguintes funções:

hash_string(input_string): Para receber uma *string* como entrada e retornar um valor de *hash SHA-256* da *string* de entrada);

provador(nome_secreto): Para receber uma informação secreta e retornar a representação *hash* daquela informação, sem que possa revelar a própria informação;

gerar_prova(nome_secreto): É o provador, vai gerar uma prova sem revelar qual a informação secreta obtida. Para que isso aconteça, é escolhido um número aleatório entre 1 e 100 (***multiplicador_aleatorio***). Em sequência, é concatenado o nome secreto junto ao número aleatório e gerado um *hash* do valor concatenado (***comprometimento***).

verificar_prova(comprometimento, multiplicador_aleatorio, hash_publico): É o verificador que tenta comprovar que sabe o nome secreto sem conhecê-lo. Para isso, um novo *hash* é obtido utilizando o (***hash_publico*** e o (***multiplicador_aleatorio***). Esse novo *hash* vai ser comparado ao comprometimento. Caso os *hashes* forem correspondentes, a prova é válida.

4.1.2 Protocolos do *Zero-Knowledge Proof* (ZKP)

Os protocolos de ZKP possuem uma vasta utilidade em diversas aplicações, principalmente em cenários onde a privacidade e segurança são considerados fundamentais. Por exemplo, nos sistemas de votação eletrônica, para garantir que o voto seja computado devidamente sem revelar a escolha de determinado eleitor (ADIDA, 2008). Além disso, no cenário de *Blockchain* e criptomoedas, esses protocolos possibilitam a realização das transações de maneira anônima, onde os protocolos de prova de conhecimento zero são considerados fundamentais para que haja garantia da privacidade das transações ocorridas (BEN-SASSON et al., 2014).

Dentro do ZKP existem 4 (quatro) tipos de protocolos, sendo estes classificados como interativos ou não interativos, apresentados na Tabela 7.

Tabela 7 – Tipos de Protocolos do ZKP

Argumentos de Conhecimento Não Interativos Sucintos (*zkSNARKs*)	Apresenta como principal característica serem sucintos, ou seja, as provas são relativamente pequenas e rápidas na verificação. Esses argumentos são amplamente utilizados em aplicações de *Blockchain* para manutenção da privacidade e eficiência.
Argumentos de Conhecimento Transparente Escalonável (*zkSTARKs*)	São uma alternativa aos *SNARKs*, pois possuem uma configuração altamente confiável, sendo considerados resistentes aos ataques de computadores quânticos. Esses argumentos são muito úteis em contextos onde os conceitos de transparência e escalabilidade são críticos, além de possuírem destaque na aplicabilidade e eficiência.
Delegação Polinomial Verificável (*zkVPD*)	É considerada uma técnica em ZKP na qual um provador vai delegar o cálculo de um polinômio para que um verificador o realize de maneira eficiente e segura.
Argumentos Não Interativos Sucintos (*zkSNARGs*)	São considerados uma forma de ZKP que permitem a geração de provas curtas e verificáveis sem interação. De modo que são cruciais em vários sistemas criptográficos na garantia da segurança e eficiência.

Fonte: Elaborado pelo Autor

O protocolo mais utilizado é o *ZkSNARKs*, por conta da sua capacidade de executar provas bastante compactas. Dessa maneira, são considerados argumentos ideais para serem adotados em sistemas que possuem o armazenamento e a largura de banda limitados, como acontece com várias *Blockchains*. Eles possibilitam que as provas de transações sejam realizadas de forma rápida e eficiente, sendo um atributo crítico para obter a escalabilidade nas criptomoedas (BEN-SASSON et al., 2013).

4.2 *Ring Signatures*

O conceito de *Ring Signatures* está relacionado a um tipo de assinatura digital que permite a um membro de um grupo realizar a assinatura de mensagens de *e-mails*, documentos e entre outras coisas, de forma anônima. Cada assinatura é feita de tal forma que torna impossível determinar qual foi o membro responsável pela assinatura. Esta propriedade as torna consideradas úteis para diversas aplicações (criptomoedas, votações eletrônicas e entre outras) que requerem o anonimato e privacidade (RIVEST; SHAMIR; TAUMAN, 2001).

Elas são amplamente utilizadas nas criptomoedas, como é o caso da *Monero*, proporcionando as transações de forma anônima. Desse modo, pode garantir o anonimato das mensagens e as transações digitais, como também ocorre em determinados sistemas de votação eletrônica (KUMAR et al., 2017).

É permitido também que um membro do grupo faça uma assinatura sem que haja a necessidade de coordenação ou cooperação dos demais membros do grupo. Isso significa dizer que uma assinatura pode ser realizada de forma independente, sendo assim, considerada uma grande vantagem em termos de praticidade e eficiência operacional (LIU; WEI; WONG, 2004).

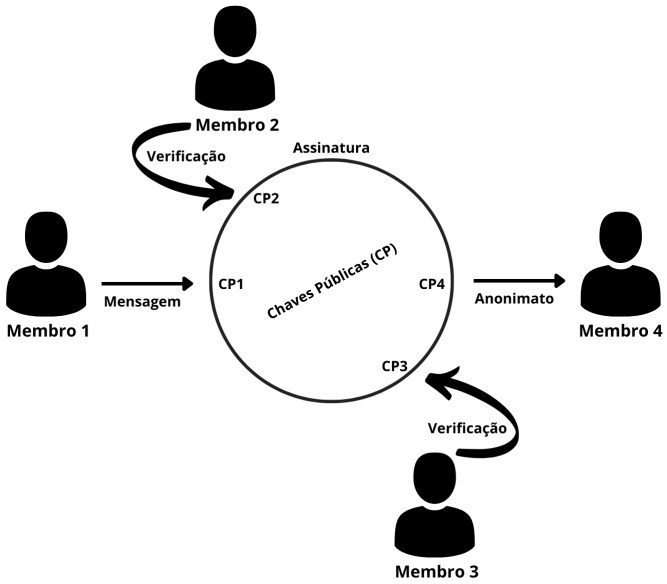
Uma das desvantagens das *Ring Signatures* está interligada diretamente ao anonimato, pelo fato de que, as *Ring Signatures* podem obter limitações de tamanho e natureza dentro de um grupo e não serem consideradas tão abrangentes em termos de privacidade quando comparadas ao ZKP. Ademais, existem limitações relacionadas a escalabilidade e gestão de grupo, principalmente tratando-se de grupos grandes ou dinâmicos (DINGLEDINE; MATHEWSON; SYVERSON, 2004).

