UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

JOÃO VICTOR MARQUES DOS SANTOS

PRIVACIDADE E SEGURANÇA: EXPLORANDO IDENTIDADES DESCENTRALIZADAS E BLOCKCHAIN COMO SOLUÇÃO PARA O SISTEMA DE SAÚDE BRASILEIRO

RECIFE
2024

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

JOÃO VICTOR MARQUES DOS SANTOS

PRIVACIDADE E SEGURANÇA: EXPLORANDO IDENTIDADES DESCENTRALIZADAS E BLOCKCHAIN COMO SOLUÇÃO PARA O SISTEMA DE SAÚDE BRASILEIRO

Monografia apresentada ao Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE), como requisito parcial para conclusão do Curso de Sistemas de Informação, orientada pelo professor Hermano Perrelli de Moura.

RECIFE
2024

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

JOÃO VICTOR MARQUES DOS SANTOS

PRIVACIDADE E SEGURANÇA: EXPLORANDO IDENTIDADES DESCENTRALIZADAS E BLOCKCHAIN COMO SOLUÇÃO PARA O SISTEMA DE SAÚDE BRASILEIRO

Monografia submetida ao corpo docente da Universidade Federal de Pernambuco, defendida e aprovada em 20 de março de 2024.

Banca Examinadora:

Orientador

Hermano Perrelli de Moura

Doutor

Examinador

Sérgio Castelo Branco Soares

Doutor

AGRADECIMENTOS

Chegamos na reta final, no momento derradeiro, no fim de uma das fases mais importantes da minha pequena grande vida, o fim da minha graduação. E, ênfase no "chegamos", pois não estou e nunca estive sozinho, e esse mérito é compartilhado com todas as mãos que me seguraram durante esse caminho.

Primeiramente, minha pequena família, mas que nunca me deixou faltar nada, minha mãe - Edneuza, obrigado por todo sacrifício, toda dedicação e toda a fé depositada em mim, a todo meu sucesso eu sempre serei eternamente grato a senhora, graças à sua história, hoje, escrevo este trabalho. Obrigado.

Agradeço também as pessoas que conheci e trilharam este caminho da UFPE juntamente comigo, vivemos juntos intensamente esta fase. Guilherme, Roseno, Diego e Pedro, a vida sorriu para mim quando me juntou com vocês. Gabriel S. e Giovanni, vocês me abraçaram no meu primeiro momento na universidade e continuam até hoje. Renato, Bruno e Gabriel F. eu não consigo pensar como seria possível estar aqui hoje sem ter tido vocês para dividir todas as cargas desse caminho. Obrigado a todos esses e outros por fazerem minha história na UFPE mais bonita e amável.

Agradeço a minha namorada, Letícia, por todo apoio, conversas, abraços, dias e noites em claro, obrigado por abraçar meu eu por inteiro. Obrigado.

Agradeço ainda aos meus amigos Lucas, Emanuel e Gabrielle, obrigado por nunca me deixarem desistir e acompanharem toda minha trajetória do começo ao fim, obrigado por todo apoio. Vinicius, que acreditou em mim no momento mais crucial da minha vida pessoal e profissional e nunca deixou de ter fé na minha capacidade, meu eterno agradecimento.

Gostaria de agradecer também ao professor Hermano Perrelli de Moura por ter aceitado o papel de me orientar durante a produção deste trabalho.

A todos que de alguma forma me apoiaram, me incentivaram, me acompanharam e, mesmo não citados, fizeram parte ativamente da construção desta conquista, meu muito obrigado por tudo.

O primeiro da família a entrar, e o primeiro a sair de uma universidade pública, escrever 100 páginas de um tcc é mais fácil do que escrever este agradecimento, esse mérito é nosso.

Muito obrigado a todos, por tudo.

Epígrafe

"Quisera encontrar aquele menino verso
Que escrevi há tantos anos atrás
Falo assim sem saudade
Falo assim por saber

Se muito vale o já feito
Mais vale o que será
Mais vale o que será
E o que foi feito é preciso
Conhecer para melhor prosseguir"

O Que Foi Feito Devera - Milton Nascimento

RESUMO

Este estudo aborda a importância da integridade dos dados médicos no setor de saúde e sua relação com o sistema de saúde brasileiro. Usando tecnologias de identidades descentralizadas e blockchain, é possível criar dados médicos independentes de entidades centrais, como o SUS, com vantagens como imutabilidade, descentralização e transparência. Isso facilita a consolidação segura das informações de saúde, garantindo acesso seguro quando necessário. A utilização de identidades descentralizadas no blockchain pode aumentar a segurança e o controle dos dados, dando aos pacientes autonomia sobre suas informações. Porém, há desafios como questões jurídicas, falta de comunicação e integração entre serviços de saúde públicos e privados que podem dificultar a adoção dessa tecnologia. O objetivo deste estudo é fazer uma revisão sistemática da literatura para identificar as características, aplicações e desafios dessa tecnologia em contextos de saúde, e como esses dados podem ajudar o contexto de saúde brasileiro.

Palavras-chave: blockchain, identidades descentralizadas, identidade auto-soberana, dados médicos, sistema de saúde, obstáculos à comunicação em saúde, integração de serviços de saúde.

ABSTRACT

This study addresses the importance of medical data integrity in the health sector and its relationship with the Brazilian health system. Using decentralized identity technologies and blockchain, it is possible to create medical data that is independent of central entities, such as the SUS, with advantages such as immutability, decentralization and transparency. This facilitates the secure consolidation of health information, guaranteeing secure access when needed. The use of decentralized identities on the blockchain can increase data security and control, giving patients autonomy over their information. However, there are challenges such as legal issues, lack of communication and integration between public and private health services that can hinder the adoption of this technology. The aim of this study is to carry out a systematic literature review to identify the characteristics, applications and challenges of this technology in healthcare contexts, and how this data can help the Brazilian healthcare context.

Keywords: blockchain, decentralized identities, self-sovereign identity, medical data, health system, obstacles to health communication, integration of health services.

Lista de Ilustrações

Figura 1. Total previsto no mercado de prontuários eletrônicos em bilhões de dólares desde 2015 a 2024. 12
Figura 2. Questionário de jovens profissionais do setor de saúde referente a tecnologia de saúde digital mais benéfica ao paciente nos próximos cinco anos. 13
Figura 3. Questionário de jovens profissionais de saúde sobre problemas experienciados com dados digitais dos pacientes em 2020 14
Figura 4. Representação visual de estruturas de um DLT 17
Figura 5. Representação visual de fluxo de SSI 26
Figura 6. Total de artigos iniciais 31
Figura 7. Representação visual de fluxo de SSI 31
Figura 8. Média das notas de qualificação 32
Figura 9. Comparação de pré e pós análise 33
Figura 10. Distribuição de artigos por ano de publicação 40
Figura 11. Porcentagem de participação de cada repositório 41
Figura 12. Fluxo de um paciente realizando uma cadastro em uma SSI 74
Figura 13. Fluxo de um paciente se autenticando em uma organização com SSI 75

Lista de Tabelas

Tabela 1. Tabela de termos frequentes na definição de blockchain. 18
Tabela 2. Nomes dos repositórios 28
Tabela 3. Lista de palavras chaves 28
Tabela 4. String de busca para resgate dos artigos 29
Tabela 5. Critérios de inclusão e exclusão de artigos 30
Tabela 6. Filtros de artigos 30
Tabela 7. Tópicos de avaliação dos artigos 32
Tabela 8. Lista de artigos aprovados 33
Tabela 9. Termos frequentes e estudos relacionados 41
Tabela 10. Aplicações no setor de saúde e estudos relacionados 52
Tabela 11 - Desafios e estudos relacionados 62

Tabela de Siglas

Sigla	Significado
DID	Decentralized Identity
SUS	Sistema Único de Saúde
IBGE	Instituto Brasileiro de Geografia e Estatística
DLT	Distributed Ledger Technology
VC	Verifiable Credentials
SSI	Self-sovereign identity
ZKP	Zero-Knowledge Proof
DIF	Decentralized Identity Foundation
W3C	World Wide Web Consortium
RSL	Revisão Sistemática da Literatura
VPN	Virtual Private Network
ES	Estudo Selecionado
CE	Critério de Exclusão
CI	Critério de Inclusão
REF	Referência
FHIR	Fast Healthcare Interoperability Resources
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
LGPD	Lei Geral de Proteção de Dados Pessoais
CFM	Conselho Federal de Medicina
RNDS	Rede Nacional de Dados em Saúde
EMR	Electronic Medical Record
IPFS	Interplanetary File System
DATASUS	Departamento de Informática do Sistema Único de Saúde

Sumário

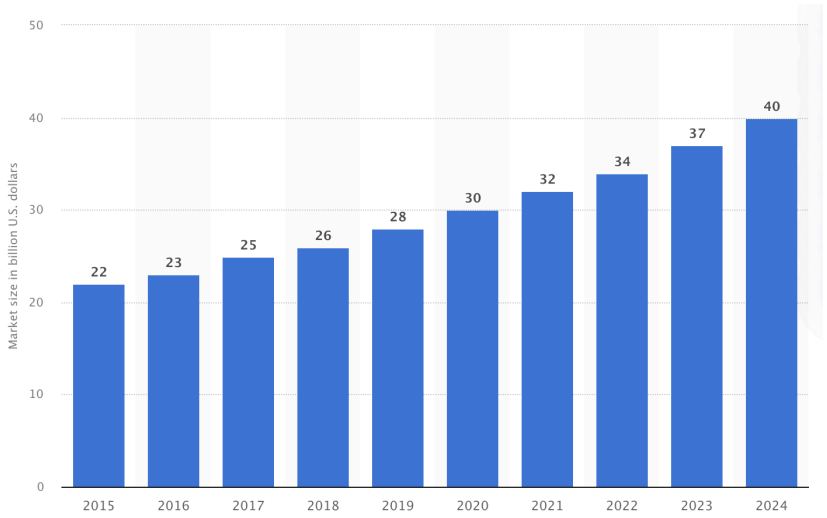
1. INTRODUÇÃO....12
1.1 Objetivos.... 15
1.1.2 Objetivo Geral....15
1.1.2 Objetivos Específicos.... 15
1.2 Pergunta de Pesquisa....16
2. ANÁLISE BREVE SOBRE OS PILARES TECNOLÓGICOS RELACIONADOS.... 16
2.1 Registros distribuídos....16
2.2 Blockchain....17
3. IDENTIDADE DESCENTRALIZADA....19
3.1 Desafios....22
4. IDENTIDADE AUTO-SOBERANA....23
4.1 Relação com DID e definição.... 23
5. METODOLOGIA....26
5.1 Estudos Relacionados....26
5.2 Etapas da Revisão....27
5.2.1 Formulação da Pergunta de Pesquisa....27
5.2.2 Elaboração do Protocolo de Revisão.... 28
5.2.3 Seleção dos Estudos....29
6. RESULTADOS....39
6.1 Interpretação dos Resultados e Redação do Relatório.... 40
6.2 Perguntas de Pesquisa....41
6.2.1 PPS1. Quais os termos técnicos mais frequentes no contexto de blockchain, identidade descentralizada e identidade auto-soberana no setor de saúde?.... 41
6.2.2 PPS2. Como a identidade descentralizada, blockchain e identidade auto-soberana podem ser aplicadas no setor de saúde?.... 51
6.2.3 PPS3. Quais os desafios enfrentados pela aplicação dessas tecnologias no contexto de saúde?....62
7. DISCUSSÃO....72
7.2 Desafios....75
7.3 Tecnologia, Brasil e Saúde.... 76
7.3.1 Contexto....76
7.3.2 Avanços e tecnologias....78
7.3.3 Desafios.... 80
7.3.4 Blockchain e DID como solução.... 81
8. CONCLUSÃO E TRABALHOS FUTUROS.... 83
REFERÊNCIAS BIBLIOGRÁFICAS....85

1. INTRODUÇÃO

No atual cenário tecnológico, a implementação da Saúde Eletrônica destaca-se como uma abordagem essencial, utilizando tecnologias de informação e comunicação para integrar clínicas, unidades de cuidado e departamentos, visando a eficiência na gestão dos sistemas de saúde e seus dados. O propósito fundamental da saúde eletrônica é proporcionar serviços de cuidado eficazes e convenientes, assegurando uma experiência positiva para os pacientes. Nesse contexto, a rápida disponibilização de registros médicos, prontuários e afins provenientes de diversas fontes, e a realização de diagnósticos ágeis por meio da colaboração entre médicos e prestadores de serviços terceirizados tornam-se elementos centrais. Isso permite acesso a dados médicos em qualquer lugar e a qualquer momento, com certas limitações.

A área de saúde lida, diariamente, com um volume massivo de dados relacionados ao estado dos pacientes. Empreitadas governamentais como a Iniciativa de Medicina Precisa, cujo objetivo é levar em consideração as particularidades individuais dos pacientes no intuito de criar um tratamento específico para lidar com uma doença encontrada, não fogem à regra, e buscam manejar os dados dos pacientes com cautela, garantindo que a privacidade dos mesmo seja respeitada [1]. De acordo com o Statista [2], o mercado de prontuários eletrônicos tradicionais está em constante evolução, com uma previsão de valorização ainda para o ano de 2024, como demonstra na figura 1:

Figura 1 - Total previsto no mercado de prontuários eletrônicos em bilhões de dólares desde 2015 a 2024.

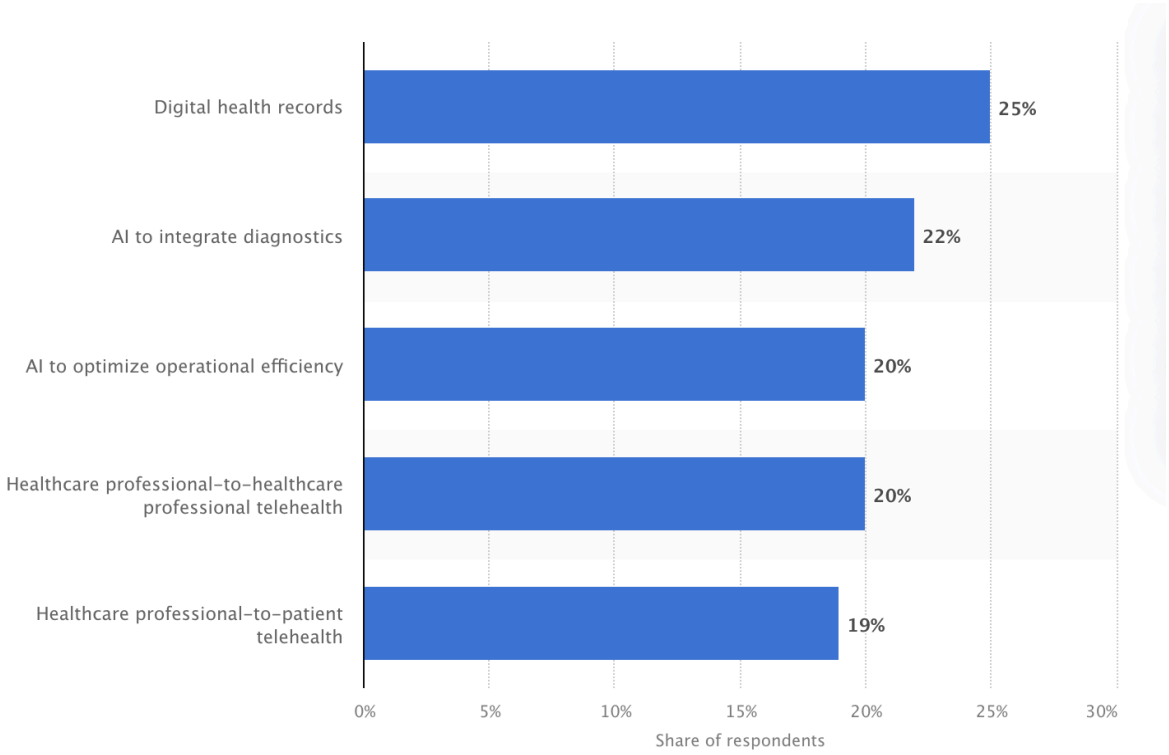


Fonte: Statista. [2]

A alta projeção monetária e o interesse do mercado em estar inserido em uma tendência rentável faz com que medidas de inovação estejam em pesquisa e desenvolvimento a todo instante, e, consequentemente, entre em pauta todas suas limitações e problemáticas para sua construção, desde ao conteúdo que é manejado e as ferramentas que o maneja [2].

O fator de lidar com dados tradicionais faz com que os prontuários, agora vistos eletronicamente, sejam uma questão mais evidenciável para o setor de profissionais de saúde, principalmente devido a anos de evolução médica ainda persistir o uso de sistemas legados e datados para manejar um dado sensível como o do setor de saúde, tendo assim uma urgente necessidade de mudança e evolução, superando até mesmo tecnologias mais disruptivas como inteligência artificial, como demonstra a figura 2 a seguir:

Figura 2 - Questionário de jovens profissionais do setor de saúde referente a tecnologia de saúde digital mais benéfica ao paciente nos próximos cinco anos.

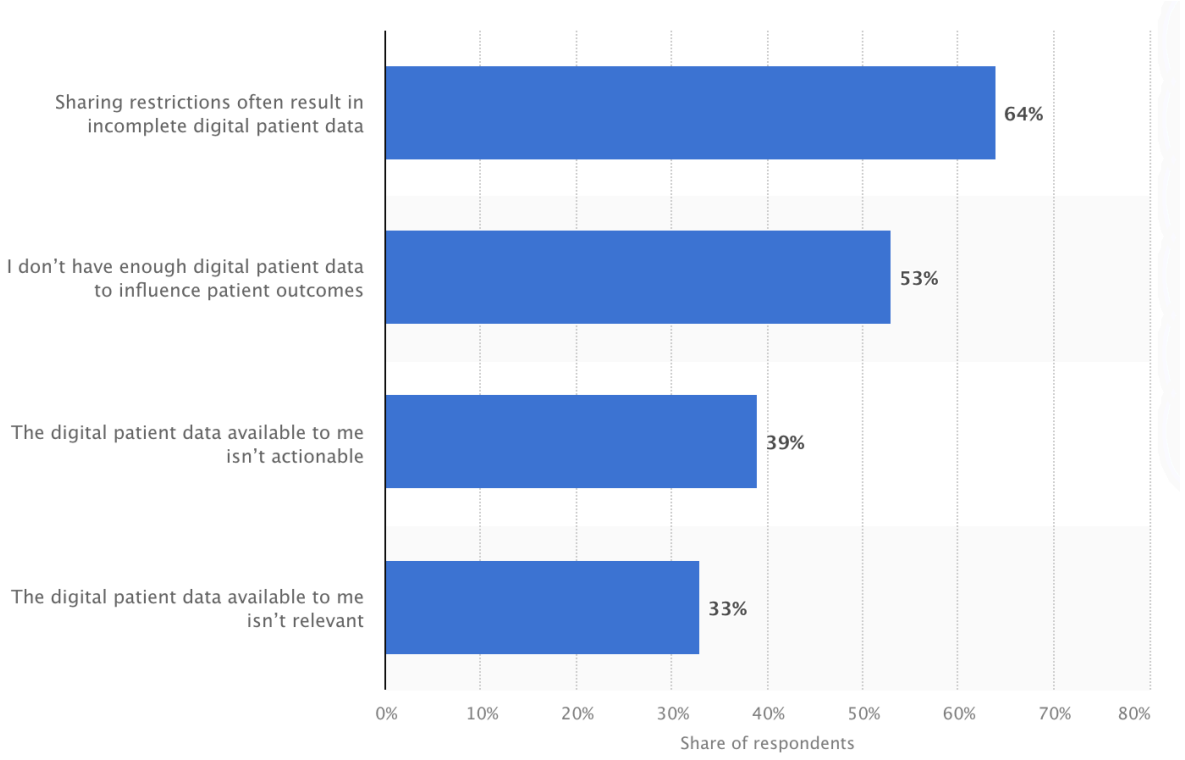


Fonte: Statista. [3]

Nesse contexto, insere-se a necessidade de avaliar com cuidado uma maneira responsável de lidar com essas informações sensíveis. É possível, com o uso de smart contracts, criar uma infraestrutura de compartilhamento de dados virtuais capaz de garantir a segurança e integridade dos dados, assim como garantir uma melhor coordenação entre as instituições que porventura lidem com os dados compartilhados. No entanto, de acordo com

Peng Zhang [4], pesquisadores da área de saúde se deparam com os seguintes problemas: provedores relutantes em compartilhar os dados dos pacientes, incompatibilidade dos sistemas eletrônicos, ausência de um link seguro entre as diferentes empresas de saúde e escalabilidade [4].

Figura 3 - Questionário de jovens profissionais de saúde sobre problemas experienciados com dados digitais dos pacientes em 2020.



Fonte: Statista [5]

No Brasil, o Sistema Único de Saúde (SUS) possui iniciativas de gerenciar e concentrar dados das suas redes de pacientes, como por exemplo o Cartão Nacional de Saúde, com mais de 144 milhões de usuários cadastrados tem como objetivo gerenciar prontuários e históricos médicos da rede pública e, recentemente, o programa "S4SP" que permite o compartilhamento de dados e históricos de todos os frequentadores das organizações da Secretária [6]. Contudo, mesmo estes projetos sendo considerados um sucesso ainda estão suscetíveis a falhas, como revelou o G1 [7] que em dezembro de 2020 em torno de 243 milhões de pacientes tiveram expostos suas informações cadastrais na base do SUS.