4.2.1 Funcionamento das *Ring Signatures*

O funcionamento das *Ring Signatures* é baseado na combinação de chaves públicas de vários participantes para criar uma única assinatura. O processo começa com um usuário (signatário) que deseja assinar uma mensagem de forma anônima. Este usuário escolhe arbitrariamente um conjunto de chaves públicas, incluindo a sua chave privada, formando um "anel"de participantes. A estrutura é projetada de tal forma que a assinatura é vinculada a este grupo, mas não revela qual membro específico do grupo a gerou (RIVEST; SHAMIR; TAUMAN, 2001).

Na medida em que um membro do grupo fornece uma assinatura, ele faz a combinação da sua chave privada com as chaves públicas dos demais membros. Dessa forma, o resultado é resumido em uma assinatura que faz a validação da mensagem, mas que não pode revelar qual o membro do grupo que assinou. Essa abordagem visa garantir o anonimato, e simultaneamente manter a integridade e autenticidade da mensagem (LIU; WEI; WONG, 2004).

Figura 7 – Funcionamento das *Ring Signatures*



Fonte: Elaborado pelo Autor

A Figura 7 representa uma sequência de etapas de forma ilustrativa que podem ser descritas da seguinte maneira:

Chave Pública: Cada um dos membros do grupo detém uma chave pública, a qual é conhecida por todos. As chaves públicas vão de CP1 até CP4.

Assinatura: Caso um dos membros do grupo queira enviar uma mensagem, o mesmo produz uma assinatura em anel com a sua chave privada e as chaves públicas dos demais membros do grupo. Isso é visto no círculo que envolve as chaves públicas, apontando com a mensagem.

Anonimato: A assinatura vai garantir ao destinatário saber que a mensagem foi assinada por um dos membros do grupo, mas não pode permitir a identificação de qual foi o membro. Sendo útil em situações onde o anonimato do remetente é considerado necessário ou desejado.

Verificação: Qualquer membro pode fazer a verificação de que aquela assinatura é válida, mas não pode acusar quem dos possíveis membros do grupo a criou. Dessa forma, implica dizer que a mensagem foi autenticada e a identidade do membro permanece anônima.

Comunicação: O funcionamento sugere que a mensagem está sendo enviada de um membro para outro, mas que poderia ser aplicada igualmente para a comunicação dos demais membros entre si, apresentando o conceito de flexibilidade presente nas assinaturas em anel nos diversos tipos de comunicação.

Figura 8 – Exemplo Prático das *Ring Signatures* em *Python*

```python
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.backends import default_backend
import os

# A função gera chaves para simular os usuários
def gerar_chaves():
    return rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048,
        backend=default_backend()
    )

# A função simula uma assinatura em anel
def assinatura_em_anel(mensagem, chaves_privadas, indice_publico):
    digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
    digest.update(mensagem.encode())
    hash_mensagem = digest.finalize()

    # Simulação da assinatura do membro do anel
    assinatura_falsa = os.urandom(256)  # Não é uma assinatura real, apenas para simulação
    assinaturas = [None] * len(chaves_privadas)
    assinaturas[indice_publico] = chaves_privadas[indice_publico].sign(
        hash_mensagem,
        padding.PSS(
            mgf=padding.MGF1(hashes.SHA256()),
            salt_length=padding.PSS.MAX_LENGTH
        ),
        hashes.SHA256()
    )

    # As demais assinaturas são consideradas falsas
    for i in range(len(chaves_privadas)):
        if i != indice_publico:
            assinaturas[i] = assinatura_falsa

    return assinaturas

# A função realiza uma verificação da assinatura em anel
def verificar_assinatura_em_anel(mensagem, assinaturas, chaves_publicas):
    digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
    digest.update(mensagem.encode())
    hash_mensagem = digest.finalize()

    # Fazendo a verificação de todas as assinaturas
    for i in range(len(assinaturas)):
        try:
            chaves_publicas[i].verify(
                assinaturas[i],
                hash_mensagem,
                padding.PSS(
                    mgf=padding.MGF1(hashes.SHA256()),
                    salt_length=padding.PSS.MAX_LENGTH
                ),
                hashes.SHA256()
            )
            return True  # Se pelo menos uma assinatura for válida, é verdadeiro
        except:
            continue
    return False  # Se nenhuma assinatura for válida, é falso

chaves_privadas = [gerar_chaves() for _ in range(5)]
chaves_publicas = [chave.public_key() for chave in chaves_privadas]

mensagem = "mensagem secreta"
indice_publico = 2  # Indice do usuário que realizou a assinatura

assinaturas = assinatura_em_anel(mensagem, chaves_privadas, indice_publico)
verificacao = verificar_assinatura_em_anel(mensagem, assinaturas, chaves_publicas)

print(f"A verificação da assinatura em anel foi {'sucesso' if verificacao else 'falha'}.")
```

Fonte: Adaptado pelo Autor

A Figura 8 apresenta um exemplo prático em *Python* do uso das *Ring Signatures*, desde a geração das chaves até a verificação das assinaturas por qualquer um dos membros do grupo.