Além do fator de insegurança entre o seu próprio sistema, o Brasil é um país com a disparidade socioeconômica aflorada, seus anos de existência e sua grande quantidade populacional fazem com que a realidade em serviços básicos tenham suas próprias

particularidades. Segundo o IBGE [8], 7 em cada 10 brasileiros utilizam o SUS, correspondendo a 71,5% da população não contratante de planos de saúde particulares, causando problemáticas como a alta demanda do sistema público e, consequentemente, um alto volume de dados médicos na sua rede, e, o restante de 28,5% da população que adere a uso de sistemas particulares para suas consultas, que também necessitam de alguma forma para fins de segurança, terem seus dados armazenados de forma segura e com acessibilidade para tanto quanto clínicas particulares e/ou públicas. [8]

1.1 Objetivos

1.1.2 Objetivo Geral

Identificar as tendências de desenvolvimento de soluções baseadas em blockchain, identidade descentralizada e identidade auto-soberana na área de saúde e correlacionar com os empecilhos não necessariamente tecnológicos a essas soluções, a fim de desmistificar as aplicações da tecnologia no meio atual e a possível transferência do estado teórico para tempos futuros.

1.1.2 Objetivos Específicos

Os objetivos específicos do trabalho proposto são os seguintes :

1. Realizar uma revisão sistemática com intuito de contextualizar e compreender as tecnologias que suportam o tema como blockchain, identidade descentralizada e identidade auto-soberana.
2. Identificar as tendências e soluções correlacionadas já em progresso na área de saúde com ênfase na tecnologia.
3. Exemplificar a importância de usos de soluções seguras e que automatizam o sistema de saúde, principalmente o sistema de saúde brasileiro.
4. Analisar as referências sociais brasileiras e internacionais que impedem a possível utilização da tecnologia na área de saúde.

1.2 Pergunta de Pesquisa

Este trabalho tem como finalidade responder à seguinte pergunta de pesquisa: "Como identidade descentralizada, identidade auto-soberana e blockchain se relacionam com o contexto de saúde e como ela se alinha a resolver os problemas do sistema de saúde brasileiro?"

2. ANÁLISE BREVE SOBRE OS PILARES TECNOLÓGICOS RELACIONADOS

A DID emerge como uma solução inovadora na gestão de identidades digitais, prometendo transformar fundamentalmente as interações online e a segurança dos dados pessoais [17]. Neste contexto, é crucial compreender as tecnologias subjacentes que impulsionam a identidade descentralizada antes de entrarmos na sua própria definição.

2.1 Registros distribuídos

Baseado em análises sobre registros distribuídos e apoiados em definições como segundo a Universidade de Cambridge [9] a Tecnologia de Registro Distribuído (DLT) representa uma inovação que capacita a concepção, manutenção e aprimoramento de um repositório eletrônico compartilhado, efetuado por uma rede de intervenientes autônomos, desprovida de uma entidade centralizadora. Esses registros são salvaguardados por camadas de criptografia e são submetidos a um processo de consenso distribuído, o qual garante a sua integridade e resiliência contra eventuais tentativas de adulteração. O fruto desse procedimento é o "livro-razão"[1], que figura como a instância autoritativa dos registros. DLT pode ser empregada em uma ampla gama de dados, que vão desde transações de ativos digitais até referências a elementos externos ao sistema. Além disso, a DLT tem a capacidade de operar em ambientes hostis, tolerando a presença de agentes maliciosos ou não confiáveis, e pode exibir distintos níveis de descentralização, variando conforme as escolhas de desenho e arquitetura adotadas para o sistema [9].

Por sua vez, a British Standards Institution [10] ressalta que os DLT têm recebido crescente atenção como um método inovador de armazenar e atualizar dados entre organizações, diferenciando-se de redes e sistemas de contabilidade centralizados.

---

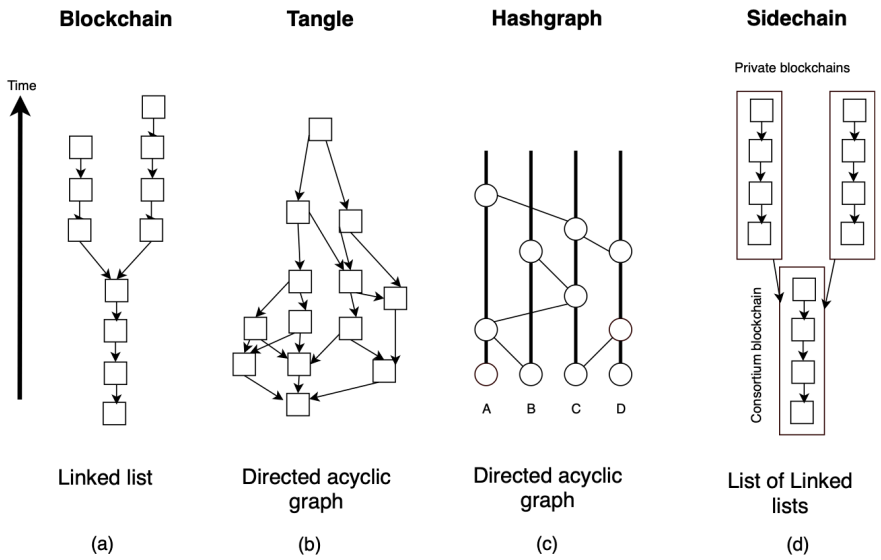
[1] No original: *ledger*

Em relação à segurança, Pahl e El Ioini [11] mencionam que um sistema de registros distribuídos pode garantir que a comunicação entre o provedor de certificação e o provedor de autenticação seja limitada ao que está registrado no ledger, o que contribui para a proteção dos dados.

Portanto, os registros distribuídos representam uma abordagem eficaz para garantir a integridade, segurança e descentralização dos dados, promovendo maior confiança e transparência nas transações e interações digitais.

A seguir temos a figura 4 que representa exemplos de estruturas de DLT em seu uso técnico.

Figura 4 - Representação visual de estruturas de um DLT



Fonte: Pahl e El Ioni [11]

Com esta definição em mente, podemos entender que DLT e Blockchain estão relacionados diretamente, com a ideia de que Blockchain é, sem exceção, um DLT, mas não vise-versa.

2.2 Blockchain

Blockchain é uma forma específica de DLT que ganhou destaque com a popularização da criptomoeda Bitcoin. Essa tecnologia consiste em uma cadeia de blocos de transações interligados e imutáveis, armazenados de forma descentralizada em diversos nós da rede. A característica fundamental dela é a sua capacidade de garantir a integridade e a segurança dos dados por meio de criptografia e consenso distribuído [10].

Conforme mencionado em [10], "A tecnologia Blockchain é uma das utilizações mais conhecidas da DLT, em que o livro-razão é composto por "blocos" de transacções, e é a tecnologia subjacente à criptomoeda Bitcoin.".[2] Essa citação destaca a associação intrínseca entre a tecnologia e Bitcoin, evidenciando a importância da tecnologia para a operação segura e transparente de criptomoedas.

O Blockchain pode ser entendido como uma estrutura em forma de "corrente" composta por blocos contendo dados, daí o nome "*block*" (bloco) e "*chain*" (corrente). Cada bloco representa um conjunto de transações e está criptograficamente ligado ao seu bloco anterior. Essa ligação é estabelecida por meio de uma identificação única de cada bloco utilizando um hash criptográfico. Os blocos subsequentes contêm, em suas informações, o hash do bloco anterior, formando assim uma sequência contínua de transações, uma "corrente" virtual.[12]

O mesmo é reconhecido como uma estrutura de dados compartilhada e um sistema descentralizado, distribuído e imutável, utilizado para armazenar uma lista crescente de transações provenientes de diversos sistemas. Sua aplicação mais conhecida é na área das criptomoedas, como o bitcoin. A sua gestão é realizada por uma rede de nós distribuídos, que verificam a validade de novos blocos utilizando técnicas de algoritmos de consenso. Estes algoritmos garantem que cada bloco seja único e que faça parte da corrente legítima, preservando as características mencionadas anteriormente e protegendo contra ataques diretos à corrente de blocos. [1,13]

Na tabela a seguir temos a descrição de termos utilizados frequentemente na definição do que é Blockchain para a compreensão melhor do tema.

Tabela 1: Tabela de termos frequentes na definição de blockchain.

(continua)

Termo	Descrição
Descentralizado	A rede descentralizada significa que não existe apenas um lugar onde a informação é armazenada. Há diversos bancos de dados (nós) e todos possuem a mesma informação. Se um dos nós deixar a rede, todos os outros já possuem a mesma informação, de forma inversa caso um novo nó seja inserido na rede, ele será uma cópia de todos os outros [14].

[2] No original: "Blockchain technology is one of the most well-known uses of DLT, in which the ledger comprises ‘blocks’ of transactions, and it is the technology that underlies the cryptocurrency Bitcoin"

Tabela 1: Tabela de termos frequentes na definição de blockchain.

(conclusão)

Transação	São informações que são armazenadas e empilhadas em cada bloco de acordo com o momento em que são processadas [14].
Transparência	Através de algoritmos de consenso, cada bloco ou transação que é adicionado à rede do blockchain não pode ser apagado e deve ser refletido e acreditado por todos os bancos de dados na rede [14].

Fonte: Adaptado de Mazonka [14].

Além disso, a tecnologia blockchain tem sido explorada em diversos setores além do financeiro. Como mencionado por Guo e Liang [15], "Blockchain Application and Outlook in the Banking Industry", a aplicação do blockchain vai além do setor financeiro, abrangendo potenciais usos em áreas como educação, indústrias criativas, agricultura e alimentação. Essa diversificação de aplicações demonstra a versatilidade e o potencial disruptivo do blockchain em diferentes contextos.

Em resumo, o blockchain representa uma inovação significativa no campo dos registros distribuídos, oferecendo segurança, transparência e confiabilidade para diversas aplicações, desde transações financeiras até a gestão de identidades digitais.

3. IDENTIDADE DESCENTRALIZADA

A identidade descentralizada é um conceito fundamental no campo da tecnologia da informação e da segurança cibernética, que visa fornecer aos usuários maior controle sobre seus dados pessoais e identidade digital [16, 17, 18]. Em contraste com os sistemas tradicionais de identidade centralizada, onde as informações dos usuários são armazenadas e gerenciadas por entidades centralizadas, a identidade descentralizada permite que os usuários tenham autonomia e propriedade sobre seus próprios dados. Neste contexto, a tecnologia de registros distribuídos desempenha um papel crucial, permitindo a criação de sistemas de identidade descentralizada seguros e eficientes [17, 19].

De acordo com Walid Fdhila et al [16], a capacidade dos indivíduos de criar e manter identidades não relacionadas é um direito humano fundamental e inalienável. Para que a

economia digital funcione de forma a apoiar esse direito humano, é essencial que os indivíduos possam controlar e limitar o que outros podem saber sobre eles em suas interações com serviços diversos. Nesse sentido, um dos principais objetivos da identidade descentralizada é garantir a privacidade e a autonomia dos usuários, permitindo-lhes gerenciar suas identidades de forma independente e segura.

Goodell e Aste [17] ressaltam a importância de permitir que os indivíduos gerenciem suas informações pessoais de maneiras diversas em diferentes contextos, defendendo a criação de identidades não relacionadas. Eles argumentam que os sistemas que incentivam a criação de uma única identidade centralizada podem restringir a liberdade dos usuários e influenciar seu comportamento. Portanto, a capacidade de manter múltiplas identidades não vinculadas é essencial para garantir a privacidade e a liberdade dos usuários em um ambiente digital em constante evolução.

Além disso, a identidade descentralizada se baseia em tecnologias de registros distribuídos, como blockchain, para garantir a segurança e integridade das informações dos usuários. Conforme mencionado por Walid Fdhila et al [16], a utilização de DLT possibilita a criação de identificadores descentralizados únicos e credenciais verificáveis (VC), que são fundamentais para estabelecer identidades confiáveis e autossuficientes. Essas tecnologias criptográficas garantem a autenticidade e a não adulteração das informações, protegendo os usuários contra fraudes e violações de dados.

Os componentes da identidade descentralizada são essenciais para a criação e gestão de identidades digitais auto suficientes e seguras. A seguir temos uma breve explicação dos mesmos:

1. **Identificadores Descentralizados**: São identificadores únicos associados a entidades digitais, como pessoas, organizações ou dispositivos. Os DID são criados e controlados pelos próprios usuários, permitindo a autogestão de identidades sem depender de autoridades centralizadas. Eles são fundamentais para estabelecer identidades digitais confiáveis e autossuficientes [16].
2. **Credenciais Verificáveis**: São declarações digitais que atestam informações sobre um indivíduo, como qualificações, afiliações ou histórico de transações. As VCs são emitidas por entidades confiáveis e podem ser verificadas por terceiros de forma independente. Elas permitem que os usuários compartilhem suas credenciais de forma segura e seletiva, mantendo o controle sobre suas informações pessoais [16].

3. **Documentos de Identidade Descentralizados**: São documentos associados aos DID que contêm informações sobre a entidade digital correspondente, como chaves públicas, serviços relacionados e métodos de autenticação. Os DID *Documents* são essenciais para validar a autenticidade e integridade das identidades descentralizadas, garantindo a confiabilidade das informações compartilhadas [16].
4. **Smart Contracts**: Em alguns casos, os smart contracts são utilizados para automatizar processos relacionados à identidade descentralizada, como a emissão e verificação de credenciais. Esses contratos inteligentes são executados automaticamente quando certas condições são atendidas, proporcionando eficiência e transparência às operações relacionadas à identidade digital [16].
5. **Agentes Autônomos**: São entidades digitais capazes de agir em nome dos usuários para interagir com sistemas e serviços de identidade descentralizada. Os agentes autônomos podem executar tarefas como solicitar e compartilhar credenciais, realizar transações e autenticar identidades de forma automatizada [16].
6. **Redes de Confiança**: São estruturas que permitem aos usuários estabelecer relações de confiança com outras entidades dentro do ecossistema de identidade descentralizada. Por meio de mecanismos criptográficos e protocolos de segurança, as redes de confiança garantem a autenticidade e integridade das interações entre os participantes [16].
7. **Protocolos de Comunicação Segura**: São padrões e protocolos de comunicação que garantem a segurança e privacidade das informações trocadas entre os diferentes componentes da identidade descentralizada. Estes protocolos incluem criptografia de ponta a ponta, autenticação de mensagens e proteção contra ataques cibernéticos [16].
8. **Interfaces de Usuário Amigáveis**: São interfaces gráficas ou aplicativos que permitem aos usuários interagir de forma intuitiva com seus dados de identidade descentralizada. As interfaces de usuário amigáveis facilitam a gestão e o compartilhamento de credenciais, garantindo uma experiência positiva para os usuários finais [16].

Após o detalhamento de seus componentes, uma DID tem sua estrutura definida por um formato específico e é composta por três partes principais: o esquema, o método e o identificador específico do método. Aqui está como um DID se parece e o que cada parte significa:

1. **Esquema**: O esquema indica o tipo de identificador utilizado e o contexto em que ele é aplicado. Por exemplo, um DID pode ser baseado em um esquema específico, como "did", que denota que se trata de um Identificador Descentralizado [16].
2. **Método**: O método descreve o protocolo ou sistema utilizado para criar e gerenciar o DID. Existem vários métodos disponíveis, como Sovrin, Bitcoin, Ethereum, entre outros, cada um com suas próprias especificações e funcionalidades [16].
3. **Identificador Específico do Método:** É a parte final do DID que identifica exclusivamente a entidade digital associada ao identificador. Esse identificador específico é único dentro do contexto do método utilizado e é usado para referenciar e localizar a entidade correspondente [16].

Em resumo, um DID é uma sequência de caracteres que segue a estrutura "Esquema:Método:Identificador Específico do Método" e é utilizado para representar de forma única e descentralizada uma entidade digital. Os DIDs são projetados para serem permanentes, resolvíveis e interoperáveis, permitindo que os usuários controlem suas identidades digitais de maneira autossuficiente e segura [16].

Outra característica técnica importante da identidade descentralizada é a ênfase na privacidade e na proteção dos dados pessoais dos usuários. Dib e Toumi [18] destacam a importância de preservar a privacidade dos usuários em sistemas de identidade descentralizada, evitando a vinculação excessiva de credenciais e informações pessoais. A abordagem descentralizada permite que os usuários compartilhem seletivamente suas informações, mantendo o controle sobre quem pode acessá-las e para quais fins.

Por fim, a identidade descentralizada apresenta características técnicas inovadoras que a tornam uma solução atraente para a gestão segura e auto suficiente da identidade digital. Por meio da utilização de tecnologias de registros distribuídos e da ênfase na privacidade dos usuários, a identidade descentralizada oferece uma abordagem promissora para enfrentar os desafios atuais relacionados à segurança e privacidade dos dados pessoais.

3.1 Desafios

Os DIDs apresentam uma série de desvantagens e desafios que podem impactar sua adoção e eficácia em sistemas de identidade descentralizada. Uma das principais preocupações está relacionada à complexidade técnica envolvida na implementação e gerenciamento de DID, exigindo conhecimentos especializados em criptografia e tecnologias distribuídas. Como apontado por Walid Fdhila et al [16], a complexidade pode dificultar a

compreensão e a utilização dos DIDs por parte de usuários menos familiarizados com esses conceitos. Além disso, a segurança dos DID é uma questão crítica, uma vez que a perda ou comprometimento das chaves criptográficas associadas pode resultar na inacessibilidade permanente das identidades digitais, levantando preocupações sobre a proteção dos dados pessoais dos usuários [16].

Em relação à escalabilidade, a crescente demanda por DIDs e transações na rede pode sobrecarregar os sistemas, causando atrasos e aumentando os custos operacionais, como destacado por Zhou et al [19]. A falta de padronização e interoperabilidade entre diferentes métodos de criação e resolução de DIDs também representa um desafio significativo, dificultando a integração e a comunicação eficaz entre os sistemas, conforme observado por Pahl e El Ioni[11].

Além disso, os custos de transação associados aos DIDs, especialmente em ambientes de blockchain, podem ser proibitivos em determinadas circunstâncias, impactando a viabilidade econômica e a acessibilidade dessas soluções [18]. Em suma, as desvantagens e problemas dos DIDs destacam a necessidade de abordar questões de segurança, escalabilidade, padronização e custos para promover uma adoção mais ampla e bem-sucedida dessas tecnologias inovadoras.

4. IDENTIDADE AUTO-SOBERANA

A SSI é uma inovação revolucionária que permite aos usuários possuir e gerenciar suas identidades digitais de maneira segura, privada e descentralizada. Segundo Toth e Anderson-Priddy [20], a SSI oferece uma nova perspectiva para a gestão de identidades, proporcionando aos usuários total controle sobre suas informações pessoais e eliminando a necessidade de intermediários centralizados.

Sendo assim, é necessário abordar como sua natureza se correlaciona com a DID e detalhar mais profundamente suas características.

4.1 Relação com DID e definição.

O conceito de Identidade Auto-Soberana (SSI) está intimamente relacionado aos DIDs, mas existem distinções importantes entre os dois. Enquanto os DIDs são identificadores únicos e auto suficientes que permitem que indivíduos e organizações controlem suas próprias identidades digitais, a SSI vai além, abrangendo todo o ecossistema

de identidade descentralizada e colocando o usuário no centro do controle de suas informações pessoais [17, 20].

Os DIDs são a espinha dorsal da SSI, atuando como identificadores únicos e autossuficientes para indivíduos e entidades. Eles facilitam a criação de relações de confiança diretas entre as partes. Além disso, as VCs são um componente crucial da SSI. Elas são equivalentes digitais de credenciais físicas, como passaportes e carteiras de motorista, que podem ser emitidas, compartilhadas e verificadas de maneira segura e autêntica [18, 20].

A SSI é projetada para proteger a privacidade dos usuários, prevenindo a divulgação desnecessária de informações pessoais e protegendo contra violações de dados. Através das Provas de Conhecimento Zero (ZKP), uma técnica criptográfica que permite a uma parte consiga provar a outra parte que uma determinada afirmação é verdadeira, sem revelar qualquer informação adicional além da veracidade da afirmação, os usuários podem comprovar a posse de informações sem revelar os dados subjacentes. Isso garante a confidencialidade e a integridade das transações de identidade [18, 20].

Existem várias soluções de SSI disponíveis atualmente, incluindo:

- Sovrin: Uma rede descentralizada baseada em blockchain que permite aos usuários possuir e controlar suas identidades digitais de forma auto suficiente e segura [18].
- Uport: Uma plataforma de identidade auto-soberana construída na blockchain Ethereum, que oferece aos usuários controle total sobre suas informações pessoais e credenciais digitais [18].
- SelfKey: Uma solução de identidade auto-soberana que utiliza a blockchain Ethereum para permitir que os usuários gerenciem e compartilhem suas identidades de forma segura e descentralizada [18].

Esses exemplos ilustram como as tecnologias de SSI estão sendo implementadas em diferentes plataformas e redes blockchain para capacitar os usuários a terem controle total sobre suas identidades digitais, seguindo os princípios de segurança, privacidade e descentralização.