Inicialmente é feita a importação do módulo ***cryptography*** (realizar operações criptográficas). Posteriormente, são implementadas as seguintes funções:

gerar_chaves(): Para gerar um par de chaves privadas ou públicas possuindo um tamanho de chave especificado e também um expoente público padrão, onde a chave privada é de fato retornada pela função;

assinatura_em_anel(): Para criar um *hash* da mensagem e depois gerar uma assinatura falsa de maneira aleatória para todos que compõem o grupo, com exceção para o membro que está de fato assinando (indicado por ***indice_publico)***;

verificar_assinatura_em_anel(): Para criar um *hash* da mensagem e depois tentar a verificação de cada assinatura utilizando a chave pública correspondente. Caso pelo menos uma das assinaturas tiver sido validada com sucesso, a função vai retornar *true*, indicando que aquela assinatura foi válida. Porém, se todas as assinaturas derem falha na verificação, a função vai retornar *false*, indicando que aquela assinatura foi inválida. Por fim, o código imprime indicando se a verificação da assinatura foi um sucesso ou não.

4.3 Discussão Comparativa

Goldreich (2004) descreve que o ZKP é uma técnica onde o provador consegue convencer o verificador de que uma afirmação é considerada verdadeira, sem revelar nenhuma outra informação, apenas a validade daquela afirmação. Por outro lado, Liu, Wei e Wong (2004) afirmam que as *Ring Signatures* são diferentes pelo fato de proporcionarem o anonimato ao assinante em um grupo, sem revelar qual o membro daquele grupo que efetuou a assinatura. A partir disso, é possível notar que existe uma distinção básica onde estabelece a natureza do ZKP como uma ferramenta capaz de validar afirmações mantendo a confidencialidade, de modo que contrasta com a finalidade das *Ring Signatures*, pois esta visa a preservação de anonimato do assinante.

Gennaro et al. (2013) destacam a flexibilidade do ZKP em variados contextos, englobando sua aplicabilidade nos sistemas de votação e também na autenticação segura. Por outro lado, Chow et al. (2004) indicam que, embora as *Ring Signatures* sejam consideradas menos versáteis, elas fornecem vantagens relevantes em termos de escalabilidade e eficiência nos sistemas onde o anonimato do assinante é fundamental.

Sahai e Vadhan (2003) discutem sobre o nível de complexidade do ZKP, evidenciando que, apesar do poder computacional, podem haver desafios inerentes à implementação prática por conta da necessidade de aumento dos recursos computacionais. Em contrapartida, Bender, Katz e Morselli (2006), ao debater as *Ring Signatures*, examinam sua maior praticabilidade nas aplicações do mundo real, principalmente em sistemas que possuem mensagens anônimas e nas criptomoedas, por causa da sua alusiva simplicidade computacional.

Chaum e Pedersen (1992) afirmam que o ZKP possui um papel relevante na proteção da confidencialidade dos dados, permitindo que ocorra a verificação das afirmações sem que haja o comprometimento a integridade da informação. Enquanto Rivest, Shamir e Tauman (2001) enfatizam que, embora as *Ring Signatures* façam a proteção da identidade do assinante, podem não fornecer o mesmo nível de proteção à integridade dos dados subjacentes, uma vez que o foco é vinculado ao anonimato e não a segurança dos dados em si.

Miers et al. (2013) investigam a integração do ZKP em contratos inteligentes, dando destaque a capacidade de realização de operações complexas sem que haja o comprometimento da privacidade dos usuários. Contudo, Fujisaki e Suzuki (2007) indicam que, enquanto as *Ring Signatures* podem oferecer o anonimato das transações, não sendo tão eficiente nas aplicações de contratos inteligentes, onde os conceitos de clareza e especificidade dos termos são considerados essenciais.

Ben-Sasson et al. (2014) destacam a capacidade do ZKP na integração com protocolos distintos em *Blockchain*, fornecendo flexibilidade para os sistemas de prova sem que possa comprometer a privacidade. No entanto, Chow et al. (2004) examinam que, embora as *Ring Signatures* ofereçam um elevado nível de anonimato, podem proporcionar desafios de interoperabilidade nos sistemas de *Blockchain* mais complexos, por conta da natureza especializada e foco no anonimato.

Gennaro et al. (2013) indicam que o ZKP, apesar de poderoso em termos de privacidade, podem ser considerados custosos em relação aos recursos computacionais e tempo de processamento na *Blockchain*. Enquanto Bender, Katz e Morselli (2006) evidenciam que as *Ring Signatures*, embora elevem o tamanho das transações, normalmente possui requisitos computacionais mais simples, de modo que pode ser considerado importante para as redes *Blockchain* que realizam um alto número de transações.

Ben-Sasson et al. (2014) e King e Nadal (2012) abordam sobre os problemas que estão associados diretamente à implementação da *Blockchain* com a utilização do ZKP ou *Ring Signatures* envolvendo questões técnicas, como a escalabilidade e a eficiência computacional, e as questões legais. São sugeridas várias abordagens para a resolução desses problemas, incluindo o desenvolvimento de protocolos de *Blockchain* que sejam mais eficientes, como os que empregam PoS ao invés do PoW, para que seja possível reduzir o consumo de energia e elevar a escalabilidade. Além disso, ao aprimorar as técnicas do ZKP para torná-las mais leves computacionalmente consegue facilitar a sua adoção em uma larga escala.

Hardwick et al. (2018) apresentam um sistema hipotético que pode fazer a utilização de *Blockchain* com ZKP e *Ring Signatures* sendo projetado para uma aplicação de votação eletrônica, onde a integridade e a anonimidade dos votos são vistas como críticas. A *Blockchain* iria servir como um livro-razão público e imutável que pode registrar os votos, enquanto que os ZKP poderiam ser usados para permitir que os eleitores possam comprovar a sua elegibilidade para votar sem que consiga revelar suas identidades. As *Ring Signatures* poderiam incluir uma

camada adicional de anonimato, de modo que permite que os votos sejam misturados, tornando impossível de determinar qual foi o eleitor que votou em qual opção. Sendo assim, este sistema poderia garantir a transparência no processo eleitoral, tendo em vista que também realiza a proteção da privacidade dos votantes.