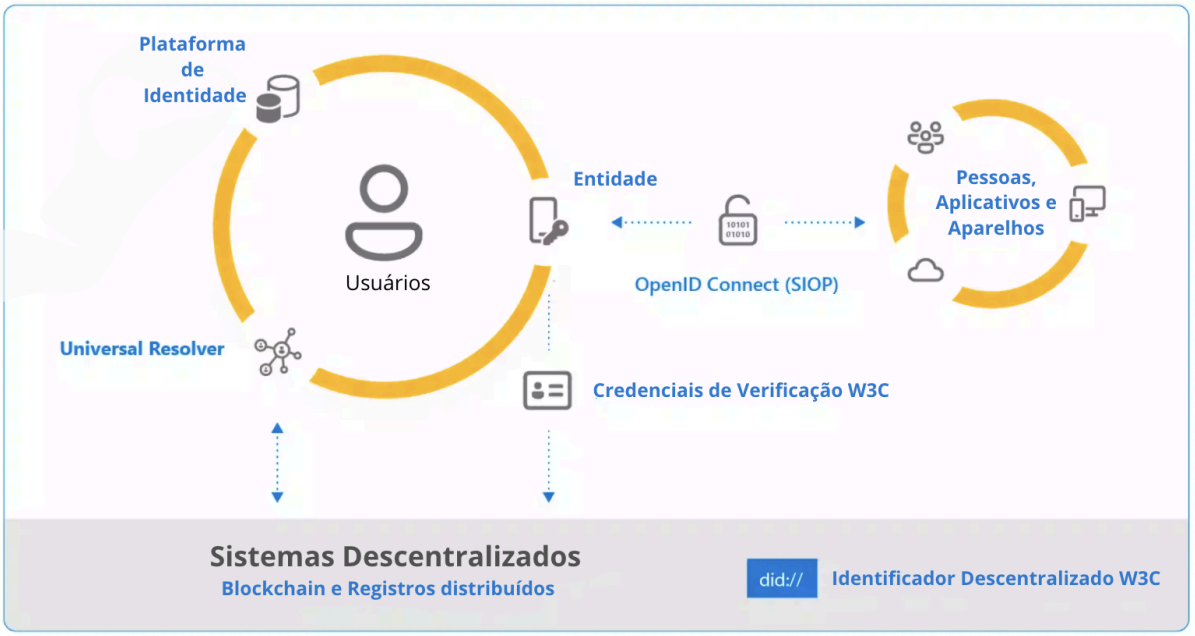
O modelo em camadas da Identidade Auto-Soberana é composto por diversas camadas que representam as diferentes operações e componentes envolvidos no sistema. Segundo Bahya Nassr Eddine et al [21], as camadas do SSI são:

- **Camada de Governança**: Esta camada engloba os frameworks de governança que estabelecem políticas, requisitos, princípios e padrões que tornam o sistema SSI seguro e confiável.
- **Camada de Credenciais e Reivindicações**: Aqui, todas as operações relacionadas ao ciclo de vida das credenciais e reivindicações são realizadas, como solicitação, emissão, assinatura, armazenamento, divulgação, verificação, revogação e expiração.
- **Camada de Autenticação**: Esta camada descreve os métodos para autenticar entidades usando seus DIDs.
- **Camada de Resolução**: Nesta camada, a resolução do DID para o documento associado pode ser realizada por meio de um método de resolução nativo definido em uma especificação de método DID ou através do DIF Universal Resolver, que é um utilitário desenvolvido pela comunidade no DIF para resolver DIDS em muitos métodos DID diferentes, com base nas especificações da World Wide Web Consortium (W3C).
- **Camada de Operações**: Esta camada define como as operações CRUD[3] definidas na especificação de método DID são executadas.
- **Camada Blockchain**: Esta camada consiste em um registro descentralizado de informações. Um blockchain compatível com o padrão DID tem um método DID associado que governa como os DIDs são ancorados no registro. O método DID pode separar o armazenamento do DID e do Documento DID do blockchain, sendo esse armazenamento tratado fora do blockchain.

Essas camadas são fundamentais para o funcionamento e a segurança de um sistema SSI, assegurando a autenticidade, integridade e privacidade das identidades digitais. A figura a seguir apresenta uma representação visual do fluxo de comunicação em um SSI.

[3] A sigla CRUD é o acrônimo dos seguintes termos: Create, Read, Update, Delete. Sua tradução seria, em ordem: Criar, Ler, Atualizar e Deletar.

Figura 5 - Representação visual de fluxo de SSI



Fonte: Adaptado de Microsoft [22]

Em resumo, a SSI representa uma nova abordagem para a gestão de identidades digitais, colocando os usuários no controle de suas informações e promovendo a segurança, a privacidade e a descentralização no ecossistema digital.

5. METODOLOGIA

Este capítulo delineia a metodologia empregada neste Trabalho de Conclusão de Curso, com ênfase na revisão da literatura como principal método de investigação. A escolha deste tema direcionou a adoção desta metodologia, dada a relevância do estudo, que, apesar de amplamente acessível no setor técnico e tecnológico, especialmente no que diz respeito à identidade descentralizada e blockchain, ainda carece de uma abordagem direta no contexto brasileiro.

Esta lacuna apresentou-se como uma oportunidade para este trabalho ser uma referência pioneira e inovadora, incentivando pesquisas e análises deste nicho tecnológico com foco na resolução de problemas específicos do Brasil.

5.1 Estudos Relacionados

O ponto de partida para a elaboração desta revisão consistiu em uma investigação abrangente nos principais periódicos internacionais, com o objetivo de identificar publicações que já abordaram o tema de forma sistemática. Embora a existência de Revisões Sistemáticas da Literatura (RSL) sobre o tema das tecnologias tenha sido satisfatoriamente encontrada, a justificativa para este trabalho reside na correlação do uso e aplicação desta RSL dessas tecnologias para auxiliar a compreensão do contexto brasileiro.

5.2 Etapas da Revisão

Este trabalho adota a revisão sistemática como principal método de investigação. A revisão sistemática é um processo rigoroso e estruturado que envolve várias etapas, descritas a seguir:

5.2.1 Formulação da Pergunta de Pesquisa

A primeira etapa deste trabalho envolve a formulação de uma pergunta de pesquisa precisa e relevante, que orienta o escopo da revisão. Para formular uma pergunta de pesquisa que tenha um impacto significativo sobre o tema, é essencial compreender as necessidades que deram origem a ela.

O autor identificou uma demanda na área de tecnologia de blockchain com ênfase em saúde, decorrente de sua experiência prévia no setor, tanto profissional quanto acadêmica. Essa demanda foi corroborada principalmente por notícias sobre problemas relacionados à perda de dados, vazamento de informações sensíveis e tentativas de integração de redes no sistema de saúde brasileiro.

Portanto, um conjunto de perguntas de pesquisa foi meticulosamente elaborado e refinado. A partir de uma pergunta de pesquisa bem definida, é possível orientar o estudo, coletar evidências, estabelecer relações entre tópicos e formular conclusões baseadas nos dados.

A formulação de uma pergunta de pesquisa necessitou de uma análise preliminar do tema para descobrir possíveis áreas não exploradas e confirmar a presença de estudos recentes, minuciosos e bem organizados relacionados ao assunto.

Dessa forma, a pergunta de pesquisa proposta foi: "Qual é a natureza da identidade descentralizada e da identidade auto-soberana, e como essas tecnologias podem contribuir para a resolução dos problemas do sistema de saúde brasileiro?"

Para auxiliar na resposta à pergunta de pesquisa principal, foram formuladas as seguintes Perguntas de Pesquisa Secundárias (PPS):

1. Quais os termos técnicos mais frequentes no contexto de blockchain, identidade descentralizada e identidade auto-soberana no setor de saúde?
2. Como a identidade descentralizada, blockchain e identidade auto-soberana podem ser aplicadas no setor de saúde?
3. Quais os desafios enfrentados pela aplicação dessas tecnologias no contexto de saúde?

5.2.2 Elaboração do Protocolo de Revisão

O protocolo de revisão é desenvolvido para detalhar o plano da revisão. Ele inclui os critérios de inclusão e exclusão dos estudos, as bases de dados a serem pesquisadas e os métodos de análise dos estudos.

Este estudo utilizou uma lista de repositórios de referência para coletar os artigos analisados. A tabela 2 a seguir mostra os mesmos:

Tabela 2 - Nomes dos repositórios

Nome
IEEE
ACM
Science Direct

Fonte: O autor.

Após a seleção de repositórios, foi necessário a definição de uma seleção de palavras chaves para poder ter uma assertividade dos artigos desejados.

Tabela 3 - Lista de palavras chaves

(continua)

Palavra-Chave EN
Blockchain
Decentralized Identity
Self Sovereign Identity

Tabela 3 - Lista de palavras chaves

(conclusão)

Health
Records
Data

Fonte: O autor.

Após isto, também foi executado uma string de busca para os repositórios citados, garantindo uma maior filtragem dos artigos e facilitando a análise.

A string executada possui condicionais booleanos (OR e AND) no intuito de gerar buscas distintas com uma combinação das palavras-chaves utilizadas para dar maior gama de busca e combinações disponíveis ao contexto do trabalho e a formatação da string de busca não necessariamente utilizou a palavra chave em sua forma original, mas sim em contextos para facilitar uma melhor assertividade.

Tabela 4 - String de busca para resgate dos artigos

String de busca
*((blockchain **OR** "decentralized identity" **OR** "self-sovereign identity") **AND** (health **OR** "health records" **OR** "health data" **OR** "healthcare"))*

Fonte: O autor.

5.2.3 Seleção dos Estudos

Os estudos identificados são avaliados com base nos critérios de inclusão e exclusão definidos no protocolo.

Alguns critérios de inclusão e de exclusão foram definidos baseados na necessidade do trabalho, no sentido de inclusão todos os artigos que envolviam as palavras chaves relacionados a tecnologia foram definidas em limitações de artigos na língua inglesa como principal para fontes técnicas sobre a tecnologia analisada em si. Também foi limitado ao uso de artigos com acessos abertos, tanto gratuitos como também artigos permitidos pela VPN do Centro de Informática, que no momento da realização deste trabalho, também eram gratuitos. Adicionalmente também foi limitado um período de ano entre 2018 e 2023, para garantir o reflexo mais atual das pesquisas.

A exclusão dos artigos foram definidas em certas limitações, em sua grande maioria anti-complementar ao critério de inclusão, como artigos diferentes da língua inglesa, artigos anteriores ao ano de 2018, artigos pagos e qualquer artigo sobre blockchain, identidade descentralizada e identidade auto-soberana que não tivesse relação com saúde.

Tabela 5 - Critérios de inclusão e exclusão de artigos

ID	Critérios de Inclusão	Critérios de Exclusão
CI1/CE1	Artigos abertos	Artigos pagos
CI2/CE2	Artigos na língua inglesa.	Qualquer artigo que não seja da língua inglesa.
CI3/CE3	Artigos entre 2018 e 2023	Artigos abaixo de 2018 ou superior a 2023
CI4/CE4	Artigos relacionados com o tema.	Artigos com relação desconexa com o tema.
CI5/CE5	Artigos primários	Artigos secundários (RSL e outros)

Fonte: O autor.

Com os critérios definidos, a próxima fase consistiu na busca e filtro nos repositórios citados para a construção do trabalho. Para a seleção dos artigos para este trabalho, foram elaborados dois filtros iniciais, como uma forma de peneirar a ampla quantidade de artigos publicados. Na tabela 6 à frente é possível observar os filtros desenvolvidos:

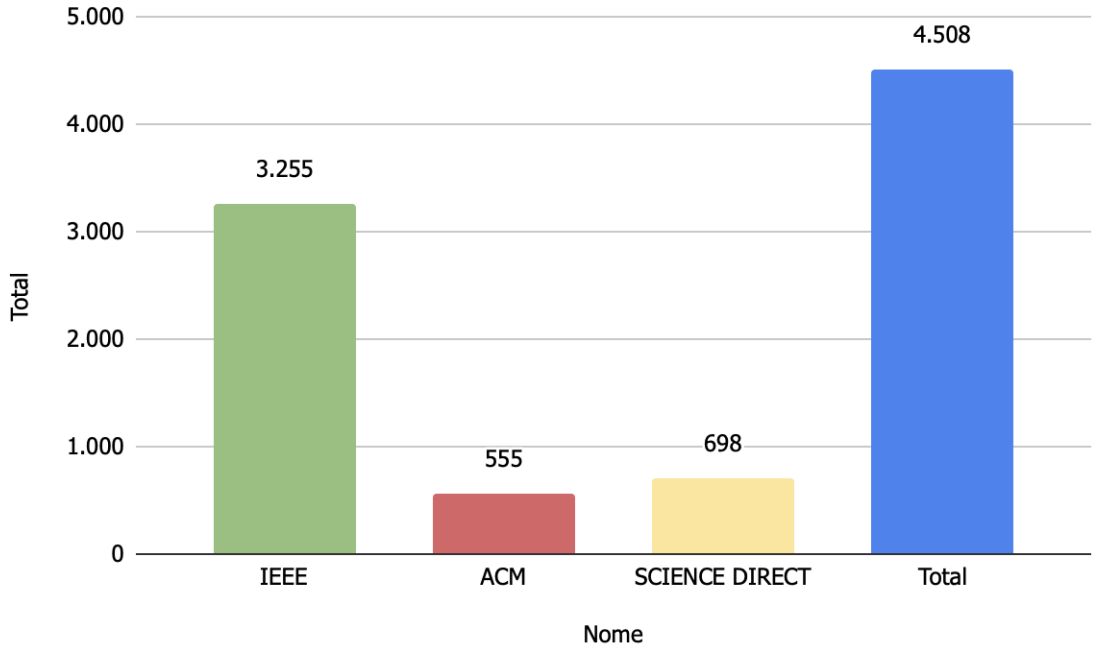
Tabela 6 - Filtros de artigos

ID	Filtros
F1	Leitura do título e do resumo
F2	Leitura da introdução e da conclusão

Fonte: O autor.

O processo de identificação de estudos iniciou com uma pesquisa simples, apenas direcionado pela string de busca nas bases utilizando o princípio de busca por metadados padrões (título, *abstract* e palavras-chave) com a data até a publicação deste estudo (março, 2024).

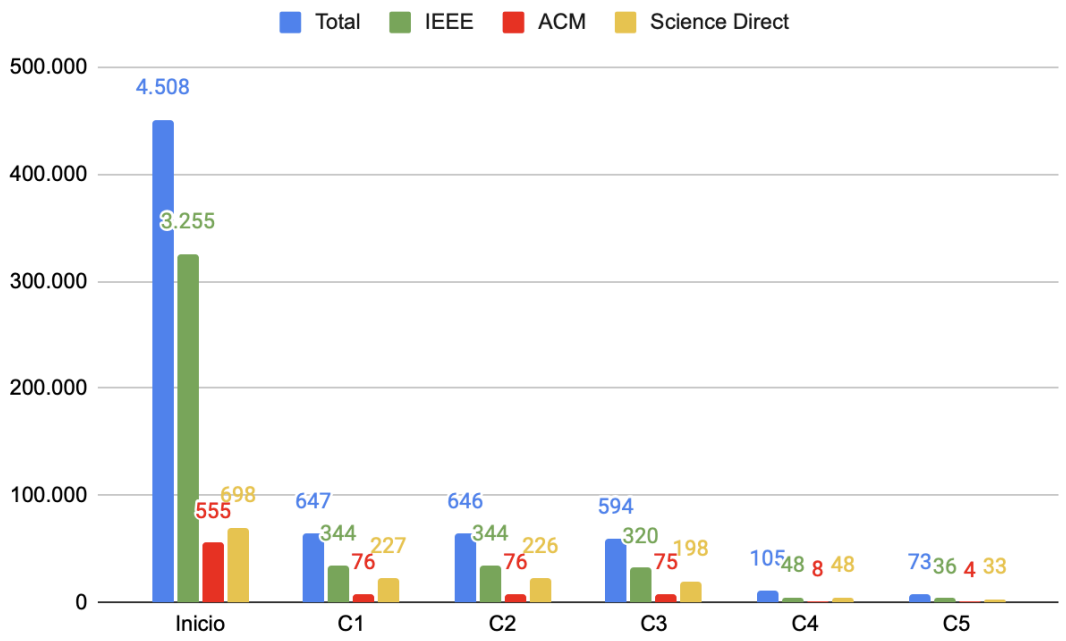
Figura 6 - Total de artigos iniciais



Fonte: O autor.

Após a visualização das bases de estudos de forma geral, foi iniciado o processo de aplicação dos CE para diminuir o quantitativo de estudos e limitar a pesquisa.

Figura 7 - Representação visual de fluxo de SSI



Fonte: O autor.

Após a análise dos artigos, os mesmos foram avaliados entre cinco tópicos, avaliado em uma escala com três componentes: 0 representa "inadequado"; 0,5 representa "parcialmente adequado"; 1 representa "adequado". Foram selecionados aqueles artigos cuja nota era maior ou igual a 3

.

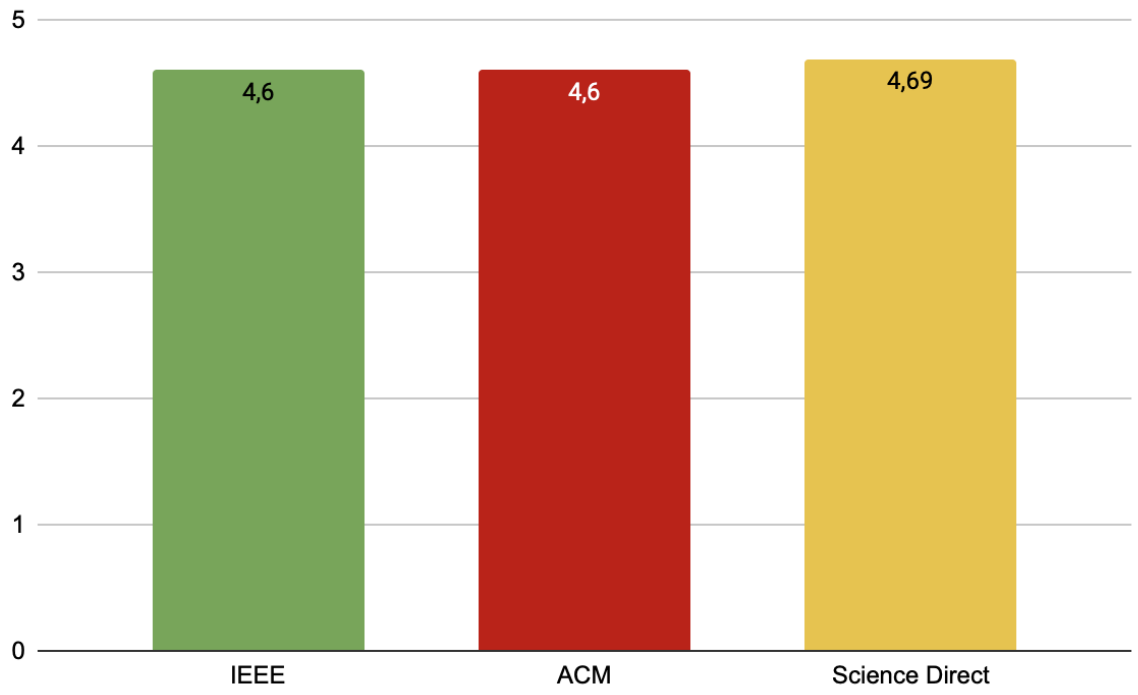
Tabela 7 - Tópicos de avaliação dos artigos

Tópicos de avaliação
Contexto Claro
Metodologia bem definida
Aplicação prática
Discussões relevantes e consistentes
Tendências de pesquisas futuras

Fonte: O autor.

Após qualificar todos os artigos, a figura 8 demonstra as médias das notas (com o máximo de 5) de cada repositório de acordo com os artigos coletados.

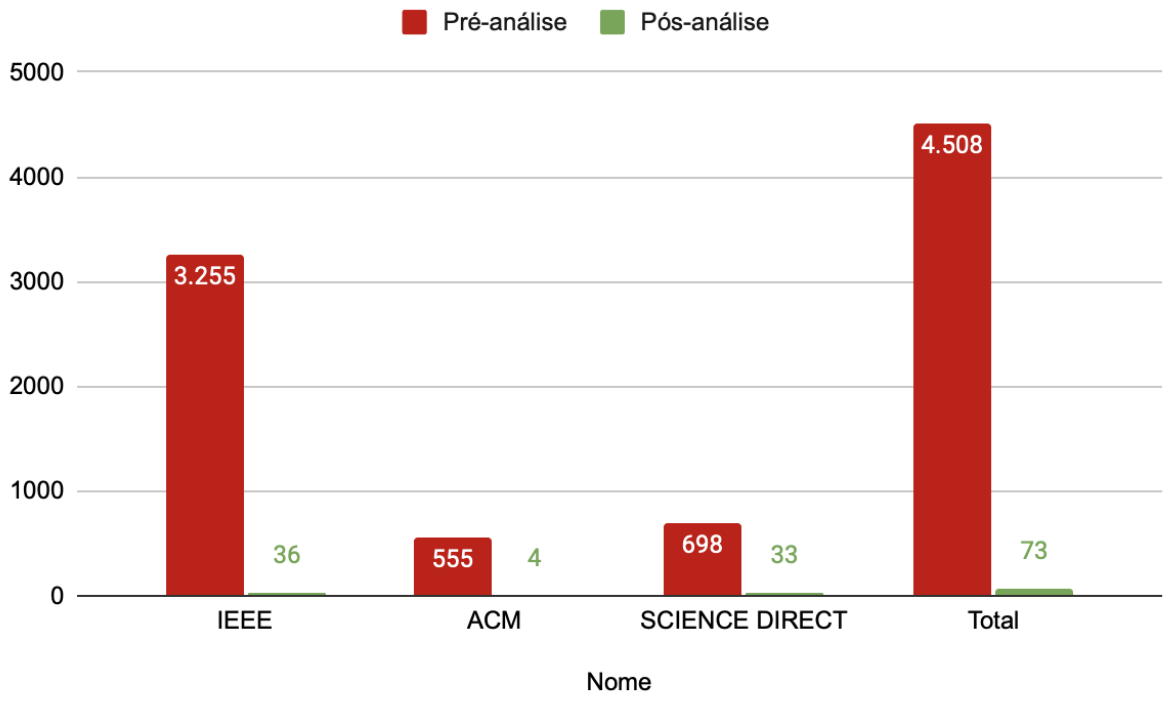
Figura 8 - Média das notas de qualificação



Fonte: O autor

E, após aplicar todos os CE, filtros e análises, a distribuição restante de quantidade de artigos de cada um dos repositórios tem a seguinte visualização como demonstrado na figura 9:

Figura 9 - Comparação de pré e pós análise.