4.4 Conformidade Regulatória

A implementação do direito de ser esquecido explícito pela LGPD e GDPR, é considerado um desafio para sistemas que utilizam o ZKP. Pois, embora essas provas realizem a proteção da privacidade, elas também podem gerar complexidades quando os indivíduos fazem uma solicitação de exclusão dos dados, pelo fato de que a verificação pode criar uma dependência das informações que, teoricamente, precisariam ser esquecidas. Essa implementação também vai de encontro ao conceito de imutabilidade presente nas *Ring Signatures* em *Blockchain*. Este direito possibilita aos indivíduos solicitar a remoção dos dados pessoais, sendo assim é visto como um desafio, pois a existência de um sistema que utiliza esses dados proporciona à permanência dos registros.

A importância da segurança dos dados na LGPD e GDPR é fundamental, sendo assim, o ZKP pode fornecer um método mais robusto para proteção dos dados contra o acesso não autorizado. Entretanto, ele também indica que a detecção e notificação de violações de dados podem ser consideradas complicadas, por conta da própria natureza do ZKP de ocultar as informações. Existe também dificuldade na aplicação da LGPD e GDPR em ambientes onde os controladores de dados não conseguem ser facilmente identificados, como é o caso desses sistemas. Pelo fato de que a LGPD e GDPR pressupõem a existência de entidades claramente identificáveis responsáveis pelo processamento dos dados, o que se torna complicado por conta da natureza anônima das *Ring Signatures*.

4.5 Conclusão

Pode-se concluir através desse estudo que é destacada uma tensão intrínseca entre os avanços na tecnologia de proteção de dados e as regulamentações de proteção de dados. A necessidade de entidades que sejam claramente identificáveis e responsáveis pelo processamento de dados, conforme descrito pela LGPD e GDPR, também é visto como desafiador em sistemas que usam ZKP e Ring Signatures devido ao anonimato que ambas proporcionam.

Assim, para obter avanço na compatibilidade entre essas tecnologias e regulamentações de proteção de dados, é fundamental que os desenvolvedores, legisladores e reguladores possam trabalhar em conjunto. Pois, devem buscar soluções inovadoras que venham a permitir o aproveitamento das vantagens das tecnologias de ZKP e Ring Signatures enquanto se conformam às exigências legais de proteção de dados e privacidade. Dessa forma, pode incluir o desenvolvimento

de novos métodos que consigam manter a eficácia dessas tecnologias, ao mesmo tempo em que buscam fornecer mecanismos para a exclusão dos dados quando necessário, de modo que respeite o direito ao esquecimento de maneira eficiente e efetiva.

5

Considerações Finais

Foi evidenciado neste trabalho que a transparência inerente a essa tecnologia permite a visibilidade de todas as transações por todos os participantes da rede e pode ser vista como uma vulnerabilidade em termos de privacidade, principalmente quando trata-se de dados sensíveis. Além disso, a conformidade regulatória com regulamentações como a LGPD e GDPR, impõe uma série de restrições rígidas sobre o processamento e proteção de informações pessoais, representando um desafio adicional para as aplicações baseadas em *Blockchain*.

Diante dos desafios, foram identificadas algumas soluções para lidar com estas questões. Dentre as propostas, destacam-se o uso de mecanismos de controle de acesso, que permitem que sejam definidas permissões para o acesso aos dados armazenados no *Blockchain*, técnicas de criptografia e anonimização dos dados para realizar a proteção da privacidade dos usuários.

Ademais, a implementação de técnicas e mecanismos de criptografia e privacidade na *Blockchain* foi sugerida como uma alternativa viável, fornecendo um maior controle sobre o acesso aos dados. Além disso, a utilização de técnicas de criptografia como o ZKP, foi vista como uma forma de processar os dados sem revelar o conteúdo original, mantendo a privacidade.

Por fim, esta dissertação contribui para o entendimento das questões relacionadas à privacidade de dados em *Blockchain* e fornece *insights* para empresas, organizações e reguladores que buscam fazer o uso dessa tecnologia de forma legal, ética e visando a conformidade regulatória com as regulamentações de proteção de dados como é o caso da LGPD e GDPR.

5.1 Trabalhos Futuros

Um possível trabalho para uma futura tese de doutorado poderia investigar a evolução das soluções de privacidade de dados na tecnologia *Blockchain*, levando em consideração o avanço das regulamentações de proteção de dados e as elevadas demandas por privacidade e segurança. O estudo poderia obter uma análise detalhada das tecnologias emergentes, como é o

caso da criptografia pós-quântica e das técnicas de privacidade aprimoradas, e sua aplicação nesses ambientes.

Existe também a possibilidade de investigar, futuramente, a eficácia das soluções propostas para tratar os desafios de privacidade de dados na *Blockchain*, através de avaliações práticas e estudos de caso em ambientes reais. Isso poderia conter a análise das métricas de desempenho, segurança e a conformidade regulatória com as regulamentações de proteção de dados. Outra área de pesquisa considerada promissora está atrelada às implicações éticas e sociais da privacidade de dados em *Blockchain*, considerando o impacto ocasionado nas relações de confiança, governança de dados e nas questões de justiça e igualdade.

Ademais, o estudo poderia abordar sobre o desenvolvimento de *frameworks* e das diretrizes para a governança ética nestes ambientes, tendo em vista as preocupações com privacidade e conformidade com regulamentações como a LGPD e GDPR.

5.2 Trabalhos Publicados

O artigo intitulado "A comparative study between zero-knowledge proof (ZKP) and ring signatures targeting the legal and regulatory implications with the general data protection law (GDPL) and general data protection regulation (GDPR)", correspondente ao capítulo 4 desta dissertação, foi publicado no periódico Observatório de La Economía Latinoamericana (OLEL), que possui Qualis A4.

Referências

ADIDA, B. Helios: web-based open-audit voting. In: *Proceedings of the 17th Conference on Security Symposium*. USA: USENIX Association, 2008. (SS'08), p. 335–348. Citado na página 61.

AHMED, J. et al. Towards blockchain-based gdpr-compliant online social networks: challenges, opportunities and way forward. In: SPRINGER. *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 1*. San Francisco, USA, 2020. p. 113–129. Citado 4 vezes nas páginas 38, 44, 51 e 55.

AL-ZABEN, N. et al. General data protection regulation complied blockchain architecture for personally identifiable information management. In: IEEE. *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. Southend, UK, 2018. p. 77–82. Citado 3 vezes nas páginas 38, 41 e 54.

ALI, M. et al. Blockstack: A global naming and storage system secured by blockchains. In: *2016 USENIX Annual Technical Conference (USENIX ATC 16)*. Denver, CO: USENIX Association, 2016. p. 181–194. ISBN 978-1-931971-30-0. Disponível em: <https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali>. Citado 2 vezes nas páginas 19 e 30.

ALVES, P. H. et al. *Permissioned Blockchains: Towards Privacy Management and Data Regulation Compliance*. 2020. Citado 4 vezes nas páginas 16, 39, 49 e 56.

ANDROULAKI, E. et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the Thirteenth EuroSys Conference*. New York, NY, USA: Association for Computing Machinery, 2018. (EuroSys '18). ISBN 9781450355841. Disponível em: <https://doi.org/10.1145/3190508.3190538>. Citado 3 vezes nas páginas 26, 27 e 29.

ANDROUTSELLIS-THEOTOKIS, S.; SPINELLIS, D. A survey of peer-to-peer content distribution technologies. *ACM computing surveys (CSUR)*, ACM New York, NY, USA, v. 36, n. 4, p. 335–371, 2004. Citado na página 21.

ANTONOPOULOS, A. M. *Mastering Bitcoin*. Sebastopol, California, USA: "O'Reilly Media, Inc.", 2014. Citado 5 vezes nas páginas 20, 21, 23, 24 e 30.

ARBABI, M. S. et al. A survey on blockchain for healthcare: Challenges, benefits, and future directions. v. 25, n. 1, p. 386–424, 2023. Citado 3 vezes nas páginas 38, 39 e 54.

ATZEI, N.; BARTOLETTI, M.; CIMOLI, T. A survey of attacks on ethereum smart contracts (sok). In: SPRINGER. *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6*. [S.l.], 2017. p. 164–186. Citado na página 25.

BAI, P. et al. Gdpr compliant data storage and sharing in smart healthcare system: A blockchain-based solution. *Electronics*, MDPI, v. 11, n. 20, p. 3311, 2022. Citado 3 vezes nas páginas 39, 49 e 56.

BAIAO, R. B. S. M. Lei geral de proteção de dados, direito ao apagamento, correção dos dados e blockchain: análise da pertinência tecnológica. *Cadernos Jurídicos*, Escola Paulista da Magistratura (EPM), v. 21, n. 53, p. 151–162, 2020. Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/142292>. Citado na página 16.

BAMAKAN, S. M. H.; MOGHADDAM, S. G.; MANSHADI, S. D. Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. *Journal of Cleaner Production*, Elsevier, v. 302, p. 127021, 2021. Citado na página 20.

BATISTA, A. O. A. et al. Identificação digital baseada em blockchain: Um conceito disruptivo no ciberespaço. *Simpósio Internacional de Inovação em Mídias Interativas*, v. 5, p. 307–320, 2018. Citado na página 21.

BEN-SASSON, E. et al. Snarks for c: Verifying program executions succinctly and in zero knowledge. In: CANETTI, R.; GARAY, J. A. (Ed.). *Advances in Cryptology – CRYPTO 2013*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 90–108. Citado 2 vezes nas páginas 58 e 61.

BEN-SASSON, E. et al. Zerocash: Decentralized anonymous payments from bitcoin. In: IEEE. *2014 IEEE Symposium on Security and Privacy*. Berkeley, CA, USA, 2014. p. 459–474. Citado 4 vezes nas páginas 31, 58, 61 e 66.

BENDER, A.; KATZ, J.; MORSELLI, R. Ring signatures: Stronger definitions, and constructions without random oracles. In: HALEVI, S.; RABIN, T. (Ed.). *Theory of Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. p. 60–79. Citado 2 vezes nas páginas 65 e 66.

BOULOS, M. N. K.; WILSON, J. T.; CLAUSON, K. A. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *International journal of health geographics*, BioMed Central, v. 17, 2018. Citado 3 vezes nas páginas 38, 43 e 55.

BRASIL. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF, 2018. Lei nº 13.709. Citado na página 32.

BROWN, R. G. et al. Corda: an introduction. *R3 CEV, August*, R3 CEV New York, NY, USA, v. 1, n. 15, p. 14, 2016. Citado na página 28.

BUTERIN, V.; GRIFFITH, V. *Casper the Friendly Finality Gadget*. [S.l.], 2017. Disponível em: <https://arxiv.org/pdf/1710.09437.pdf>. Citado 2 vezes nas páginas 25 e 26.

BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, v. 3, n. 37, p. 2–1, 2014. Citado na página 28.

BYGRAVE, L. A. Data Privacy Law: An International Perspective. In: . Oxford, United Kingdom: Oxford University Press, 2014. ISBN 9780199675555. Citado na página 31.