Fonte: O autor.

Após toda esta análise, os estudos aprovados e selecionados para a composição deste trabalho podem ser vistos na tabela 8 a seguir:

Tabela 8 - Lista de artigos aprovados

(continua)

REF	ES	Título	Autores	Ano	REP
25	1	Authenticated Range Querying of Historical Blockchain Healthcare Data using Authenticated Multi-Version Index	Shlomi Linoy, Suprio Ray, Natalia Stakhanova, Erik Scheme	2023	ACM
26	2	Blockchains for Government: Use Cases and Challenges	James Clavin, Sisi Duan, Haibin Zhang, Vandana P. Janeja, Karuna P. Joshi, Yelena Yesha, Lucy C. Erickson, Justin D. Li	2020	ACM

Tabela 8 - Lista de artigos aprovados

(continua)

27	3	Scrybe: A Secure Audit Trail for Clinical Trial Data Fusion	Jonathan Oakley, Carl Worley, Lu Yu, Richard R. Brooks, İlker Özçelik, Anthony Skjellum, Jihad S. Obeid	2022	ACM
28	4	Permissioned Blockchains: Properties, Techniques and Applications	Mohammad Javad Amiri, Divyakant Agrawal, Amr El Abbadi	2021	ACM
29	5	Secure decentralized electronic health records sharing system based on blockchains	Khaled Shuaib, Juhar Abdella, Farag Sallabi, Mohamed Adel Serhani	2022	Science Direct
30	6	ChainSure: Agent free insurance system using blockchain for healthcare 4.0	Amiya Karmakar, Pritam Ghosh, Partha Sarathi Banerjee, Debashis De	2023	Science Direct
31	7	A blockchain-based fine-grained data sharing scheme for e-healthcare system	Gaofan Lin, Haijiang Wang, Jian Wan, Lei Zhang, Jie Huang	2022	Science Direct
32	8	Data exchanges based on blockchain in m-Health applications	Antonio Clim, Răzvan Daniel Zota, Radu Constantinescu	2019	Science Direct
33	9	A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods	Luca Brunese, Francesco Mercaldo, Alfonso Reginelli, Antonella Santone	2019	Science Direct
34	10	Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations	Efthymios Chondrogiannis, Vassiliki Andronikou, Efstathios Karanastasis, Antonis Litke, Theodora Varvarigou	2022	Science Direct
35	11	Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0	Mohit Kumar, Hritu Raj, Nisha Chaurasia, Sukhpal Singh Gill	2023	Science Direct
36	12	Analyzing the performance of a blockchain-based personal health record implementation	Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, José Roberto Goldim, Douglas C. Schmidt	2019	Science Direct
37	13	Permissioned Blockchain Approach using Open Data in Healthcare	João Cunha, Ricardo Duarte, Tiago Guimarães, Manuel Filipe Santos	2022	Science Direct

Tabela 8 - Lista de artigos aprovados

(continua)

38	14	A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system	Prabhat Kumar, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, Alireza Jolfaei, A.K.M. Najmul Islam	2023	Science Direct
39	15	Monetisation of digital health data through a GDPR-compliant and blockchain enabled digital health data marketplace: A proposal to enhance patient's engagement with health data repositories	Mohamed Maher, Imtiaz Khan, Verma Prikshat	2023	Science Direct
40	16	Blockchain-powered distributed data auditing scheme for cloud-edge healthcare system	Yi Li a, Meiqin Tang	2023	Science Direct
41	17	Care4U: Integrated healthcare systems based on blockchain	Randa Kamal, Ezz El-Din Hemdan, Nawal El-Fishway	2023	Science Direct
42	18	Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare	Yinghui Zhang, Xuanni Wei, Jin Cao, Jianting Ning, Zuobin Ying, Dong Zheng	2022	Science Direct
43	19	Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study	Sara Ait Bennacer, Abdessadek Aaroud, Khadija Sabiri, Mohamed Amine Rguibi, Bouchaib Cherradi	2022	Science Direct
44	20	HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system	Sireejaa Uppal, Bindiya Kansekar, S. Mini, Deepak Tosh	2023	Science Direct
45	21	Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis	Mark Foy, Dolores Martyn, Debra Daly, Aoife Byrne, Chinwe Aguneche, Rob Brennan	2022	Science Direct
46	22	BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten	Eugenio Balistri, Francesco Casellato, Carlo Giannelli, Cesare Stefanelli	2021	Science Direct
47	23	Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing	Ya Gao, Aiqing Zhang, Shu Wu, Jindou Chen	2022	Science Direct
48	24	BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security	Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi	2022	Science Direct
49	25	A blockchain-enabled sharing platform for personal health records	Yibin Dong, Seong K. Mun, Yue Wang	2023	Science Direct

Tabela 8 - Lista de artigos aprovados

(continua)

50	26	A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case	Sabri Barbaria, Halima Mahjoubi, Hanene Boussi Rahmouni	2023	Science Direct
51	27	Designing Personalized Integrated Healthcare Monitoring System through Blockchain and IoT	Gunawan Wang, Aldian Nurcahyo	2023	Science Direct
52	28	Preserving the Privacy of Electronic Health Records using Blockchain	Yogesh Sharma, B. Balamurugan	2020	Science Direct
53	29	Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation	K.A. Koshechkin, G.S. Klimenko, I.V. Ryabkov, P.B. Kozhin	2018	Science Direct
54	30	Blockchain Analytics - Real-time Log Management in Healthcare	Tiago Guimarães, Ricardo Duarte, Bruno Pinheiro, Daniel Faria, Paulo Gomes, Manuel Filipe Santos	2022	Science Direct
55	31	Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology	Yan Zhuang, Chi-Ren Shyu, Shenda Hong, Pengfei Li, Luxia Zhang	2023	Science Direct
56	32	Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain	Sarath Sabu, H.M. Ramalingam, M Vishaka, H.R. Swapna, Swaraj Hegde	2021	Science Direct
57	33	The case of HyperLedger Fabric as a blockchain solution for healthcare applications	McSeth Antwi, Asma Adnane, Farhan Ahmad, Rasheed Hussain, Muhammad Habib ur Rehman, Chaker Abdelaziz Kerrache	2021	Science Direct
58	34	A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique	Abdur Rehman, Sagheer Abbas, M.A. Khan, Taher M. Ghazal, Khan Muhammad Adnan, Amir Mosavi	2022	Science Direct
59	35	An efficient privacy-preserving control mechanism based on blockchain for E-health applications	Hanan Naser Alsuqaih, Walaa Hamdan, Haythem Elmessiry, Hussein Abulkasim	2023	Science Direct
60	36	Secured Health Data Sharing System using IPFS and Blockchain with Beacon Proxy	Dr. S. Jayanthy, A. Arunkumar, Mr. J. Judeson Antony Kovilpillai, M. Bhuvardhena, K. Dinesh Pandian	2023	Science Direct

Tabela 8 - Lista de artigos aprovados

(continua)

61	37	A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions	Alexander Garrido, Leonardo Juan Ramírez López, Nicolás Beltrán Álvarez	2021	Science Direct
62	38	Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems	R. Guo; H. Shi; Q. Zhao; D. Zheng	2018	IEEE
63	39	An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records	F. Tang; S. Ma; Y. Xiang; C. Lin	2019	IEEE
64	40	Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable	S. Wang; D. Zhang; Y. Zhang	2019	IEEE
65	41	Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain	S. Niu; L. Chen; J. Wang; F. Yu	2019	IEEE
66	42	Lightweight Blockchain for Healthcare	L. Ismail; H. Materwala; S. Zeadally	2019	IEEE
67	43	Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems	D. C. Nguyen; P. N. Pathirana; M. Ding; A. Seneviratne	2019	IEEE
68	44	EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain	A. R. Rajput; Q. Li; M. Taleby Ahvanooey; I. Masood	2019	IEEE
69	45	Using Blockchain for Electronic Health Records	A. Shahnaz; U. Qamar; A. Khalid	2019	IEEE
70	46	EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange	R. Akkaoui; X. Hei; W. Cheng	2020	IEEE
71	47	Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain	A. E. B. Tomaz; J. C. D. Nascimento; A. S. Hafid; J. N. De Souza	2020	IEEE
72	48	Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach	M. A. Rahman; M. S. Hossain; M. S. Islam; N. A. Alrajeh; G. Muhammad	2020	IEEE
73	49	Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records	M. Zarour; M. T. J. Ansari; M. Alenezi; A. K. Sarkar; M. Faizan; A. Agrawal; R. Kumar; R. A. Khan	2020	IEEE
74	50	A Consent Model for Blockchain-Based Health Data Sharing Platforms	V. Jaiman; V. Urovi	2020	IEEE

Tabela 8 - Lista de artigos aprovados

(continua)

75	51	A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems	X. Xiang; M. Wang; W. Fan	2020	IEEE
76	52	A Patient-Centric Health Information Exchange Framework Using Blockchain Technology	Y. Zhuang; L. R. Sheets; Y. -W. Chen; Z. -Y. Shae; J. J. P. Tsai; C. -R. Shyu	2020	IEEE
77	53	SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities	M. Zghaibeh; U. Farooq; N. U. Hasan; I. Baig	2020	IEEE
78	54	A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain	A. Musamih; K. Salah; R. Jayaraman; J. Arshad; M. Debe; Y. Al-Hammadi; S. Ellahham	2021	IEEE
79	55	MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address	D. Lee; M. Song	2021	IEEE
80	56	Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations	G. Subramanian; A. Sreekantan Thampy	2021	IEEE
81	57	Development of an Internet-of-Healthcare System Using Blockchain	S. Yongjoh; C. So-In; P. Kompunt; P. Muneesawang; R. I. Morien	2021	IEEE
82	58	Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective	Y. Liu; G. Shan; Y. Liu; A. Alghamdi; I. Alam; S. Biswas	2022	IEEE
83	59	Integrating Healthcare Services Using Blockchain-Based Telehealth Framework	N. Z. Bawany; T. Qamar; H. Tariq; S. Adnan	2022	IEEE
84	60	A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain	A. G. Alzahrani; A. Alhomoud; G. Wills	2022	IEEE
85	61	Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm	Z. Pang; Y. Yao; Q. Li; X. Zhang; J. Zhang	2022	IEEE
86	62	DDMIA: Distributed Dynamic Mutual Identity Authentication for Referrals in Blockchain-Based Health Care Networks	M. Hegde; R. R. Rao; B. M. Nikhil	2022	IEEE
87	63	Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test	Y. S. Bae; Y. Park; S. M. Lee; H. H. Seo; H. Lee; T. Ko; E. Lee; S. M. Park; H. -J. Yoon	2022	IEEE

Tabela 8 - Lista de artigos aprovados

(conclusão)

88	64	Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs	A. Alnuaimi; A. Alshehhi; K. Salah; R. Jayaraman; I. A. Omar; A. Battah	2022	IEEE
89	65	DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data	H. Saidi; N. Labraoui; A. A. A. Ari; L. A. Maglaras; J. H. M. Emati	2022	IEEE
90	66	A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT	A. N. Gohar; S. A. Abdelmawgoud; M. S. Farhan	2022	IEEE
91	67	A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain	R. P. Pinto; B. M. C. Silva; P. R. M. Inácio	2022	IEEE
92	68	A Blockchain Based System for Healthcare Digital Twin	S. S. Akash; M. S. Ferdous	2022	IEEE
93	69	Sec-Health: A Blockchain-Based Protocol for Securing Health Records	L. D. Costa; B. Pinheiro; W. Cordeiro; R. Araújo; A. Abelém	2023	IEEE
94	70	Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System	T. Haritha; A. Anitha	2023	IEEE
95	71	Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS	A. Bisht; A. K. Das; D. Niyato; Y. Park	2023	IEEE
96	72	Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications	S. Thapliyal; M. Wazid; D. P. Singh; A. K. Das; S. Shetty; A. Alqahtani	2023	IEEE
97	73	Trustworthy Healthcare Professional Credential Verification Using Blockchain Technology	A. Alnuaimi; D. Hawashin; R. Jayaraman; K. Salah; M. Omar	2023	IEEE

Fonte: O autor

6. RESULTADOS

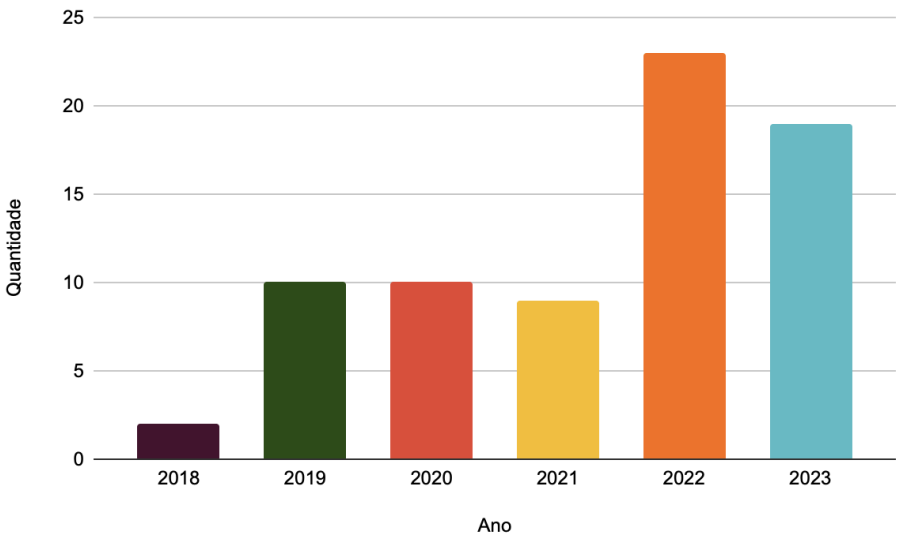
Após todas as etapas anteriores a seleção culminou na lista de 74 artigos aprovados, distribuídos entre as bases selecionadas previamente. Diante desta lista, o estudo pode iniciar sua interpretação de cada um dos estudos colhidos e seus respectivos impactos.

6.1 Interpretação dos Resultados e Redação do Relatório

Os resultados da revisão são interpretados no contexto da pergunta de pesquisa, e um relatório detalhado da revisão é escrito. Cada revisão sistemática é única e pode exigir etapas adicionais dependendo do tópico e da pergunta de pesquisa. Este plano garante a qualidade e a confiabilidade dos resultados.

Ao analisar as informações bases dos estudos selecionados, percebemos a seguinte distribuição por anos entre os estudos na figura 10:

Figura 10 - Distribuição de artigos por ano de publicação

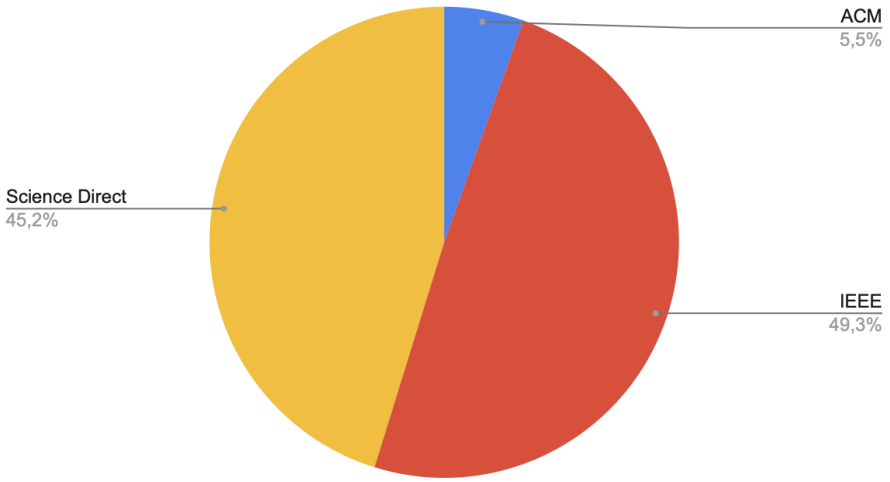


Fonte: O autor.

Os números de estudos foram crescendo ao longo dos anos, demonstrando uma estabilidade e uma característica de que o tema tem sido mais relevante ao passar do tempo. Outro indicativo desse gráfico é o número de alta discrepante entre os anos de 2020/2021 para 2022/2023, após o fim da Pandemia do Covid-19, esse tema se tornou ainda mais importante devido a sua característica de impacto direta no setor de saúde e dados.

A distribuição por bases, demonstrada pela a figura 11 a seguir, mostra um equilíbrio entre as duas principais, Science Direct e IEEE, com menos participação da ACM.

Figura 11 - Porcentagem de participação de cada repositório



Fonte: O autor.

Após todas as etapas anteriores, chegou o momento de avaliar os estudos em busca de responder às perguntas de pesquisa.

6.2 Perguntas de Pesquisa

6.2.1 PPS1. Quais os termos técnicos mais frequentes no contexto de blockchain, identidade descentralizada e identidade auto-soberana no setor de saúde?

Ao iniciarmos a avaliação dos estudos, foi necessário a construção de conhecimento referente a quais os termos mais utilizados na construção da área da tecnologia com a ênfase no setor de saúde. Ao decorrer da literatura, foi identificado alguns termos importantes na concepção que engloba quase toda a sua definição e aplicabilidade em contexto, sendo eles: 1. Interoperabilidade, 2. Privacidade, 3. Dados, 4. Segurança, 5.Transparência, 6. Integridade. Na tabela 9 a seguir temos a distribuição dos termos encontrados e os respectivos estudos:

Tabela 9 - Termos frequentes e estudos relacionados

(continua)

Conceitos	Estudos
Interoperabilidade	[ES2], [ES6], [ES7], [ES9], [ES11], [ES12], [ES13], [ES16], [ES19], [ES25], [ES26], [ES27], [ES29], [ES32], [ES33], [ES34], [ES35], [ES37], [ES41], [ES42], [ES44], [ES45], [ES47], [ES51], [ES53], [ES54], [ES55], [ES56], [ES57], [ES58], [ES59], [ES61], [ES62], [ES63], [ES64], [ES65], [ES67], [ES68], [ES69], [ES71], [ES72], [ES73]

Tabela 9 - Termos frequentes e estudos relacionados

(conclusão)

Privacidade	[ES2], [ES5], [ES6], [ES9], [ES10], [ES16], [ES17], [ES19], [ES20], [ES22], [ES24], [ES25], [ES26], [ES27], [ES28], [ES29], [ES30], [ES31], [ES32], [ES34], [ES35], [ES36], [ES37], [ES38], [ES39], [ES40], [ES41], [ES43], [ES44], [ES45], [ES46], [ES47], [ES48], [ES51], [ES52], [ES53], [ES55], [ES56], [ES58], [ES59], [ES60], [ES61], [ES62], [ES64], [ES65], [ES66], [ES67], [ES70], [ES71], [ES72], [ES73]
Dados	[ES1], [ES2], [ES5], [ES7], [ES9], [ES10], [ES11], [ES17], [ES19], [ES20], [ES25], [ES27], [ES28], [ES29], [ES30], [ES31], [ES32], [ES33], [ES34], [ES37], [ES40], [ES42], [ES43], [ES44], [ES46], [ES48], [ES49], [ES51], [ES53], [ES54], [ES55], [ES56], [ES61], [ES65], [ES67], [ES69]
Segurança	[ES1], [ES2], [ES5], [ES6], [ES7], [ES9], [ES10], [ES11], [ES12], [ES13], [ES17], [ES19], [ES20], [ES21], [ES22], [ES24], [ES25], [ES26], [ES27], [ES28], [ES29], [ES30], [ES31], [ES32], [ES33], [ES34], [ES35], [ES36], [ES37], [ES40], [ES43], [ES43], [ES44], [ES45], [ES46], [ES47], [ES48], [ES49], [ES51], [ES52], [ES53], [ES54], [ES55], [ES56], [ES57], [ES58], [ES59], [ES60], [ES62], [ES63], [ES64], [ES65], [ES66], [ES67], [ES68], [ES69], [ES70], [ES71], [ES72], [ES73]
Integridade	[ES1], [ES2], [ES6], [ES10], [ES13], [ES16], [ES17], [ES21], [ES22], [ES25], [ES26], [ES29], [ES30], [ES32], [ES33], [ES35], [ES36], [ES37], [ES40], [ES41], [ES43], [ES46], [ES47], [ES48], [ES51], [ES52], [ES54], [ES57], [ES60], [ES61], [ES63], [ES65], [ES67], [ES68], [ES69], [ES71], [ES72], [ES73]
Transparência	[ES1], [ES7], [ES17], [ES28], [ES29], [ES32], [ES36], [ES37], [ES44], [ES46], [ES52], [ES54], [ES56], [ES66], [ES67], [ES69], [ES72], [ES73]
Autenticação	[ES1], [ES2], [ES6], [ES7], [ES9], [ES10], [ES11], [ES19], [ES20], [ES29], [ES30], [ES32], [ES33], [ES34], [ES35], [ES36], [ES37], [ES43], [ES44], [ES45], [ES47], [ES51], [ES52], [ES53], [ES55], [ES56], [ES58], [ES59], [ES60], [ES62], [ES66], [ES70], [ES71], [ES72], [ES73]

Fonte: O autor.