CACHIN, C.; KURSAWE, K.; SHOUP, V. Random oracles in constantinople: Practical asynchronous byzantine agreement using cryptography. *Journal of Cryptology*, 2000. Citado na página 22.

CACHIN, C. et al. Architecture of the hyperledger blockchain fabric. In: CHICAGO, IL. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. IBM Research - Zurich, CH-8803 Ruschlikon, Switzerland, 2016. v. 310, n. 4, p. 1–4. Citado 2 vezes nas páginas 26 e 27.

CACHIN, C.; VUKOLIĆ, M. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*, 2017. Citado na página 29.

CAMENISCH, J.; STADLER, M. Proof systems for general statements about discrete logarithms. *Technical Report/ETH Zurich, Department of Computer Science*, ETH Zurich, v. 260, 1997. Citado na página 58.

CHAPPLE, M.; STEWART, J. M.; GIBSON, D. *Certified Information Systems Security Professional Study Guide 6th Edition*. [S.l.: s.n.], 2013. Citado na página 34.

CHAPPLE, M.; STEWART, J. M.; GIBSON, D. *(ISC)^2 CISSP Certified Information Systems Security Professional Official Study Guide*. Hoboken, New Jersey, USA: John Wiley & Sons, 2018. Citado na página 32.

CHAUM, D.; PEDERSEN, T. P. Wallet databases with observers. In: *Annual International Cryptology Conference*. Berlin, Heidelberg: Springer, 1992. p. 89–105. Citado na página 66.

CHIARINI, A.; COMPAGNUCCI, L. Blockchain, data protection and p2p energy trading: A review on legal and economic challenges. *Sustainability*, MDPI, v. 14, n. 23, p. 16305, 2022. Citado 3 vezes nas páginas 38, 47 e 55.

CHOW, S. S. M. et al. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In: LIM, J.-I.; LEE, D.-H. (Ed.). *Information Security and Cryptology - ICISC 2003*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 352–369. Citado 2 vezes nas páginas 65 e 66.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. *Ieee Access*, Ieee, v. 4, p. 2292–2303, 2016. Citado na página 26.

CHUEN, D. L. K. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. [S.l.]: Academic Press, 2015. Citado na página 21.

CROSBY, M. et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, v. 2, n. 6-10, p. 71, 2016. Citado 2 vezes nas páginas 27 e 28.

DICK, C. I.; PRAKTIKNJO, A. Blockchain technology and electricity wholesale markets: Expert insights on potentials and challenges for otc trading in europe. *Energies*, MDPI, v. 12, n. 5, p. 832, 2019. Citado 3 vezes nas páginas 38, 48 e 55.

DINGLEDINE, R.; MATHEWSON, N.; SYVERSON, P. *Tor: The Second-Generation Onion Router*. [S.l.], 2004. Citado na página 62.

DWYER, G. P. The economics of bitcoin and similar private digital currencies. *Journal of financial stability*, Elsevier, v. 17, p. 81–91, 2015. Citado na página 25.

FEILER, L.; FORGÓ, N.; WEIGL, M. The eu general data protection regulation (gdpr): A commentary. *(No Title)*, 2018. Citado na página 33.

FEKETE, D. L.; KISS, A. Toward building smart contract-based higher education systems using zero-knowledge ethereum virtual machine. *Electronics*, MDPI, v. 12, n. 3, p. 664, 2023. Citado 3 vezes nas páginas 39, 50 e 56.

FILIPPI, P. D.; LOVELUCK, B. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet policy review*, v. 5, n. 4, 2016. Citado na página 29.

FUJISAKI, E.; SUZUKI, K. Traceable ring signature. In: *International Workshop on Public Key Cryptography*. Berlin, Heidelberg: Springer, 2007. p. 181–200. Citado na página 66.

GENNARO, R. et al. Quadratic span programs and succinct nizks without pcps. In: JOHANSSON, T.; NGUYEN, P. Q. (Ed.). *Advances in Cryptology – EUROCRYPT 2013*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 626–645. Citado 2 vezes nas páginas 65 e 66.

GOLDREICH, O. *Foundations of Cryptography, Volume 2*. Cambridge, UK: Cambridge University Press, 2004. Citado 2 vezes nas páginas 59 e 65.

GOLDWASSER, S.; MICALI, S.; RACKOFF, C. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, SIAM, v. 14, n. 1, p. 186–208, 1989. Citado 2 vezes nas páginas 58 e 59.

GUDGEON, L. et al. Sok: Layer-two blockchain protocols. In: *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers*. [S.l.]: Springer International Publishing, 2020. v. 24, p. 201–226. Citado na página 21.

HAN, S.; PARK, S. A gap between blockchain and general data protection regulation: A systematic review. *IEEE Access*, v. 10, p. 103888–103905, 2022. Citado 4 vezes nas páginas 38, 39, 50 e 54.

HAQUE, A. B. et al. Gdpr compliant blockchains–a systematic literature review. *IEEE Access*, v. 9, p. 50593–50606, 2021. Citado 5 vezes nas páginas 38, 40, 50, 51 e 54.

HARDWICK, F. S. et al. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. [S.l.: s.n.], 2018. p. 1561–1567. Citado na página 66.

HARO-OLMO, F. J. de; VARELA-VACA, Á. J.; ÁLVAREZ-BERMEJO, J. A. Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, MDPI, v. 20, n. 24, p. 7171, 2020. Citado 3 vezes nas páginas 38, 47 e 55.

HARTZOG, W. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA, USA: Harvard University Press, 2018. Citado na página 31.

HONAN, B. *ISO27001 in a Windows Environment*. [S.l.]: IT Governance Publishing, 2017. Citado na página 34.

KAKARLAPUDI, P. V.; MAHMOUD, Q. H. A systematic review of blockchain for consent management. In: MDPI. *Healthcare*. [S.l.], 2021. v. 9, n. 2, p. 137. Citado 3 vezes nas páginas 38, 45 e 55.