Evidências:

"A veracidade dos dados fornecidos será garantida pelo fato de que o hash dos dados de saúde serão armazenados no blockchain, compartilhado entre diferentes empresas de forma imutável e associado a um carimbo de data/hora. Desta forma, a blockchain continuará a manter permanentemente apenas hashes seguros de dados e, portanto, será impossível, para os indivíduos não autorizados reconstruir os dados de saúde alheios" (**ES22**, tradução do autor)[4]

"(...) fornecer interfaces gráficas de usuário para que os usuários tenham uma melhor visualização da interação com o sistema blockchain, e (2) duas camadas de configurações de segurança para garantir que apenas usuários autorizados possam executar determinadas funções e minimizar o problema de violação de dados, e (3) um mecanismo de hashing para garantir a consistência dos dados e (4) a segmentação personalizada de dados dá aos pacientes a capacidade de controlar seus registros escolhendo apenas as informações que gostariam de compartilhar, e (5) seleção de contatos para os médicos selecionarem os registros de saúde relacionados à visita sem navegar por todos os registros e (6) uma simulação em grande escala usando o modelo proposto implementado para avaliar a viabilidade, estabilidade e robustez do modelo blockchain proposto para a aplicação HIE" (**ES52**, tradução do autor)[5]

"A utilização da Blockchain na área da saúde irá garantir, em primeiro lugar, a confiabilidade dos dados armazenados. (...) Em segundo lugar, os dados permanecerão inalterados ao longo do tempo. Ninguém poderá fazer alterações no registro sem concordar com outras fontes e muito menos excluir os dados. E em terceiro lugar, será garantida a devida segurança dos dados, uma vez que ninguém poderá aceder aos mesmos sem o consentimento da fonte dos dados." (**ES29**, tradução do autor)[6]

---

[4] No original: The truthfulness of provided data will be guaranteed by the fact that the secure hash of health data will be stored in the Blockchain, shared between different companies in an immutable way and associated with a timestamp. In this way, the Blockchain will continue to permanently maintain only secure hashes of data and therefore it will be impossible, for subjects not legitimated to do this, to reconstruct the related health data

[5] No original: (...) provide graphical user interfaces for users to have a better visualization of the interaction with the blockchain system, and (2) two layers of security settings to ensure that only authorized users can execute certain smart contract functions and minimize the data breach problem, and (3) a hashing mechanism to ensure data consistency and (4) personalized data segmentation gives patients the ability to control of their records by choosing only the information they would like to share, and (5) touchpoint selection for clinicians to select the health records that related to the visit without browsing through entire records, and (6) a large-scale simulation using the implemented proposed model to evaluate the feasibility, stability, and robustness of the proposed blockchain model for the HIE application

[6] No original: The use of Blockchain in healthcare will ensure, first, the reliability of the stored data. (...) Secondly, the data will remain unchanged over time. No one will be able to make changes to the record without agreeing with other sources, let alone deleting the data. And thirdly, the proper data security will be ensured, since no one can access them without the consent of the data source.

"Esta solução foi projetada para lidar com dados sensíveis de saúde em várias instituições de saúde e pesquisa, garantindo a segurança por meio de um paradigma descentralizado que demonstra sua resiliência às atuais ameaças cibernéticas." (**ES26**, tradução do autor)[7]
"Levamos em consideração os três parâmetros principais: segurança, escalabilidade e tempo de processamento. A segurança é garantida usando o proxy de re-criptografia combinado com Blockchain para armazenar dados hash. Os contratos inteligentes são usados para controle de acesso." (**ES24**, tradução do autor)[8]

"O setor da Saúde pode ser revolucionado com a intervenção da tecnologia Blockchain equipada com sistemas de armazenamento IoT e IPFS. Blockchain neste setor irá resolver todas as preocupações de segurança, privacidade e eliminará fraudes" (**ES20**, tradução do autor)[9]

"Neste trabalho, a principal contribuição é integrar um passaporte de saúde digital baseado em Blockchain privado para garantir alta proteção de informações sensíveis, segurança e privacidade entre todos os atores (Governo, Ministério do Interior, Ministério da Saúde, verificadores) que cumprem com a CNDP (Comissão Nacional para o Controle da Proteção de Dados Pessoais) e a Lei Marroquina 09-08." (**ES19**, tradução do autor)[10]

"Blockchain fornece uma possível direção para auditoria de integridade de dados para sistema de saúde na nuvem-edge." (**ES16**, tradução do autor)[11]

"A tecnologia Blockchain poderia ser usada como solução para esses problemas, pois garante uma ordem cronológica dos dados, bem como sua autenticidade, privacidade, imutabilidade e segurança." (**ES13**, tradução do autor)[12]

---

[7] No original: This solution is designed to handle sensitive healthcare data across many healthcare and research institutions, assuring the safety of his sensitive data through a decentralized paradigm that demonstrates their resiliency to current cyber threats.
[8] No original: We took into consideration three main parameters: security, scalability, and processing time. The security is ensured by using the re-encryption proxy combined with Blockchain to store hash data. Smart contracts are used for access control.
[9] No original: The Healthcare sector can be revolutionized with the intervention of Blockchain technology equipped with IoT and IPFS storage systems. Blockchain in this sector will resolve all security and privacy concerns and eliminates fraud
[10] No original:In this work, the main contribution is integrating a private Blockchain-based digital health passport to ensure high protection of sensitive information, security and privacy among all the actors (Government, Ministry of Interior, Ministry of Health, verifiers) that comply with the CNDP (National Commission for the Control of Personal Data Protection) and the Moroccan Law 09–08.
[11] No original: Blockchain provides a possible direction for data integrity audit- ing for cloud-edge healthcare system
[12] No original: The Blockchain technology that could be used as a solution to these problems, as it ensures a chronological order of data, as well as its authenticity, privacy, immutability, and security.

"Um dos principais desafios na área da saúde é a natureza fragmentada dos dados dos pacientes entre diferentes provedores e sistemas de saúde. Blockchain pode facilitar a interoperabilidade e troca de dados criando uma plataforma unificada e padronizada para armazenar e compartilhar registros de saúde dos pacientes de forma segura." (**ES11**, tradução do autor)[13]

"Nós propusemos uma arquitetura de saúde robusta habilitada por blockchain para um método centrado no paciente que fornece um mecanismo de controle de acesso criptográfico para um provedor de saúde com uma instituição médica diferente." (**ES11**, tradução do autor)[14]

"O blockchain pode ser utilizado nestes casos para alcançar a acessibilidade e integridade seguras dos dados de saúde. (...) A tecnologia blockchain promete oferecer imensas oportunidades no setor de saúde, como armazenamento e compartilhamento seguros de dados entre várias partes interessadas, interoperabilidade nacional de dados e modos flexíveis e rápidos de faturamento e pagamento." (**ES9**, tradução do autor)[15]

"Neste esquema, com a ajuda do blockchain, as transações de compartilhamento de EMRs são transparentes e não podem ser adulteradas. Rastreamos com precisão o fluxo de EMRs; uma vez que são usadas de forma imprópria, os usuários podem ser identificados imediatamente, portanto, o uso de EMRs pode ser supervisionado efetivamente." (**ES7**, tradução do autor)[16]

"Por outro lado, uma das principais capacidades dos sistemas de blockchain é a autenticidade e integridade dos dados. Devido a essas capacidades, além de serem descentralizados, seguros, fornecerem transparência e proveniência de dados, e serem verificáveis, vários esforços de pesquisa ainda estão sendo conduzidos rigorosamente para utilizar sistemas de blockchain para gerenciar dados relacionados à saúde." (**ES1**, tradução do autor)[17]

---

[13] No original:One of the key challenges in healthcare is the fragmented nature of patient data across different healthcare providers and systems. Blockchain can facilitate data inter- operability and exchange by creating a unified and standardized platform for securely storing and sharing patient health records.

[14] No original: We have proposed blockchain-enabled robust healthcare architecture for a patient-centric method that provides a cryptographic access control mechanism for a healthcare provider with a distinct medical institution

[15] No original: Blockchain can be utilized in these cases to achieve the secure accessibility and integrity of the healthcare data. (...) Blockchain technology promises to provide immense opportunities in the healthcare sector such as secure data storing and sharing among various stakeholders, nationwide data interoperability and flexible and quick billing and payment modes.

[16] No original: In this scheme, with the aid of the blockchain, the EMRs sharing transactions are transparent, and cannot be tampered with. We accurately track the flow of EMRs, once they are used improperly, users can be identified immediately, hence the EMRs usage can be supervised effectively

[17] No original: On the other hand, one of the main capabilities of blockchain systems is data authenticity and integrity. Due to these capabilities in addition to being decentralized, secured, providing data transparency and provenance, and being verifiable, multiple research efforts are still being rigorously conducted to utilize blockchain systems to manage health related data

"Por outro lado, violações de segurança e privacidade associadas aos sistemas e dados de saúde estão se tornando cada vez mais importantes de serem abordadas. (...) dados dos pacientes estão sendo vendidos por hackers a um preço até 20 vezes maior do que o dos dados bancários. Ataques a bancos de dados de saúde resultaram em uma perda de quase US$30 bilhões nos últimos 20 anos (...) a tecnologia Blockchain tem sido proposta por vários pesquisadores como uma solução para muitos dos problemas mencionados anteriormente. (...) A tecnologia Blockchain pode proporcionar vários benefícios para os sistemas de saúde, incluindo uma infraestrutura descentralizada, permitindo interoperabilidade, segurança, autenticação e integridade." (**ES5**, tradução do autor)[18]

"Satoshi propôs inicialmente o blockchain, que pode ser considerado um banco de dados distribuído que satisfaz a descentralização, resistência à adulteração e criptografia assimétrica. Além disso, contratos inteligentes no blockchain também podem melhorar a interoperabilidade dos dados médicos e têm um forte potencial de aplicação no campo médico." (**ES41**, tradução do autor)[19]

"O uso de blockchain em EHRs promete, com cinco características dos EHRs que devem ser abordadas por qualquer solução blockchain: governança, interoperabilidade, privacidade, escalabilidade e segurança." (**ES2**, tradução do autor)[20]

"Neste trabalho, propomos um sistema de saúde eficiente baseado em blockchain para lidar com registros de pacientes para um tratamento de saúde mais preciso. O sistema proposto garante a privacidade e integridade dos dados dos pacientes e reduz a latência que pode resultar em blocos massivos para a cadeia." (**ES17**, tradução do autor)[21]

"Os esquemas usados para armazenar EHRs têm sido muito inseguros na era atual de cidades e casas inteligentes. Os dados podem ser facilmente violados por hackers e partes externas não autorizadas. Além disso, os dados não são acessíveis aos pacientes e provedores de

---

[18] No original: On the other hand, security and privacy breaches associated with healthcare systems and data are also becoming increasingly important to address. (...) data is being sold by hackers at a price of up to 20 times higher than that of banking data. Attacks on health databases have resulted in a loss of nearly $30 billion in the past 20 years alone (...) Blockchain technology has been proposed by several researchers as a solution to many of the aforementioned problems. (...) Blockchain technology can provide several benefits for healthcare systems including a decentralized infrastructure, allowing interoperability, security, authentication, and integrity

[19] No original: Satoshi firstly proposed the blockchain, which can be regarded as a distributed database that satisfies the decentralization, tamper resistance, and asymmetric encryption. In addition, smart contracts in the blockchain can also enhance the interoperability of medical data and have strong application potential in the medical field

[20] No original: Blockchain usage in Electronic Health Records (EHRs) holds promise, with five characteristics of EHRs that must be addressed by any blockchain solution: governance, interoperability, privacy, scalability, and security.

[21] No original:In this work, we propose an efficient blockchain-based healthcare system to handle patient records for more accurate health treatment. The proposed system guarantees the privacy and integrity of patients' data and reduces the latency that may result in massive blocks to the chain.

cuidados. Esses esquemas são incapazes de criar um equilíbrio entre segurança e acessibilidade de dados. Mas o blockchain pode resolver esses problemas. O blockchain cria um sistema de contabilidade que é imutável e permite que as transações ocorram de maneira descentralizada." (**ES28**, tradução do autor)[22]

"Por outro lado, uma solução baseada em blockchain oferece segurança de dados, transparência, imutabilidade, proveniência e registros de transações autenticadas. Blockchain é um livro-razão compartilhado e imutável descentralizado que pode ser aplicado a uma variedade de cenários de negócios envolvendo processos de transações." (**ES54**, tradução do autor)[23]

"O blockchain introduziu uma maneira descentralizada de implementar transações seguras entre nós em uma rede não confiável por meio de um algoritmo de consenso que valida as transações para todos os nós da rede. Ele oferece características importantes como acessibilidade, imutabilidade e não repúdio, criando sistemas transparentes que economizam dinheiro e tempo ao reduzir a necessidade de intermediários. A saúde móvel pode se beneficiar significativamente com a integração da tecnologia blockchain." (**ES67**, tradução do autor)[24]

"A tecnologia de registro distribuído (blockchain) proporciona a capacidade de gerir emergências, minimizar atrasos, proporcionar transparência ao sistema de saúde e aumentar a confiança dos pacientes de que as suas informações de saúde estão seguras." (**ES56**, tradução do autor)[25]

---

[22] No original:The schemes used to store EHRs have been very insecure in the present era of smart cities and homes. The data can be easily breached by hackers and unauthorized external parties. Also, the data is not accessible to patients and care providers. These schemes are unable to create a balance between data security and data accessibility. But blockchain can resolve these issues. Blockchain creates a ledger system that is immutable and allows the transactions to take place in a decentralized manner.

[23] No original: On the other hand, a blockchain based solution offers data security, transparency, immutability, provenance and authenticated transaction records. Blockchain is a decentralized, immutable shared ledger that can be applied to a variety of business settings involving transaction processes

[24] No original: Blockchain introduced a decentralized way to implement secure transactions between nodes in an untrustworthy network through a consensus algorithm validating the transactions for all the nodes of the network. It offers important characteristics such as accessibility, immutability, and non-repudiation, creating transparent systems saving money and time by reducing the need for intermediaries. m-health can benefit significantly with the integration of blockchain technology.

[25] No original: Distributed ledger technology (blockchain) provides the ability to manage emergencies, minimize delays, provide transparency to the healthcare system, and increase patient confidence that their healthcare information is secure.

Interoperabilidade:

A interoperabilidade nos sistemas de saúde é essencial para a troca eficaz de informações entre diferentes plataformas e instituições, o que é vital para a prestação de cuidados de saúde de alta qualidade. A integração de tecnologias inovadoras, como a blockchain, e a adoção de padrões como FHIR, são fundamentais para superar as barreiras à interoperabilidade. Essas tecnologias não apenas facilitam a comunicação segura e descentralizada de dados de saúde, mas também promovem a privacidade e a segurança dos pacientes. A implementação bem-sucedida de sistemas interoperáveis é um passo crucial para avançar na eficiência operacional dos cuidados de saúde e na melhoria contínua dos resultados dos pacientes. Além disso, a importância da interoperabilidade nos cuidados de saúde é sublinhada no contexto da construção de um centro nacional de dados de saúde sem comprometer a segurança. A capacidade de trocar registos de saúde num país é crucial para melhorar a qualidade dos serviços de saúde e facilitar os avanços da investigação. Um quadro de cadeias de blocos que apoie a interoperabilidade pode fazer a ponte entre os EHR típicos e permitir a sincronização de dados entre diferentes sistemas de saúde.

Privacidade e Autenticação:

A salvaguarda da privacidade nos sistemas de saúde é imperativa para assegurar a confiança dos pacientes e a proteção dos seus dados sensíveis. A importância da privacidade é enfatizada nos estudos sobre sistemas de saúde que utilizam a tecnologia blockchain, onde se destaca a necessidade de mecanismos que permitam aos pacientes um controle direto sobre o acesso aos seus dados de saúde.

Esses sistemas propõem soluções inovadoras, como a gestão descentralizada de políticas de acesso e a distribuição de chaves de criptografia, para garantir que apenas entidades autorizadas possam acessar as informações. Tais medidas não só reforçam a privacidade, mas também promovem a autonomia dos pacientes na gestão dos seus próprios dados, fortalecendo a confiança no sistema de saúde.

Os desafios de manter a privacidade em sistemas de saúde móveis são abordados com soluções como ZKP e a aplicação de blockchain, que visam proteger os dados contra acessos não autorizados e manter a confidencialidade das informações ao longo do tempo. O desenvolvimento de plataformas de troca de informações de saúde baseadas em blockchain é

também uma estratégia para preservar a confidencialidade e a integridade dos dados dos pacientes.

Em resumo, a privacidade é um pilar central na gestão de dados de saúde, e sua priorização é essencial para proteger os direitos dos pacientes e cumprir com os padrões regulatórios. A adoção de tecnologias de preservação da privacidade e as funcionalidades de segurança oferecidas pela blockchain podem significar melhorar a proteção dos dados, fomentar a confiança dos pacientes e promover uma cultura de respeito pela privacidade e segurança dos dados no setor de saúde.

Dados:

Os dados são vitais para os sistemas de saúde contemporâneos, catalisando decisões informadas, aprimorando a assistência ao paciente e impulsionando pesquisas. A coleta, administração e análise de dados competentes são cruciais para fornecer cuidados de saúde de qualidade e aumentar a eficiência operacional. A relevância dos dados é enfatizada nos artigos sobre sistemas de saúde que utilizam blockchain.

A troca de dados no setor de saúde é essencial para fortalecer a colaboração e elevar a qualidade do atendimento ao paciente. Com a blockchain, é possível compartilhar e acessar dados de pacientes de maneira segura entre várias instituições, promovendo decisões mais esclarecidas e tratamentos individualizados. A interoperabilidade dos dados pode descomplicar o fluxo de trabalho em saúde e incentivar a cooperação entre diferentes especialistas.

Os artigos também ressaltam a importância dos dados na criação de prontuários eletrônicos seguros e confiáveis. A blockchain proporciona uma infraestrutura descentralizada e imune a alterações indevidas para o armazenamento e gerenciamento de prontuários eletrônicos, assegurando a integridade e veracidade dos dados. Utilizando blockchain para prontuários eletrônicos, as instituições de saúde podem reforçar a proteção dos dados, minimizar riscos de violações e manter um histórico detalhado e acurado das informações dos pacientes.

Em suma, os dados constituem o alicerce dos sistemas de saúde modernos, fomentando inovação, melhorando resultados dos pacientes e embasando decisões clínicas. Ao capitalizar os dados e incorporar tecnologias como a blockchain, os profissionais de saúde podem acessar insights valiosos, otimizar processos e oferecer cuidados mais personalizados e eficazes.

Segurança:

A proteção e segurança, em ênfase nos dados, no setor de saúde é uma questão de extrema importância, envolvendo a segurança das informações sensíveis dos pacientes, a preservação da confidencialidade e a prevenção de acessos indevidos ou violações. A adoção de estratégias de segurança eficazes é crucial para proteger a integridade e a privacidade dos dados de saúde, sustentar a confiança dos pacientes e atender às exigências regulatórias. A segurança é um tema de destaque nos artigos sobre sistemas de saúde que incorporam a tecnologia blockchain.

Um ponto crítico é a necessidade de enfatizar a segurança para possibilitar o compartilhamento seguro de dados em sistemas de saúde. Os especialistas consultados no estudo reconhecem a importância da segurança nas aplicações de blockchain para compartilhamento de dados, ressaltando a necessidade de mecanismos de segurança descentralizados e eficazes. Priorizando a segurança, as instituições de saúde podem mitigar riscos, proteger os dados dos pacientes de acessos não autorizados e assegurar a confidencialidade e integridade das informações.

Os artigos também exploram os benefícios da blockchain na ampliação da segurança e privacidade dos sistemas de saúde. Utilizando criptografia avançada, protocolos de consenso e armazenamento de dados imutáveis, os sistemas baseados em blockchain podem oferecer imutabilidade, transparência e integridade às informações de saúde. Essas características de segurança são fundamentais para prevenir adulterações, modificações não autorizadas e garantir a autenticidade dos registros de saúde, elevando assim a segurança dos dados.

Esses esquemas possibilitam o controle de acesso seguro e eficiente, permitindo que os profissionais de saúde gerenciem o acesso aos dados com base em atributos e funções específicas. Com medidas de segurança avançadas, como múltiplas autoridades para autenticação e autorização, às instituições de saúde podem fortalecer a proteção dos dados, prevenir violações e salvaguardar a privacidade dos pacientes.

Integridade e Transparência:

Transparência e integridade são pilares vitais para os sistemas de saúde, fundamentais para estabelecer confiança, assegurar responsabilidade e manter a qualidade e precisão dos dados de saúde. A clareza nos procedimentos e a fidelidade das informações são essenciais

para conquistar a confiança dos pacientes, possibilitar decisões bem fundamentadas e incentivar condutas éticas no âmbito da saúde. Os artigos analisados ressaltam a importância crítica desses princípios em sistemas de saúde que adotam a tecnologia blockchain.

Um ponto crucial é o reforço da transparência e da confiança na gestão dos dados de saúde proporcionados pela blockchain. Utilizando suas características de registro imutável e com timestamp, as instituições de saúde podem assegurar a integridade dos dados, prevenir alterações não autorizadas e criar um sistema de gestão de registros eletrônicos de saúde transparente e auditável. Essa clareza não só fortalece a segurança dos dados, mas também promove a responsabilidade e a confiança entre todos os envolvidos no ecossistema de saúde.

Os artigos também destacam as vantagens da blockchain para aprimorar a comunicação e a transparência dos dados entre os prestadores de saúde. Com plataformas de intercâmbio de informações de saúde baseadas em blockchain, é possível simplificar o compartilhamento de dados, aprimorar a interoperabilidade e garantir o acesso seguro às informações dos pacientes. A transparência garantida pela tecnologia blockchain permite que os profissionais de saúde tenham acesso a dados precisos e atualizados, levando a decisões mais informadas e a melhores resultados no atendimento aos pacientes.

6.2.2 PPS2. Como a identidade descentralizada, blockchain e identidade auto-soberana podem ser aplicadas no setor de saúde?

A aplicação da identidade descentralizada, blockchain e identidade auto-soberana no setor de saúde representa uma promissora evolução tecnológica que pode revolucionar a maneira como as informações médicas são gerenciadas e compartilhadas. Essas tecnologias oferecem soluções inovadoras para desafios como privacidade, segurança e interoperabilidade de dados, possibilitando uma abordagem mais eficaz e centrada no paciente. Neste contexto, explorar como esses conceitos podem ser integrados ao ambiente da saúde é fundamental para entender seu potencial impacto e benefícios.

Durante a análise dos estudos foram encontradas as respectivas aplicações: 1. Segurança dos dados e privacidade. 2. Interoperabilidade e rastreamento dos dados entre sistemas. 3. Autonomia dos pacientes referente aos seus dados. 4. Viabilização da melhora dos dados de tratamento remoto.

Tabela 10 - Aplicações no setor de saúde e estudos relacionados

Aplicações	Estudos
Segurança dos dados e privacidade	[ES1], [ES2], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES15], [ES17], [ES24], [ES25], [ES26], [ES27], [ES28], [ES29], [ES31], [ES32], [ES33], [ES35], [ES38], [ES39], [ES40], [ES41], [ES42], [ES49], [ES50], [ES51], [ES52], [ES59], [ES61], [ES65], [ES67], [ES69]
Interoperabilidade e rastreamento dos dados de pacientes e suplementos entre sistemas	[ES1], [ES2], [ES3], [ES5], [ES7], [ES8], [ES9], [ES10], [ES11], [ES17], [ES19], [ES24], [ES25], [ES26], [ES27], [ES28], [ES29], [ES31], [ES32], [ES33], [ES38], [ES39], [ES40], [ES42], [ES43], [ES46], [ES49], [ES50], [ES51], [ES52], [ES54], [ES59], [ES61], [ES67], [ES69]
Autonomia dos pacientes referente aos seus dados	[ES1], [ES2], [ES4], [ES5], [ES7], [ES8], [ES10], [ES11], [ES15], [ES16], [ES17], [ES24], [ES27], [ES30], [ES31], [ES32], [ES33], [ES35], [ES38], [ES39], [ES40], [ES42], [ES43], [ES46], [ES49], [ES50], [ES51], [ES52], [ES54], [ES59], [ES65], [ES67], [ES69]
Viabilização da melhora dos dados de tratamento e acompanhamento remoto	[ES3], [ES4], [ES10], [ES11], [ES17], [ES20], [ES24], [ES27], [ES29], [ES32], [ES39], [ES42], [ES43], [ES49], [ES51], [ES52], [ES54], [ES59], [ES61]
Pesquisa e evolução do setor médico	[ES13], [ES26], [ES27], [ES29], [ES30], [ES35], [ES59]

Fonte: O autor.

Evidências:

> "O monitoramento remoto de pacientes está ganhando constantemente espaço. Para este fim, o paciente muitas vezes é equipado com dispositivos eletrônicos vestíveis ou implantados, que monitoram sua condição em tempo real e transmitem suas medições para um dispositivo principal, como um telefone celular, enquanto em alguns casos, eles podem até mesmo tomar certas ações (por exemplo, tentar mudar o comportamento do paciente) com o objetivo final de evitar situações perigosas ou potencialmente fatais. (...) os autores apresentaram um sistema baseado em tecnologias blockchain, para o gerenciamento eficaz de dados do paciente provenientes de sensores e a prestação de uma resposta imediata para acionar as ações necessárias, quando requerido." (**ES10**, tradução do autor)[26]

[26] No original: Remote patient monitoring is constantly gaining ground. For this purpose, the patient is often equipped with wearable or implanted electronic devices, which monitor their condition in real time and transmit their measurements to a master device, such as a mobile phone, while in some cases, they can even take certain actions (e.g., try to change the patient's behavior) with the ultimate goal being the avoidance of dangerous or life-threatening situations. (...) the authors presented a system based on blockchain technologies, for the effective

"Particularmente, a integração do sistema de e-saúde com serviços inteligentes em blockchain pode ser um tópico interessante. Por exemplo, plataformas automáticas de suporte clínico usando mineração de dados ou aprendizado de máquina podem ser integradas na nuvem para analisar registros médicos e prever problemas de saúde dos pacientes de forma dinâmica. Isso pode ajudar os provedores de saúde, ou seja, médicos, a fornecer serviços de saúde instantâneos, enquanto a privacidade e segurança dos dados são ainda garantidas." (**ES43**, tradução do autor)[27]

"Neste artigo, propusemos o processamento de reclamações de seguro saúde para medicamentos prescritos usando blockchain de maneira confidencial, privada, segura, confiável e descentralizada. O sistema proposto utiliza um blockchain Ethereum privado, onde dois contratos inteligentes foram desenvolvidos para contribuir para registrar e registrar eventos automaticamente. Além disso, para lidar com a limitação de armazenamento, a rede foi integrada com armazenamento *off-chain* (IPFS) para armazenar os dados de grande tamanho que são caros para serem armazenados na rede blockchain. Uma análise de segurança foi conduzida para demonstrar a robustez e segurança de nossa solução proposta contra importantes vulnerabilidades de segurança. O sistema descentralizado proposto fornece resiliência e segurança contra o problema de ponto único de falha, que é crítico para um sistema de saúde. Por fim, o sistema proposto pode ser generalizado para atender diferentes sistemas de reclamações de seguro saúde, incluindo pacientes internados ou ambulatoriais." (**ES64**, tradução do autor)[28]

---

management of patient data stemming from sensors and the provision of an immediate response for triggering the necessary actions, when required

[27] No original: Particularly, the integration of e-health system with intelligent services on blockchain can be an interesting topic. For instance, automatic clinical support platforms using data mining or machine learning can be integrated at the cloud to analyze medical records and predict health problems of patients in a dynamic manner. This can help healthcare providers, i.e. doctors to provide instant healthcare services, while data privacy and security are still guaranteed

[28] No original: In this paper, we proposed processing health insurance claims for prescription drugs using blockchain in a confidential, private, secure, trustworthy, and decentralized manner. The proposed system utilizes a private Ethereum blockchain, where two smart contracts were developed to contribute to recording and logging events automatically. Also, to deal with the limitation of storage, the network was integrated with off-chain storage (IPFS) to store the large-sized data that is expensive to be stored on the blockchain network. A security analysis was conducted to demonstrate the robustness and security of our proposed solution against major security vulnerabilities. The proposed decentralized system provides resilience and security against the single point of failure problem, which is critical to a healthcare system. Lastly, the proposed system can be generalized to serve different health insurance claims systems, including inpatient or outpatient

"A presença da tecnologia blockchain na saúde tem levado a melhorias significativas em: (1) sistema automatizado de registro de saúde; (2) compartilhamento de informações confiáveis; (3) análise em Big Data; (4) colaboração na prática clínica e diagnóstico." (**ES27**, tradução do autor)[29]

"Acreditamos que usar tal solução em sistemas de informações de saúde adicionaria mais confiança à tomada de decisões médicas baseadas em IA. Consequentemente, poderia melhorar significativamente a qualidade da assistência médica, aumentando também a satisfação e envolvimento dos pacientes." (**ES26**, tradução do autor)[30]

"Este sistema inclui contratos inteligentes para manter dados no blockchain, que são mais atemporais e funcionais. Às vezes, a distância entre o médico e os pacientes será um problema importante para obter um serviço de saúde de qualidade e também dificuldades no monitoramento regular da saúde. Portanto, o sistema de saúde médica baseado em IoT ajuda o paciente a obter atenção médica adequada em um local onde se sentem confortáveis." (**ES32**, tradução do autor)[31]

"Blockchain é um livro-razão digital compartilhado e imutável que facilita o processo de registro de transações e rastreamento de ativos em uma rede de negócios. A característica compartilhável permite que os dados sejam compartilhados dentro de membros autorizados, enquanto a imutabilidade permite proteger a integridade dos dados." (**ES27**, tradução do autor)[32]

"O framework apresenta onze componentes principais abrangendo todos os serviços que poderiam fazer parte da indústria de saúde, que inclui a propriedade do paciente sobre seus dados, profissionais de saúde confiáveis, cadeia de suprimentos de medicamentos auditáveis desde sua origem até atacadistas e farmácias, e farmacovigilância principalmente. (...) O núcleo do framework é baseado na tecnologia blockchain, que garante o fornecimento de dados seguros, tolerantes a falhas, transparentes e à prova de adulteração. Além disso, o uso de contratos inteligentes permite a aplicação de controle de acesso,

[29] No original: The presence of blockchain technology in healthcare have led significant improvements in [12]: (1) automated healthcare record system; (2) sharing reliable information; (3) analysis in Big Data; (4) collaboration in clinical practice and diagnosis.

[30] No original: We believe that using such a solution in health information systems would add more trust to AI based medical decision making. Consequently, it might significantly improve healthcare quality while also increasing patient satisfaction and involvement.

[31] No original: This system includes smart contracts to keep data on the blockchain, which is more timeless and functional. Sometimes the distance between the doctor and patients will be a major problem to get a health-care service quality and also trouble in regular health monitoring. So IoT based medical healthcare system helps the patient to get proper medical attention at a place where they are comfortable.

[32] No original: Blockchain is a shared and immutable digital ledger that facilitates the process of recording transactions and tracking assets in a business network. Shareable feature enables the data to be shared within authorized member while immutable enables to protect the integrity of data.

melhora a confiança e rastreabilidade, aprimora a segurança e executa transações de forma transparente." (**ES59**, tradução do autor)[33]

"Por exemplo, a criação de um registro eletrônico de medicamentos baseado em tecnologia blockchain permitirá que o próximo nível do caminho digital de desenvolvimento na esfera de produtos medicinais avance. (...) Conforme segue as informações do Serviço Federal de Supervisão em Saúde, multas são frequentemente aplicadas por armazenamento impróprio de medicamentos e violação do prazo de validade. Informações corretas sobre os requisitos de prazo de validade, condições de armazenamento e data de fabricação permitirão minimizar o fechamento de dados, bem como melhorar a segurança da farmacoterapia reduzindo os riscos de tomar medicamentos com prazo de validade vencido." (**ES29**, tradução do autor)[34]

"Este sistema oferece um conjunto de benefícios para monitoramento remoto de pacientes. Ele fornece coleta diária de dados, compartilhamento e segurança de dados. O sistema é dividido em três lados. O primeiro lado é responsável pela coleta de dados, este lado está usando dispositivos de saúde IoT para garantir a coleta. O segundo lado é responsável por compartilhar dados de forma segura, a tecnologia que está garantindo isso é o Blockchain. O último lado é para armazenamento de dados e está usando IPFS para isso." (**ES24**, tradução do autor)[35]

"Com a crescente adoção da telemedicina e monitoramento remoto de pacientes, o Blockchain pode fornecer uma infraestrutura segura e transparente para gerenciar dados de pacientes e garantir a integridade dos serviços de saúde remotos. Contratos inteligentes baseados em Blockchain podem facilitar pagamentos automatizados, aplicar acordos de nível de serviço e manter um registro auditável de interações de telemedicina e dados de monitoramento de pacientes." (**ES11**, tradução do autor)[36]

---

[33] No original: The framework features eleven major components encompassing all services that could be part of the healthcare industry which includes patient ownership to his data, trusted healthcare practitioners, auditable drugs supply chain from their origin to wholesalers and pharmacy, and pharmacovigilance primarily. (...) The core of the framework is based on blockchain technology which ensures the provision of secure, fault-tolerant, transparent, and tamper-proof data. Moreover, the use of smart contracts enables enforcement of access control, enhance trust and traceability, improve security and execute transactions transparently.

[34] No original: For example, the creation of an electronic register of medicines based on Blockchain technology will allow the next level of the digital path of development in the sphere of medicinal products to move to the next level. You can talk about the so-called Internet of things for medicines. (...) As follows from the information of the Federal Service for Surveillance in Health Care (Roszdravnadzor), fines are often charged for improper storage of medicines and violation of shelf life. Correct information about the requirements for shelf life, storage conditions and release date will allow minimizing foreclosure data, as well as improving the safety of pharmacotherapy by reducing the risks of taking drugs with expired shelf life

[35] No original: This system is offering a set of benefits for remote patient monitor- ing. It provides daily data collection, data sharing and security. The system is divided into three sides. The first side is responsible for data collection, this side is using IoT healthcare devices to ensure the collection. The second side is responsible for sharing data securely, the technology which is ensuring that is Blockchain. The last side is for data storage and it is using IPFS for that.

[36] No original: With the increasing adoption of telemedicine and remote patient monitoring, Blockchain can provide a secure and transparent infrastructure for managing patient data and ensuring the integrity of remote

"O proprietário dos EMRs, os pacientes controlam o direito de usar os dados. Os pacientes primeiro criptografam os registros fisiológicos com sua chave pública por meio de clientes móveis, como celulares ou smartwatches, e depois enviam esses textos cifrados para o servidor em nuvem do hospital. Quando o hospital pretende usar os registros de saúde pessoal, é obrigado a obter o consentimento dos pacientes primeiro. O hospital adquire uma chave de re-criptografia gerada pelos pacientes se eles forem aprovados." (**ES7**, tradução do autor)[37]

"A segurança na área da saúde envolve a preservação da confidencialidade, integridade e disponibilidade, bem como a gestão da autenticação, autorização e contabilidade. Os aspectos de segurança são divididos em sistemas centrais e suplementares. O sistema central engloba o banco de dados central do registro, sistema de identidade descentralizada (DID) e sistemas desenvolvidos colaborativamente. A segurança do sistema suplementar inclui ferramentas médicas, importação de dados e plataformas de telemedicina. O projeto de um sistema robusto de segurança em saúde requer uma gestão abrangente tanto dos componentes centrais quanto dos suplementares, onde as diversas perspectivas envolvidas em proteger ativos e garantir a integridade e confidencialidade dos registros de saúde são reconhecidas." (**ES3**, tradução do autor)[38]

"Atualmente, muitos hospitais e clínicas utilizam blockchain para armazenar com segurança os registros médicos de seus pacientes. Quando um registro médico de um paciente é gerado e testado, ele pode ser adicionado à rede blockchain, o que oferece aos pacientes a garantia de que o registro não pode ser alterado. Esses registros de saúde personalizados podem ser criptografados e mantidos na rede blockchain com uma chave privada, que permite apenas que usuários verificados acessem os registros de saúde em momentos cruciais, garantindo assim a privacidade do paciente." (**ES28**, tradução do autor)[39]

---

healthcare services. Blockchain- based smart contracts can facilitate automated payments, enforce service-level agreements, and maintain an auditable log of telemedicine interactions and patient monitoring data

[37] No original: The owner of the EMRs, the patients control the right to use the data. The patients first encrypt the physiological records with their public key through mobile clients such as cell phones or smart watches and then upload these ciphertexts to the cloud server of the hospital. When the hospital intends to use the personal health records, it is obliged to obtain the consent of the patients first. The hospital acquires a re-encryption key generated by patients if they get approved

[38] No original: Security in healthcare involves preserving confidentiality, integrity, and availability (CIA), as well as managing authentication, authorization, and accounting (3As). Security aspects are divided into central and supplementary systems. The central system encompasses the registry's central database, decentralized identity (DID) system, and collaboratively developed systems. Supplementary system security includes medical tools, data importation, and telemedicine platforms. Designing a robust healthcare security system necessitates comprehensive management of both central and supplementary components, whereby the diverse perspectives involved in safeguarding assets and ensuring the integrity and confidentiality of healthcare records are recognized

[39] No original: Nowadays many hospitals and clinics use blockchain in order to securely store their patients' medical records. When a medical record of a patient is generated and tested, it can be added on to the blockchain network, which offers patients with the perfect assurance that the record cannot be altered. These personalized

"Os pacientes desempenham um papel importante como participantes no sistema de EHR. Eles são donos de seus registros de saúde que estão sendo criados e adicionados à blockchain. Eles podem alterar suas informações pessoais. Portanto, eles têm a autoridade para regular quem pode acessar seus registros. Qualquer indivíduo não autorizado ou terceirizado é bloqueado pelos pacientes para acessar seus registros." (**ES28**, tradução do autor)[40]

"As soluções tradicionais para alcançar a rastreabilidade dentro da cadeia de suprimentos farmacêuticos são tipicamente centralizadas e carecem de transparência entre os participantes da cadeia de suprimentos, o que permite que a autoridade central modifique as informações sem notificar outras partes interessadas. Por outro lado, uma solução baseada em blockchain oferece segurança de dados, transparência, imutabilidade, proveniência e registros de transações autenticadas. Blockchain é um livro-razão compartilhado e imutável descentralizado que pode ser aplicado a uma variedade de cenários de negócios envolvendo processos de transações." (**ES54**, tradução do autor)[41]

"Um sistema torna as informações disponíveis para organizações de pesquisa e empresas farmacêuticas. Uma plataforma chamada BlockRx tem sido empregada de forma produtiva em aplicações reais. O sistema inclui tecnologias poderosas de DLT digital da iSolve com blockchain. A plataforma incorpora informações de saúde das organizações de pesquisa e biomédicas. O BlockRx tem feito progressos significativos desde que foi implementado pela primeira vez na prática." (**ES35**, tradução do autor)[42]

---

health records could be encrypted and kept on the blockchain network with a private key, which allows only verified users to access the health records in crucial time, thereby ensuring the privacy of the patient

[40] No original:Patients play an important role as a participant in the EHR system. They own their health records that are being created and added to the blockchain. They can change their personal information. Therefore, they have the authority to regulate who all can access their records. Any unauthorized care provider or third-party is blocked by the patients from accessing their records

[41] No original: Traditional solutions to achieve traceability within the pharmaceutical supply chain are typically centralized and lack transparency across participants of the supply chain, which allows the central authority to modify information without notifying other stakeholders. On the other hand, a blockchain based solution offers data security, transparency, immutability, provenance and authenticated transaction records. Blockchain is a decentralized, immutable shared ledger that can be applied to a variety of business settings involving transaction processes

[42] No original: A system makes information available to research organizations and medicinal firms. A platform called BlockRx has been productively employed in actual applications. The system includes powerful digital ledger technologies from iSolve with blockchain. The platform incorporates health information from the research and biomedical organizations. BlockRx has made significant progress since it was first implemented in practice

"Ele oferece características importantes, como acessibilidade, imutabilidade e não repúdio, criando sistemas transparentes que economizam dinheiro e tempo ao reduzir a necessidade de intermediários. A saúde móvel pode se beneficiar significativamente com a integração da tecnologia blockchain. Qualquer acesso, inserção ou modificação dos dados no sistema é salvo como um evento na blockchain, concedendo imutabilidade e não repúdio ao sistema." (**ES67**, tradução do autor)[43]

"A tecnologia blockchain garante transparência, melhorando assim a confidencialidade e integridade geral nos sistemas de monitoramento remoto de saúde." (**ES3**, tradução do autor)[44]

[43] No original:It offers important characteristics such as accessibility, immutability, and non-repudiation, creating transparent systems saving money and time by reducing the need for intermediaries. m-health can benefit significantly with the integration of blockchain technology. Any access, insertion, or modification of the data in the system is saved as an event in the blockchain granting immutability and non-repudiation to the system

[44] No original: Blockchain technology ensures transparency, thereby enhancing overall confidentiality and integrity in remote healthcare monitoring systems

Segurança dos dados e privacidade:

A segurança e a privacidade são de suma importância no setor de saúde, onde a proteção de informações sensíveis do paciente é crucial. Com a crescente digitalização dos registros de saúde e a natureza interconectada dos sistemas de saúde, garantir medidas de segurança robustas é essencial para salvaguardar violações de dados e acesso não autorizado e tecnologias como blockchain e identidade descentralizada oferecem soluções inovadoras para melhorar a segurança e a privacidade na gestão de registros de saúde [ES2].

Ao implementar essas tecnologias, os provedores de saúde podem estabelecer um framework seguro que protege os dados do paciente contra ameaças cibernéticas. Essa abordagem proativa não apenas promove a confiança entre pacientes e provedores de saúde, mas também garante a conformidade com regulamentos relativos à confidencialidade e integridade dos dados [ES69].

Interoperabilidade e rastreamento dos dados entre sistemas:

A interoperabilidade e a rastreabilidade eficaz dos dados são componentes vitais no setor de saúde, permitindo uma comunicação contínua e a troca segura de informações entre vários sistemas e partes interessadas. Ao fomentar a interoperabilidade, as organizações de saúde podem integrar sistemas diversos, compartilhar dados de maneira eficiente e aprimorar a coordenação de cuidados em diferentes contextos de saúde. Essa interoperabilidade assegura que a informação do paciente esteja acessível quando necessário, levando a uma tomada de decisão clínica mais informada e a melhores resultados para os pacientes. Além disso, mecanismos robustos de rastreamento e rastreabilidade desempenham um papel crucial na manutenção da integridade e segurança dos dados de saúde.

A implementação de tecnologias como blockchain pode fornecer um registro transparente e imutável das transações de dados, melhorando a precisão, a auditabilidade e a segurança dos dados. Ao priorizar a interoperabilidade e a rastreabilidade dos dados no setor de saúde, as organizações podem otimizar os processos, melhorar a qualidade dos dados e, finalmente, fornecer cuidados mais eficazes e centrados no paciente. Num contexto de cuidados de saúde, a interoperabilidade permite que o EHR de um doente seja acedido sem problemas por diferentes prestadores de cuidados de saúde envolvidos nos cuidados do doente, tais como médicos de cuidados primários, especialistas e hospitais.

Esta interoperabilidade garante que todos os prestadores de cuidados de saúde tenham acesso em tempo real ao historial médico do doente, aos resultados dos testes e aos planos de tratamento, o que conduz a uma prestação de cuidados mais coordenada e informada. Também no contexto de saúde, mas fugindo dos registros hospitalares, considere um cenário em que uma empresa farmacêutica utiliza a tecnologia blockchain para rastrear toda a jornada de um medicamento, desde a produção até a distribuição.