KASSEM, J. A. et al. Dns-idm: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences*, MDPI, v. 9, n. 15, p. 2953, 2019. Citado 3 vezes nas páginas 38, 48 e 55.

KING, S.; NADAL, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, v. 19, n. 1, 2012. Citado 2 vezes nas páginas 22 e 66.

KOSBA, A. et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: IEEE. *2016 IEEE symposium on security and privacy (SP)*. [S.l.], 2016. p. 839–858. Citado na página 27.

KUMAR, A. et al. *Traceability of Monero Transactions*. 2017. Preprint at https://eprint.iacr.org. Citado na página 62.

KUNER, C.; BYGRAVE, L. A.; DOCKSEY, C. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press, 2020. Citado na página 33.

LANTZ, L.; CAWREY, D. *Mastering Blockchain: Unlocking the Power of Cryptocurrencies and Smart Contracts*. Sebastopol, California, USA: "O'Reilly Media, Inc.", 2020. Citado na página 15.

LARIMER, D. *Delegated Proof-of-Stake (DPOS)*. 2014. Bitshare whitepaper. Citado na página 23.

LEE, W.-S. et al. Spchain: A smart and private blockchain-enabled framework for combining gdpr-compliant digital assets management with ai models. *IEEE Access*, v. 10, p. 130424–130443, 2022. Citado 3 vezes nas páginas 38, 41 e 54.

LIMA, C.; COSTA, H.; SILVA, V. *LGPD: Guia de Implementação*. São Paulo: Editora Revista dos Tribunais, 2019. Citado na página 15.

LIU, J. K.; WEI, V. K.; WONG, D. S. Linkable spontaneous anonymous group signature for ad hoc groups. In: WANG, H.; PIEPRZYK, J.; VARADHARAJAN, V. (Ed.). *Information Security and Privacy*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 325–335. Citado 2 vezes nas páginas 62 e 65.

MA, S.; CAO, Y.; XIONG, L. Efficient logging and querying for blockchain-based cross-site genomic dataset access audit. *BMC medical genomics*, BioMed Central, v. 13, n. 7, p. 1–13, 2020. Citado 4 vezes nas páginas 38, 42, 51 e 54.

MALDONADO, V. N.; BLUM, R. O. *LGPD: Lei Geral de Proteção de Dados Comentada*. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2019. Citado na página 32.

MAURER, B.; NELMS, T. C.; SWARTZ, L. "when perhaps the real problem is money itself!": the practical materiality of bitcoin. *Social semiotics*, Taylor & Francis, v. 23, n. 2, p. 261–277, 2013. Citado 2 vezes nas páginas 18 e 25.

MAZIERES, D. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, v. 32, p. 1–45, 2015. Citado na página 27.

MEIKLEJOHN, S. et al. A fistful of bitcoins: characterizing payments among men with no names. In: *Proceedings of the 2013 conference on Internet measurement conference*. USA: Association for Computing Machinery, 2013. p. 127–140. Citado na página 15.

MENDLING, J. et al. Blockchains for business process management-challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, ACM New York, NY, USA, v. 9, n. 1, p. 1–16, 2018. Citado na página 26.

MERLEC, M. M. et al. A smart contract-based dynamic consent management system for personal data usage under gdpr. *Sensors*, MDPI, v. 21, n. 23, p. 7994, 2021. Citado 3 vezes nas páginas 38, 45 e 55.

MIERS, I. et al. Zerocoin: Anonymous distributed e-cash from bitcoin. In: IEEE. *2013 IEEE Symposium on Security and Privacy*. San Francisco, California, USA, 2013. p. 397–411. Citado 3 vezes nas páginas 19, 26 e 66.

MOUGAYAR, W. *Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet*. Rio de Janeiro, Brasil: Alta Books Editora, 2018. Citado na página 14.

MULLAN, C. Blockchain basics: A non-technical introduction in 25 steps. 2018. Citado na página 26.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260, 2008. Citado 7 vezes nas páginas 15, 18, 19, 21, 22, 23 e 24.

NARAYANAN, A. et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton, NJ, USA: Princeton University Press, 2016. Citado 6 vezes nas páginas 15, 18, 24, 29, 30 e 31.

NBR ISO/IEC 27001–Tecnologia da Informação–Técnicas de Segurança–Sistemas de Gestão da Segurança da Informação–Requisitos. *Rio de Janeiro: ABNT*, 2013. Citado 2 vezes nas páginas 32 e 34.

NBR ISO/IEC 27002. *Tecnologia da Informação–Técnicas de Segurança–Sistemas de Gestão da Segurança da Informação–Requisitos*. Rio de Janeiro, 2013. NBR ISO/IEC 27002. Citado na página 32.

PETERS, G. W.; PANAYI, E. *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*. Springer, 2016. (New Economic Windows). Disponível em: <https://doi.org/10.1007/978-3-319-42448-4_13>. Citado na página 28.

PETERSEN, K. e. a. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, v. 64, p. 1–18, 2015. Citado na página 35.

POLITOU, E. et al. Blockchain mutability: Challenges and proposed solutions. v. 9, n. 4, p. 1972–1986, 2021. Citado 4 vezes nas páginas 38, 40, 51 e 54.

RANTOS, K. et al. A blockchain-based platform for consent management of personal data processing in the iot ecosystem. *Security and Communication Networks*, Hindawi Limited, v. 2019, p. 1–15, 2019. Citado 3 vezes nas páginas 38, 44 e 55.

REBELLO, G. et al. *Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric*. 2019. Sociedade Brasileira de Computação. Citado na página 22.

REEGU, F. A. et al. Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, MDPI, v. 15, n. 8, p. 6337, 2023. Citado 3 vezes nas páginas 38, 46 e 55.