Cada etapa da cadeia de abastecimento, incluindo o fabrico, a embalagem, o envio e a entrega às farmácias, é registada na cadeia de blocos. Este sistema de rastreio permite às partes interessadas rastrear a origem de cada medicamento, verificar a sua autenticidade e identificar e resolver rapidamente quaisquer problemas, como recolhas ou produtos contrafeitos, garantindo a segurança dos doentes e a conformidade regulamentar. [ES54]

Autonomia dos pacientes referentes aos seus dados:

A autonomia dos dados do paciente no setor de saúde é um conceito poderoso que permite aos indivíduos terem controle sobre suas informações de saúde e processos de tomada de decisão. Isso é evidente em vários cenários, como a gestão de consentimento, onde os pacientes podem usar soluções de identidade auto-soberana para gerenciar o consentimento para compartilhar seus dados de saúde com os provedores de saúde. Por exemplo, um paciente pode conceder acesso temporário a registros médicos específicos para um especialista para uma segunda opinião, garantindo transparência e controle sobre quem pode visualizar suas informações.

Com a identidade descentralizada, os pacientes podem participar ativamente na criação de planos de tratamento personalizados com base em seus dados de saúde e preferências. Isso permite que um paciente com uma condição crônica colabore com os provedores de saúde para adaptar um plano de cuidados que se alinha com seu estilo de vida e metas, promovendo autonomia nas decisões de saúde.

Além disso, os pacientes podem aproveitar a tecnologia blockchain para compartilhar de forma segura dados de saúde em tempo real de dispositivos vestíveis ou ferramentas de monitoramento remoto com sua equipe de saúde. Isso permite o monitoramento proativo de métricas de saúde e intervenções oportunas, capacitando os pacientes a assumir o controle de sua saúde e bem-estar. Através de sistemas de EHR baseados em blockchain, os pacientes podem ter a propriedade de seus dados de saúde e controlar quem pode acessá-los e atualizá-los.

Essa propriedade capacita os indivíduos a manter registros de saúde precisos e abrangentes, garantindo a continuidade dos cuidados em diferentes ambientes e provedores de saúde. Finalmente, os pacientes podem optar por contribuir com seus dados de saúde identificados para estudos de pesquisa ou ensaios clínicos usando soluções de identidade auto-soberana. Ao controlar o uso de seus dados para fins de pesquisa, os indivíduos podem apoiar avanços médicos enquanto mantêm a privacidade e a autonomia sobre suas informações.

Viabilização da melhora dos dados de tratamento remoto:

Os serviços de saúde remotos aprimorados pela tecnologia blockchain oferecem uma maneira segura e eficiente de fornecer cuidados de saúde à distância, revolucionando o modelo tradicional de prestação de cuidados de saúde. Ao aproveitar a natureza descentralizada e à prova de violação do blockchain, os provedores de saúde remotos podem garantir a integridade, segurança e privacidade dos dados do paciente durante consultas virtuais, monitoramento e tratamento. O blockchain permite transações transparentes e rastreáveis, possibilitando o compartilhamento seguro de informações de saúde sensíveis entre diferentes entidades e sistemas de saúde remotamente. Esta tecnologia também facilita processos de autenticação e autorização contínuos, garantindo que apenas indivíduos autorizados tenham acesso aos dados do paciente.

Além disso, as soluções de saúde remota baseadas em blockchain melhoram a interoperabilidade dos dados, permitindo que os provedores de saúde acessem informações do paciente abrangentes e atualizadas, independentemente das barreiras geográficas. No geral, o blockchain na saúde remota não apenas aprimora a segurança e a privacidade dos dados, mas também promove confiança, eficiência e qualidade nos serviços de saúde remota, levando finalmente a melhores resultados para os pacientes e à prestação de cuidados de saúde [ES3].

Pesquisa e evolução do setor médico:

As inovações mencionadas, como blockchain, identidade descentralizada e identidade auto-soberana, têm grande potencial para aprimorar a pesquisa em saúde e outros campos. Essas tecnologias prometem aumentar a integridade, segurança e interoperabilidade dos dados de pesquisa. Com o uso do blockchain, é possível armazenar dados de maneira segura e manter registros transparentes, resultando em pesquisas mais confiáveis e replicáveis. As

soluções de identidade descentralizada possibilitam o compartilhamento e acesso seguro aos dados, com controle sobre identidades e permissões, o que facilita a colaboração e o intercâmbio de informações. A implementação de identidade auto-soberana prioriza a privacidade dos dados e o gerenciamento de consentimento, assegurando a aderência às regulamentações e fortalecendo a confiança nos métodos de pesquisa. Em resumo, a adoção de blockchain e identidade descentralizada pode simplificar o gerenciamento de dados, aumentar a transparência e incentivar a inovação na pesquisa.[ES26] [ES30]

6.2.3 PPS3. Quais os desafios enfrentados pela aplicação dessas tecnologias no contexto de saúde?

Tabela 11 - Desafios e estudos relacionados

Desafios	**Estudos**
Adoção	[ES2], [ES20], [ES21], [ES22], [ES25], [ES27], [ES30], [ES32], [ES42], [ES73]
Regulamentação	[ES1], [ES2], [ES20], [ES21], [ES25], [ES26], [ES32], [ES34], [ES52], [ES60], [ES73]
Dados	[ES1], [ES2], [ES8], [ES15], [ES20],[ES21], [ES25], [ES26], [ES27], [ES30], [ES32], [ES34], [ES43], [ES46], [ES52], [ES54], [ES60], [ES73]
Interoperabilidade	[ES1], [ES2], [ES8], [ES15], [ES20],[ES21], [ES27], [ES32], [ES34], [ES52], [ES54], [ES55], [ES58], [ES60], [ES73]
Custos	[ES2], [ES8], [ES20], [ES25], [ES27], [ES47], [ES60], [ES73]
Escalabilidade	[ES2], [ES20], [ES21], [ES22], [ES25], [ES27], [ES30], [ES32], [ES42], [ES45], [ES46], [ES52], [ES54], [ES55], [ES58], [ES60], [ES66], [ES73]

Fonte: O autor.

Evidências:

"O download e gerenciamento de dados históricos fora da cadeia, no entanto, têm seus próprios desafios: (1) os dados baixados não fazem parte do protocolo de consenso. Como resultado, um mecanismo adicional é necessário para garantir sua resistência a alterações e fidelidade à fonte de dados da blockchain a fim de cumprir os requisitos regulatórios, (2) para permitir a consulta de grandes volumes de dados históricos, eles primeiro precisam ser baixados e posteriormente indexados (usando um índice externo). Isso pode ser bastante lento e, portanto, não adequado para consultas em tempo real, (3) os dados históricos só podem ser acessados por nós que gerenciam ativamente seu histórico e, como resultado, não podem ser sincronizados e autenticados usando um protocolo de consenso entre nós participantes para garantir que os mesmos dados sejam compartilhados." (**ES1**, tradução do autor)[45]

"A adoção pela indústria e pelo governo. Compreender as diferentes implementações do blockchain e suas capacidades representa desafios para os tomadores de decisão quando se trata de governança de dados, regulamentações de privacidade e segurança e padrões. Para resolver tais questões, os formuladores de políticas devem dedicar tempo para avaliar a tecnologia, buscar o desenvolvimento de padrões e obter experiência com a tecnologia." (**ES2**, tradução do autor)[46]

"No entanto, uma rede blockchain privada e com permissão, sozinha não é suficiente para atender aos requisitos do GDPR e os problemas permanecem. (...) uma Avaliação de Impacto de Proteção de Dados é crucial para identificar riscos que podem ser amplificados devido à natureza imutável permanente do blockchain. Um modelo eficaz de governança de dados também é necessário para mitigar riscos, por exemplo, o ponto de venda do blockchain é sua natureza verificável, mas isso não garante a precisão dos dados inseridos na cadeia; a governança eficiente é essencial para alcançar esses objetivos." (**ES21**, tradução do autor)[47]

---

[45] No original: Downloading and managing historical data-of-chain, however, has its own challenges: (1) the downloaded data are not part of the consensus protocol. As a result, an additional mechanism is required to ensure their tamper-resistance and fidelity to the blockchain data source in order to adhere to regulatory requirements, (2) to enable querying of large volumes of historical data, they first need to be downloaded and further indexed (using an external index). This can be quite slow and hence, not suitable for real time queries, (3) the historical data can only be accessed by nodes that actively manage their history and, as a result, cannot be synchronized and authenticated using a consensus protocol between participating nodes to ensure the same data are shared

[46] No original: Industry and government adoption. Grasping the different implementations of blockchain and their capabilities pose challenges for decision makers when it comes to data governance, privacy and security regulations, and standards. To address such issues, policy makers should take time to assess the technology, look for standards to be developed, and gather experience with the technology

[47] No original: A private permissioned blockchain network alone, however, is not enough to meet GDPR requirements and issues remain. (...) a Data Protection Impact Assessment is crucial to identify risks which may be amplified due to the permanent immutable nature of blockchain. An effective data governance model is also

"Isso, no entanto, pode se alinhar à questão de se o blockchain é um exagero; se um usuário perder uma chave privada, então qualquer ativo digital, ou no nosso caso um certificado de imunidade, é perdido. É computacionalmente inviável regenerar a mesma chave privada. Isso pode ser um grande desafio para o público em geral e pode-se questionar se esse nível de segurança é necessário. Aplicando o fluxograma 'Precisamos de blockchain?' do Departamento de Ciência e Tecnologia da Segurança Interna dos EUA, descobrimos que, embora ainda possa haver um caso de uso útil para o blockchain, existem algumas etapas que indicam que um banco de dados criptografado seria suficiente para o armazenamento de certificados de saúde." (**ES21**, tradução do autor)[48]

"A força do blockchain em garantir a integridade dos dados por meio da imutabilidade pode ter um custo, em comparação com ter a mesma garantia em uma aplicação centralizada. Os custos de transação foram encontrados para serem mais altos para blockchains sem permissão quando comparados a soluções centralizadas, e as aplicações de blockchain podem custar significativamente mais para operar do que um equivalente centralizado baseado na nuvem, mesmo após controlar as taxas de utilização do serviço em nuvem." (**ES2**, tradução do autor)[49]

"Independentemente de sua utilidade, a adoção da tecnologia blockchain vem com sua parcela justa de barreiras. Enquanto a capacidade de armazenamento em DLT de blockchain é limitada, esses limites de gás (ou seja, a quantidade máxima de computação permitida) são desafiados pelo uso de padrões especializados." (**ES8**, tradução do autor)[50]

---

necessary to mitigate risks, for example blockchain's selling point is its verifiable nature but this doesn't guarantee the accuracy of data input on the chain; efficient governance is essential to reaching these goals

[48] No original: This however may align with the question of whether blockchain is an overkill; if a user loses a private key, then any digital asset, or in our case an immunity certificate, is lost. It is computationally infeasible to regenerate the same private key. This might be a big ask for the general public and one may question whether this level of security is necessary. By applying the US Department of Homeland Security Science and Technology Directorate's 'Do we need blockchain?' flowchart we found although there may still be a useful blockchain use case, there are some stages that indicate that an encrypted database would be sufficient for the storage of health certificates

[49] No original: Blockchains' strength in guaranteeing data integrity through immutability may come at a premium, relative to having the same guarantee in a centralized application. Transaction costs have been found to be higher for permissionless blockchains when compared to centralized solutions, and blockchain applications can cost significantly more to operate than a cloud-based centralized equivalent, even after controlling for cloud service utilization fees.

[50] No original: Irrespective of its usefulness, the adoption of blockchain technology comes with its fair share of barriers. While storage capacity on blockchain ledgers is limited, these gas limits (i.e., the maximum amount of computation allowed) are challenged by using specialized flyweight patterns.

"No entanto, a integração com diversos sistemas legados tem seus desafios tecnológicos, especialmente do ponto de vista da padronização ontológica e semântica e interoperabilidade, o que é uma preocupação prevalente nos sistemas de saúde devido ao seu impacto direto na segurança e privacidade do paciente. Além disso, adotar tecnologias novas e disruptivas como blockchain é um dilema, especialmente em ambientes de saúde, onde pessoal envolvido com gerenciamento de dados são relutantes em adotar novas tecnologias e resistentes à mudança na cultura de gerenciamento de dados." (**ES15**, tradução do autor)[51]

"As potenciais desvantagens incluem adoção limitada, complexidade, alto consumo de energia, desafios regulatórios, falta de padronização, problemas de escalabilidade, funcionalidade limitada, dependência de fornecedores terceirizados e preocupações legais e éticas. Como uma nova tecnologia, o blockchain ainda está sendo adotado, e os profissionais de saúde devem se familiarizar mais com a tecnologia para usá-la efetivamente. Além disso, conformidade regulatória e padronização de dados também podem representar desafios para a adoção da tecnologia blockchain na saúde. Como tal, as organizações de saúde devem avaliar cuidadosamente os benefícios e riscos potenciais antes de usar a tecnologia blockchain na área da saúde." (**ES20**, tradução do autor)[52]

"Por fim, a complexidade e novidade da tecnologia Blockchain podem representar um limite para a adoção da solução Block-Health. Na verdade, muitas empresas podem perceber o Blockchain como uma tecnologia complexa difícil de implantar e demorada para manter" (**ES22**, tradução do autor)[53]

"A maioria dos pacientes provavelmente não possui capacidade para estabelecer tal sistema devido ao tempo, habilidades técnicas ou restrições monetárias" (**ES25**, tradução do autor)[54]

---

[51] No original: However, integration with diverse legacy systems has its technological challenges, particularly from ontological and semantic standardization and interoperability point of view, which is a pervasive concern in healthcare systems due to its direct impact on patient safety and privacy. Moreover, adopting new and disruptive technology like blockchain is a predicament, particularly in healthcare settings, where personnel involved with data management are reluctant to adopt new technology and resistant to change in data management culture

[52] No original: The potential disadvantages include limited adoption, complexity, high energy consumption, regulatory challenges, lack of standardization, scalability issues, limited functionality, dependence on third- party vendors, and legal and ethical concerns. As a new technology, blockchain is still being adopted, and healthcare professionals must become more familiar with the technology to use it effectively. Moreover, regulatory compliance and data standardization could also pose challenges to the adoption of blockchain technology in healthcare. As such, healthcare organizations must carefully evaluate the potential benefits and risks before using blockchain technology in healthcare

[53] No original: Finally, the complexity and novelty of the Blockchain technology can represent a limit for the adoption of the Block- Health solution. In fact, many companies can perceive the Blockchain as a complex technology difficult to deploy and time-consuming to maintain

[54] No original: Most patients probably do not have capabilities to establish such a system due to time, technical skills, or monetary constraints

"Para garantir a conformidade com os regulamentos atuais, precisamos esclarecer políticas adicionais de endosso. No entanto, a propriedade existente de dados médicos continua sendo um problema, e atualmente não existem padrões para usar blockchain para lidar com a propriedade em conformidade com os frameworks legais como a Lei de Portabilidade e Responsabilidade do Seguro de Saúde. HIPAA e outras Leis Europeias (ou seja, GDPR)" (**ES26**, tradução do autor)[55]

"No entanto, existem desafios que devem ser considerados ao adotar a tecnologia blockchain na área da saúde. O primeiro desafio está relacionado à transparência e confidencialidade. Neste sistema, todos podem ver tudo, então há alta transparência e baixa confidencialidade. A transparência das informações durante uma transação é geralmente considerada uma limitação. Além disso, mesmo se um usuário for anônimo, ao usar valores hash, ele pode ser identificado inspecionando e analisando as informações de transação publicamente disponíveis na rede. Isso é um problema crítico para aplicativos de saúde, porque os dados relacionados ao paciente são altamente sensíveis. O segundo desafio é velocidade e escalabilidade. Os tempos de transação podem ser longos, dependendo do protocolo usado, e uma restrição de velocidade pode limitar a escalabilidade de aplicativos baseados em blockchain" (**ES30**, tradução do autor)[56]

"As limitações da tecnologia blockchain foram identificadas como confidencialidade, velocidade, escalabilidade e ameaça de ataque malicioso, ou seja, ataque de 51%. Os autores identificaram essas limitações como críticas para o setor de saúde ou biomédico, pois estão sendo usadas para armazenar registros médicos ou clínicos sensíveis." (**ES45**, tradução do autor)[57]

---

[55] No original: To guarantee compliance with current regulations, we need to clarify additional endorsement policies. However, existing medical data ownership remains an issue, and there are presently no standards for using blockchain to handle ownership in line with legal frameworks such as the Health Insurance Portability and Accountability Act. HIPAA and other European Law (i.e., GDPR).

[56] No original: However, there are challenges that must be considered when adopting blockchain technology in healthcare. The first challenge is related to transparency and confidentiality. In this system everyone can see everything, so there is high transparency and low confidentiality. Transparency of information during a transaction is usually considered a limitation. In addition, even if a user is anonymous, when using hash values, they can be identified by inspecting and analyzing the transaction information publicly available on the network. This is a critical issue for healthcare applications because patient-related data is highly sensitive. The second challenge is speed and scalability. Transaction times can be long, depending on the protocol used and a speed constraint can limit the scalability of blockchain-based applications

[57] No original: The limitations of blockchain technology were identified to be confidentiality, speed, scalability and threat of malicious attack, i.e., 51% attack. The authors identified these limitations to be critical for the healthcare or biomedical sector as they are being used to store sensitive medical or clinical records.

"De fato, o problema de escalabilidade, precisamente em termos de baixo throughput, alta latência, drenagem de recursos e altura do razão, reduz a praticidade de qualquer sistema baseado em blockchain em grande escala. Na verdade, à medida que o número de transações processadas aumenta, o espaço de armazenamento necessário para o registro imutável aumenta drasticamente." (**ES46**, tradução do autor)[58]

"A rede IPFS é usada aqui porque o custo financeiro de armazenar arquivos grandes no blockchain é muito alto. Neste caso, uma rede IPFS pode ser usada para armazenar registros de saúde, enquanto o blockchain armazena apenas o hash de dados e metadados." (**ES47**, tradução do autor)[59]

"Outra limitação são as restrições de escalabilidade do protocolo blockchain. Ethereum pode lidar com aproximadamente 13-15 transações por segundo até o momento. A qualquer momento, o número total de transações, incluindo a concessão de permissões, seleção de pontos de toque e inserção/recuperação de chaves de descriptografia, pode exceder o limite." (**ES52**, tradução do autor)[60]

"A principal limitação de nossa abordagem é a configuração necessária em cada instituição de saúde. Cada instituição de saúde deve fornecer pelo menos um nó para o blockchain e concluir o processo de conversão de servidores em adaptadores de blockchain. Limitações secundárias incluem a dependência do desempenho do modelo nas propriedades dos nós do blockchain, a necessidade potencial dos pacientes fornecerem nós de blockchain para dados gerados por dispositivos da Internet das Coisas (IoT) e a necessidade de as instituições concordarem com um padrão de interoperabilidade como os Recursos de Interoperabilidade de Assistência Médica Rápida (FHIR)." (**ES52**, tradução do autor)[61]

---

[58] No original: In point of fact, the scalability issue, precisely in terms of low throughput, high latency, resource draining, and ledger height, lower the practicality of any blockchain-based system on a large-scale. Actually, as the number of processed transactions builds up the storage space required for the immutable ledger increases drastically.

[59] No original: The IPFS network is used here because the financial cost of storing large files on the blockchain is very high. In this case, an IPFS network can be used to store health records, while the blockchain stores only the data hash and metadata.

[60] No original: Another limitation is scalability constraints from the blockchain protocol. Ethereum can handle roughly 13- 15 transactions per second as of today. At any moment, the total number of transactions, including permission granting, touchpoint selection, and decrypt key insertion/retrieval, may exceed the limit.

[61] No original: The main limitation of our approach is the setup required at each healthcare facility. Each healthcare facility is required to provide at least one node to the blockchain and complete the process of converting servers into blockchain adapters. Secondary limitations include the dependence of the model's performance on the blockchain nodes' properties, the potential need for patients to provide blockchain nodes for data generated by Internet of Things (IoT) devices, and the need for facilities to agree on an interoperability standard such as Fast Healthcare Interoperability Resources (FHIR

"Como a tecnologia ainda está em fase embrionária, é certo que haverá desafios para sua aplicação no setor de saúde. Falta qualquer estrutura de padronização. Há uma necessidade de padrões devidamente autenticados e certificados que atendam aos requisitos internacionais para sistemas no setor de saúde ao redor do mundo, incluindo a natureza dos dados compartilhados na rede, uma avaliação do tamanho e o formato apropriado para troca sobre a rede blockchain." (**ES60**, tradução do autor)[62]

"Primeiro, encontrar maneiras de dimensionar a infraestrutura blockchain mantendo um desempenho ótimo é uma consideração significativa. Segundo, convencer os profissionais de saúde a adotar o sistema de verificação de credenciais baseado em blockchain pode encontrar resistência e ceticismo. Além disso, há uma necessidade de um certo nível de experiência técnica para construir nosso sistema proposto. Terceiro, o custo relacionado à implementação e sustentação da infraestrutura de uma rede blockchain pode potencialmente desencorajar organizações a adotarem sua adoção. Além disso, há um desafio em alcançar a troca de dados perfeita e a interoperabilidade entre diferentes sistemas, garantindo o funcionamento suave do sistema enquanto se cumpre com as regulamentações relevantes e requisitos legais." (**ES73**, tradução do autor)[63]

“Armazenar dados médicos em blockchain é caro, por isso sugerimos um mecanismo de gerenciamento de dados seguro fora da cadeia” (**ES60**, tradução do autor)[64]

[62] No original: Because the technology is still in its infancy, there are bound to be challenges to its application to the health sector. It lacks any standardization structures. There is a need for properly authenticated and certified standards that meet international requirements for systems in the health sector around the world, including the nature of the data shared on the network, an evaluation of size and the appropriate format for exchange over the blockchain network

[63] No original: First, finding ways to scale the blockchain infrastructure while maintaining optimal performance is a significant consideration. Second, convincing healthcare professionals to embrace the blockchain-based credential verification system can be met with resistance and skepticism. Additionally, there is a need for a certain level of technical expertise to build our proposed system. Third, the cost related to implementing and sustaining the infrastructure of a blockchain network could potentially discourage organizations from embracing its adoption. Moreover, there is a challenge in achieving seamless data exchange and interoperability between different systems, ensuring the smooth operation of the system while ensuring compliance with relevant regulations and legal requirements

[64] No original: Storing medical data on blockchain is expensive, so we suggest an off-chain secure data management mechanism

Adoção:

A implementação de tecnologias emergentes como blockchain, identidade descentralizada e identidade autossuficiente no setor de saúde apresenta desafios, principalmente na aceitação do usuário e na complexidade operacional. As empresas podem perceber o blockchain como uma solução complexa e demorada, o que pode inibir sua adoção generalizada. A tecnologia, sendo complexa e inovadora, pode ser vista como uma barreira para a implementação da solução. Além disso, o caráter inovador das soluções de identidade descentralizada e auto suficiente pode ser um obstáculo para usuários não familiarizados com esses conceitos. Para superar esses obstáculos, recomenda-se a utilização de máquinas virtuais pré-configuradas ou contêineres que incluam os módulos de software necessários, simplificando assim o processo de integração. Fornecendo ferramentas de fácil uso e diretrizes claras para implementação, as instituições de saúde podem superar as dificuldades de adoção e aproveitar os benefícios dessas tecnologias avançadas para o gerenciamento seguro e compartilhamento de dados de saúde [ES21, ES22].