REGULATION, G. D. P. General data protection regulation (gdpr). *Intersoft Consulting, Accessed in October*, v. 24, n. 1, 2018. Citado na página 33.

REVOREDO, T. *Blockchain: tudo que você precisa saber (potencial e realidade)*. [S.l.]: The Global Strategy, 2019. Citado na página 25.

RIVEST, R. L.; SHAMIR, A.; TAUMAN, Y. How to leak a secret. In: BOYD, C. (Ed.). *Advances in Cryptology — ASIACRYPT 2001*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 552–565. Citado 2 vezes nas páginas 62 e 66.

ROMAN-MARTINEZ, I. et al. Blockchain-based service-oriented architecture for consent management, access control, and auditing. v. 11, p. 12727–12741, 2023. Citado 3 vezes nas páginas 38, 39 e 54.

SAHAI, A.; VADHAN, S. A complete problem for statistical zero knowledge. *Journal of the ACM (JACM)*, ACM New York, NY, USA, v. 50, n. 2, p. 196–249, 2003. Citado na página 65.

SCHAEFER, C.; EDMAN, C. Transparent logging with hyperledger fabric. In: IEEE. *IEEE International Conference on Blockchain and Cryptocurrency*. Seoul, Korea (South), 2019. p. 65–69. Citado 3 vezes nas páginas 38, 41 e 54.

SCHOLLMEIER, R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: IEEE. *Proceedings first international conference on peer-to-peer computing*. [S.l.], 2001. p. 101–102. Citado na página 21.

SCHWARTZ, P. M.; PEIFER, K. N. *Data Privacy Law: A Study of United States Data Protection*. Virginia: Michie, 2020. Citado na página 33.

SKYPRO. *ISO 27001 Information Security Management System*. [S.l.], 2018. Disponível em: <https://skypro.co.id/iso-27001-post/>. Acesso em: 12 mai. 2022. Citado na página 34.

SOLOVE, D. J. A taxonomy of privacy. *U. Pa. l. Rev.*, HeinOnline, v. 154, p. 477, 2005. Citado na página 31.

SOLOVE, D. J. *Understanding Privacy*. USA: Harvard University Press, 2010. Citado na página 14.

SOLOVE, D. J.; SCHWARTZ, P. M. *Information Privacy Law*. USA: Aspen Publishing, 2020. Citado na página 14.

SOUSA, J.; BESSANI, A.; VUKOLIC, M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: IEEE. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. [S.l.], 2018. p. 51–58. Citado na página 23.

STALLINGS, W.; BRESSAN, G.; BARBOSA, A. *Criptografia e segurança de redes* . [S.l.]: Pearson Educacion, 2008. Citado 2 vezes nas páginas 19 e 25.

STELZER, J. et al. A lei geral de proteção de dados pessoais e os desafios das instituições de ensino superior para a adequação. In: *XIX Colóquio Internacional de Gestão Universitária*. Florianópolis, Santa Catarina: [s.n.], 2019. Citado na página 32.

SWAN, M. *Blockchain: blueprint for a new economy*. [S.l.]: O'Reilly Media, Inc., 2015. Citado 2 vezes nas páginas 28 e 30.

SZABO, N. Formalizing and securing relationships on public networks. *First monday*, 1997. Citado na página 25.

TAPSCOTT, D.; TAPSCOTT, A. Blockchain revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo. *São Paulo: SENAI-SP Editora*, p. 36, 2016. Citado 6 vezes nas páginas 14, 20, 24, 25, 27 e 28.

TASCA, P.; HAYES, A.; LIU, S. The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships. *The Journal of Risk Finance*, v. 19, n. 2, p. 94–126, 2018. Citado na página 23.

TEIXEIRA, T. *Lei Geral de Proteção de Dados Pessoais: Comentada artigo por artigo-4ª edição 2022*. [S.l.]: Saraiva Educação SA, 2022. Citado na página 29.

UPADRISTA, V.; NAZIR, S.; TIANFIELD, H. Secure data sharing with blockchain for remote health monitoring applications: a review. *Journal of Reliable Intelligent Environments*, Springer, p. 1–20, 2023. Citado 3 vezes nas páginas 38, 43 e 55.

VALIM, T. R. A. Da privacidade à proteção de dados pessoais:: fundamentos da lei geral de proteção de dados. *Inova Jur*, v. 1, n. 1, 2022. Citado na página 32.

VUKOLIĆ, M. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: SPRINGER. *Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*. [S.l.], 2016. p. 112–125. Citado 2 vezes nas páginas 27 e 29.

WANG, S. et al. Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, v. 49, n. 11, p. 2266–2277, 2019. Citado na página 21.

WOOD, G. et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, v. 151, n. 2014, p. 1–32, 2014. Citado na página 24.

WYLDE, V. et al. Cybersecurity, data privacy and blockchain: a review. *SN Computer Science*, Springer, v. 3, n. 2, p. 127, 2022. Citado 4 vezes nas páginas 38, 42, 51 e 54.

XU, H. et al. Blockchain-based crowdsourcing makes training dataset of machine learning no longer be in short supply. *Wireless Communications and Mobile Computing*, Hindawi, v. 2022, 2022. Citado 4 vezes nas páginas 38, 46, 51 e 55.

ZHENG, Z. et al. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE. *2017 IEEE international congress on big data (BigData congress)*. [S.l.], 2017. Citado 2 vezes nas páginas 22 e 28.

ZHENG, Z. et al. Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, Inderscience Publishers (IEL), v. 14, n. 4, p. 352–375, 2018. Citado 2 vezes nas páginas 28 e 29.

ZOHAR, A. Bitcoin: under the hood. *Communications of the ACM*, ACM New York, NY, USA, v. 58, n. 9, p. 104–113, 2015. Citado 3 vezes nas páginas 24, 25 e 31.