Regulamentação:

A regulamentação é um componente chave na estruturação dos sistemas de saúde, assegurando a aderência às normativas, a proteção dos direitos dos pacientes e o fomento de condutas éticas. Contudo, os desafios regulatórios associados a tecnologias inovadoras como a blockchain trazem complexidades particulares para as entidades de saúde. Os artigos examinados iluminam os obstáculos regulatórios em sistemas de saúde que integram a blockchain.

Um desafio primordial é assegurar a conformidade com as regulamentações e leis aplicáveis ao adotar a blockchain na saúde. As entidades precisam manobrar em um ambiente regulatório intrincado para que seus sistemas baseados em blockchain estejam em conformidade com as legislações de proteção de dados, normas de privacidade e padrões do setor. A conformidade regulatória é vital para proteger as informações dos pacientes, minimizar riscos e preservar a confiança no ecossistema de saúde.

Os textos também abordam as dificuldades de integrar a blockchain aos frameworks de saúde existentes, considerando as questões regulatórias. Os provedores de saúde devem alinhar as soluções de blockchain com as diretrizes regulatórias, mantendo a segurança dos dados, a privacidade e a interoperabilidade com sistemas legados. A observância das normas

regulatórias e a implementação da blockchain na gestão de dados apresentam desafios em termos de governança de dados, protocolos de compartilhamento de informações e mecanismos de proteção de dados.

A necessidade de enfrentar os desafios regulatórios também é ressaltada no contexto de esquemas seguros para o compartilhamento de registros eletrônicos de saúde. As entidades de saúde devem navegar pelos marcos regulatórios para implementar controles de acesso seguros, protocolos de criptografia e práticas de gestão de dados que estejam em conformidade com as regulamentações do setor. Assegurar a conformidade regulatória é crucial para proteger a privacidade dos pacientes, prevenir violações de dados e manter a integridade dos registros eletrônicos de saúde.

Dados e Interoperabilidade:

A administração de dados e a interoperabilidade são elementos cruciais nos sistemas de saúde, com a tecnologia blockchain trazendo novas possibilidades e desafios. A blockchain pode transformar a gestão de dados ao oferecer uma plataforma segura e transparente para armazenar e compartilhar informações de saúde. Contudo, há desafios significativos a serem superados para maximizar os benefícios da blockchain na saúde.

Um desafio importante é gerir de forma segura os dados de saúde, mantendo a interoperabilidade entre diferentes prestadores de cuidados. A descentralização inerente à blockchain requer novas abordagens para a governança de dados, controle de acesso e protocolos de compartilhamento. As organizações de saúde devem gerir dados num registro distribuído, mantendo a interoperabilidade com sistemas existentes para assegurar uma troca de dados fluida e a continuidade dos cuidados.

Os artigos também ressaltam a necessidade de abordar a integridade e privacidade dos dados ao implementar soluções blockchain na gestão de dados de saúde. A blockchain proporciona um registro imutável e transparente, mas assegurar a integridade dos dados e a proteção da privacidade são desafios que envolvem conformidade regulatória, criptografia e acesso seguro aos dados. Os prestadores de saúde precisam superar esses desafios para construir confiança, proteger as informações dos pacientes e cumprir com as leis de proteção de dados.

Além disso, é crucial superar os desafios de interoperabilidade ao integrar a blockchain nos sistemas de saúde. As discrepâncias de interoperabilidade entre plataformas blockchain e sistemas legados podem complicar o intercâmbio de dados de saúde, prejudicar a

coordenação dos cuidados e restringir o acesso às informações dos pacientes. As organizações de saúde devem enfrentar esses desafios desenvolvendo formatos de dados padronizados, protocolos interoperáveis e mecanismos seguros de troca de dados para garantir a continuidade dos dados e a interoperabilidade entre sistemas diversos.

Custos e Escalabilidade:

A gestão de custos é um fator decisivo na adoção da tecnologia blockchain em sistemas de saúde. Apesar dos benefícios como segurança aprimorada, integridade de dados e interoperabilidade, os custos de implementação e manutenção representam um desafio significativo.

O equilíbrio entre os benefícios da blockchain e os custos associados é crucial. As organizações de saúde devem considerar as implicações financeiras, incluindo custos iniciais, despesas contínuas e recursos para treinamento em blockchain. A eficiência de custo é vital na tomada de decisão, ponderando os benefícios em relação ao investimento necessário.

Os desafios de escalabilidade e uso de recursos nas redes blockchain podem impactar a eficiência de custos, especialmente em ambientes de saúde de grande escala. Problemas como escalabilidade limitada, latência e operações que exigem muitos recursos podem elevar os custos operacionais. As organizações precisam otimizar o uso de recursos e minimizar custos operacionais para garantir a sustentabilidade das soluções blockchain.

A falta de escalabilidade afeta o rendimento, a latência e o uso de recursos nas redes blockchain, impactando a velocidade e eficiência do processamento de dados. As instituições de saúde devem superar esses obstáculos para otimizar o desempenho da rede, melhorar a troca de dados e atender aos requisitos de escalabilidade dos aplicativos de saúde.

Avaliar o retorno sobre o investimento e a relação custo-benefício é essencial. As organizações devem analisar a viabilidade financeira dos projetos de blockchain, considerando o custo total de propriedade, economias potenciais e oportunidades de receita.

Em suma, os desafios de custo, escalabilidade e uso de recursos devem ser cuidadosamente avaliados. Com análises detalhadas de custos e priorização de soluções rentáveis, as organizações de saúde podem superar esses desafios e aproveitar a blockchain para melhorar a segurança dos dados, interoperabilidade e eficiência dos cuidados de saúde. Equilibrar custos e benefícios é fundamental para promover inovação, melhorar resultados dos pacientes e maximizar o valor da blockchain na saúde.

7. DISCUSSÃO

A tecnologia blockchain tem despertado um interesse crescente em diversas áreas, e a saúde não é exceção. A aplicação dessa tecnologia no setor da saúde promete revolucionar a forma como os dados são compartilhados, armazenados e protegidos. A descentralização e a distribuição de dados proporcionadas por essa inovação têm o potencial de melhorar a segurança, transparência e eficiência dos sistemas de saúde.

Os sistemas de saúde tradicionais estão sob uma pressão constante para evoluir, enfrentando o desafio de se adaptar rapidamente às crescentes demandas e inovações tecnológicas que exigem uma transformação que abrace a telemedicina e a digitalização dos registros de saúde. Essas mudanças são fundamentais para aprimorar a acessibilidade, a eficiência e a qualidade do atendimento ao paciente.

A implementação de tecnologias inovadoras, incluindo blockchain, DID e SSI é essencial para a evolução dos sistemas de saúde. A pesquisa realizada indica que a aplicação dessas tecnologias pode resultar em impactos significativas em várias pilares fundamentais:

- Interoperabilidade: Facilita a comunicação e o intercâmbio de informações entre diferentes sistemas de saúde, promovendo uma rede mais conectada e eficiente.
- Privacidade: Reforça a proteção dos dados pessoais dos pacientes, assegurando que apenas indivíduos autorizados tenham acesso às informações sensíveis.
- Dados: Melhora a organização, o armazenamento e a análise de grandes volumes de dados de saúde, contribuindo para uma tomada de decisão mais informada.
- Segurança: Aumenta a resistência contra ataques cibernéticos e vazamentos de dados, protegendo as informações contra acessos não autorizados.
- Integridade: Garante a precisão e a consistência dos dados ao longo do tempo, evitando alterações não autorizadas ou acidentais.
- Transparência: Proporciona uma visão clara e auditável das operações e transações, aumentando a confiança no sistema de saúde.
- Autenticação: Assegura que os usuários sejam quem dizem ser, garantindo uma autonomia maior sobre seus dados

A sua aplicabilidade transcende os aspectos técnicos, estendendo-se a casos práticos no cotidiano dos sistemas de saúde. A análise dos artigos permite afirmar que a adoção dessas tecnologias está intrinsecamente ligada a melhorias em áreas vitais, tais como:

- Segurança dos dados e privacidade
- Interoperabilidade e rastreamento de dados referentes a pacientes e suplementos.
- Autonomia e controle dos dados pelo paciente.
- Saúde remota.
- Pesquisa e evolução dos dados.

Cada um desses pontos pode ser aplicado com um exemplo prático e real de uma unidade que pertence a cadeia de saúde, como:

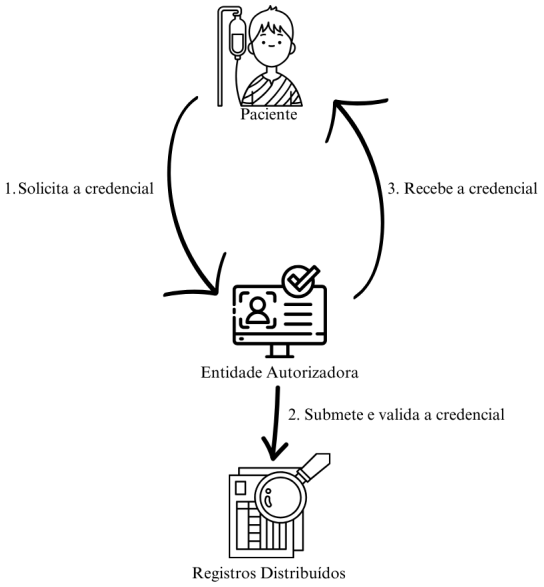
- **Sistema de Registros de Saúde Eletrônicos:** A implementação de blockchain pode aprimorar a interoperabilidade e a segurança dos registros eletrônicos de saúde, conferindo aos pacientes maior controle sobre seus dados.
- **Rede de Hospitais:** A conexão de hospitais por meio de uma rede descentralizada de registros pode facilitar o compartilhamento seguro de informações, promovendo a eficiência e a qualidade do acompanhamento remoto.
- **Rede de Laboratórios:** O armazenamento de registros de exames em blockchain assegura a integridade e a autenticidade dos resultados, fortalecendo a confiança no processo diagnóstico.
- **Rede de Farmácias:** O uso de blockchain para rastrear a cadeia de suprimentos de medicamentos pode prevenir fraudes e garantir a segurança dos produtos farmacêuticos.

A seguir temos uma demonstração de uma arquitetura básica referente ao uso de uma SSI, abstraindo suas tecnicidades e exemplificando visualmente como funcionaria a autenticação do usuário mediante uma instituição.

Primeira fase:

- O paciente requisita uma credencial a uma entidade autorizada a emitir tal documento.
- O verificador submete a credencial e sua assinatura digital a uma DLT para servir como referência de validação.
- Após a verificação, o verificador concede a credencial ao paciente, que a armazena em sua carteira digital.

Figura 12 - Fluxo de um paciente realizando uma cadastro em uma SSI

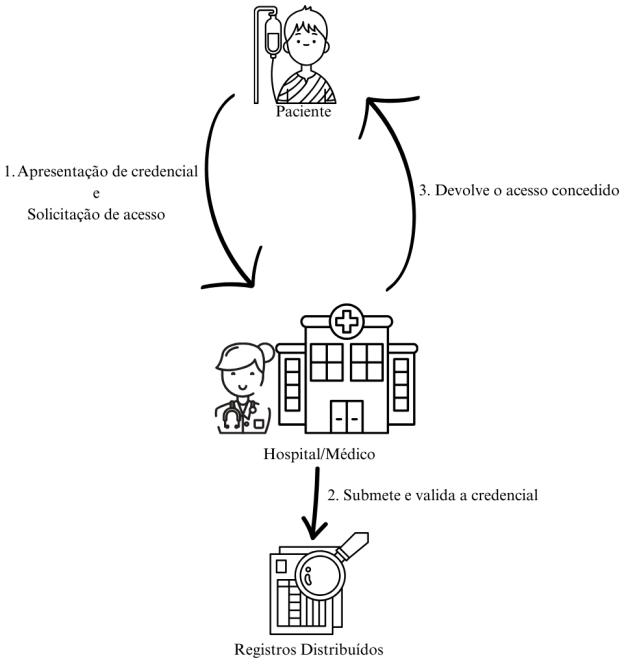


Fonte: O autor

Segunda fase:

- O paciente solicita ao prestador de serviços, apresentando a credencial válida, o acesso aos seus dados pessoais.
- O prestador de serviços consulta a DLT para confirmar a autenticidade das credenciais.
- Com a verificação concluída e aprovada pela DLT, o prestador de serviços libera o acesso solicitado pelo paciente.

Figura 13 - Fluxo de um paciente se autenticando em uma organização com SSI



Fonte: O autor.

7.2 Desafios

A implementação de Blockchain, DID e SSI nos sistemas de saúde é um processo complexo, repleto de desafios que exigem uma abordagem colaborativa e detalhada para serem superados. Baseado no estudo executado, foi identificado os seguintes pontos importantes para levar em consideração os desafios da tecnologia no contexto de saúde:

- Adoção
- Regulamentação
- Dados
- Interoperabilidade
- Custos
- Escalabilidade

A falta de processos de integração seguros que conectem sistemas de saúde independentes e também a adequação e fusão de sistemas legados com novos sistemas descentralizados para formar uma rede acessível é um problema significativo. Isso é exacerbado por barreiras à interoperabilidade, como software incompatível e falta de acesso a

dados fora do ambiente de saúde. A troca contínua de dados críticos entre diferentes prestadores de cuidados de saúde é dificultada, aumentando o risco de erros e atrasos no tratamento, sendo inadmissível principalmente devido às regulamentações da área como a Lei de Portabilidade e Responsabilidade de Provedores de Saúde (HIPAA), uma legislação dos Estados Unidos criada em 1996. Ela estabelece padrões para a proteção de registros médicos e outras informações de saúde, garantindo a confidencialidade, integridade e disponibilidade desses dados .

O consentimento e controle dos pacientes sobre seus dados são críticos e requerem sistemas que permitam aos pacientes gerenciar o compartilhamento de suas informações, devido a natureza imutável da tecnologia a inserção incorreta de dados pode se tornar um problema devido a sua falta de flexibilidade na hora de executar uma transação, e, graças a sua transparência, isso pode influenciar negativamente em algum processo subsequente.

Padronizar formatos de dados e esquemas de codificação é crucial para melhorar a troca de dados e a interoperabilidade entre os sistemas de saúde. Investimento em infraestrutura técnica robusta é necessário para coletar, armazenar e analisar grandes volumes de dados de saúde.

A comprovação e verificação de identidade são críticas, especialmente considerando as limitações das soluções atuais de Gerenciamento de Identidade baseadas em blockchain. Os altos custos de desenvolvimento associados aos sistemas de saúde baseados em blockchain são um desafio, exigindo definições claras dos tipos de custos para todos os stakeholders.

Para abordar esses desafios, é necessário um esforço colaborativo entre organizações de saúde, fornecedores de tecnologia e órgãos reguladores, adotando tecnologias interoperáveis como o Blockchain e seguindo as melhores práticas de privacidade e segurança de dados.

7.3 Tecnologia, Brasil e Saúde

7.3.1 Contexto

A inovação em saúde é um tema de grande relevância no cenário brasileiro, dada a magnitude e complexidade do sistema público de saúde do país. O Brasil, apesar de seu potencial, ainda enfrenta desafios significativos em relação à inovação. Isso é evidenciado pelo seu posicionamento no Índice Global de Inovação (IGI), onde ocupa a 49ª posição entre 126 países avaliados, ficando atrás dos da China e da Índia que fazem parte do BRICS [100].

Este posicionamento reflete a necessidade de aprimoramentos no ecossistema de inovação em saúde brasileiro.

A integridade e a segurança dos dados de saúde representam um pilar fundamental para o funcionamento eficaz do SUS no Brasil. Recentemente, uma série de eventos colocou em xeque a gestão desses dados, suscitando preocupações e debates significativos.

Inicialmente, um levantamento realizado pelo jornal O Globo revelou que ao menos 15 estados brasileiros relataram problemas com os sistemas de dados do Ministério da Saúde [101]. Essas instabilidades, decorrentes de um ataque hacker, resultaram em um apagão de dados que impediu cientistas de estimarem a gravidade da pandemia no país. A situação alarmante evidenciou a vulnerabilidade dos sistemas e a necessidade urgente de medidas robustas de segurança cibernética.

Em um desdobramento relacionado, o Tribunal de Contas da União (TCU) abriu uma investigação sobre um ex-diretor do Departamento de Informática do SUS (DATASUS), que migrou os dados para a Amazon Web Services e, posteriormente, assumiu um cargo na mesma empresa [102]. Esse caso levantou questões sobre conflito de interesses e a ética na gestão de dados públicos, além de potenciais riscos à soberania nacional.

Adicionalmente, o Ministério da Saúde admitiu falhas nos dados sobre vacinados, com a ausência de registros de ao menos 30 milhões de doses aplicadas [103]. Esse cenário de desencontro de informações entre as bases de dados municipais, estaduais e federais ressalta a importância de uma infraestrutura de dados coesa e bem gerida.

Esses eventos sublinham a necessidade de uma governança de dados mais transparente e segura, que possa garantir a confiabilidade das informações e, consequentemente, a efetividade das políticas públicas de saúde. A modernização do DATASUS, com a implementação de sistemas integrados e a adoção de práticas de segurança cibernética avançadas, torna-se imperativa para restaurar a confiança no sistema de saúde e proteger os dados sensíveis da população brasileira.

Um dos aspectos fundamentais para impulsionar a inovação em saúde no Brasil é a compreensão da importância de conhecer e mensurar os processos e resultados. Conforme destacado por Mazzucato (apud AGUILLAR et al, 2021), a inovação não se limita a corrigir mercados, mas também a criá-los, direcionando a demanda de inovação para impactar positivamente a vida de milhões de pessoas. Para inovar de forma eficaz, é essencial entender quais processos impactam nos resultados desejados e verificar se as melhorias almejadas foram alcançadas [104].

No contexto brasileiro, a ausência de ferramentas que identifiquem com precisão os problemas do sistema de saúde é um dos principais obstáculos para a inovação. A dispersão e a falta de qualidade dos dados de saúde dificultam a tomada de decisões qualificadas, prejudicando o avanço da inovação no setor. Além disso, a burocracia pública e as desigualdades regionais também se destacam como entraves para a inovação em saúde no Brasil [104].

Para superar esses desafios, é fundamental investir na construção de um sistema de inovação mais robusto e maduro no setor de saúde. Isso envolve a criação de mecanismos que incentivem a geração de soluções inovadoras, como competições e desafios que estimulem a criatividade e a resolução de problemas específicos, como o exemplo da Índia na melhoria dos equipamentos de proteção individual em hospitais [104].

7.3.2 Avanços e tecnologias

A incorporação de inovações tecnológicas que manipulam dados exige uma avaliação meticulosa das leis pertinentes para assegurar a conformidade, segurança e eficiência das soluções sugeridas. Neste cenário, é imprescindível levar em conta a legislação brasileira vigente relativa à proteção de dados de saúde, interoperabilidade de sistemas, telemedicina e outros elementos cruciais para a saúde digital. A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, tem um papel fundamental na salvaguarda das informações de saúde dos cidadãos brasileiros. A conformidade das soluções de saúde digital com a LGPD é vital para assegurar a privacidade e segurança dos dados dos pacientes, além de prevenir possíveis penalidades legais resultantes de infrações de privacidade [105, 107].

Adicionalmente, a legislação associada à interoperabilidade dos sistemas de saúde é essencial para facilitar a troca segura e eficaz de informações entre diferentes instituições de saúde. A determinação de padrões e protocolos interoperáveis, em linha com as diretrizes estipuladas pelo Ministério da Saúde e pela Agência Nacional de Saúde Suplementar, é crucial para garantir a integração adequada dos sistemas de informação em saúde.

No âmbito da telemedicina, a regulamentação específica, como no Conselho Federal de Medicina a Resolução CFM nº 2.227/2018, é importante para guiar a prática de teleconsulta e telemonitoramento, assegurando a qualidade e segurança dos serviços oferecidos remotamente. A aderência às normas estabelecidas pelo CFM e outras entidades reguladoras é fundamental para garantir a legalidade e ética das atividades de telemedicina [106, 107].

A implementação do programa de Estratégia de Saúde Digital para o Brasil 2020-2028 [107] também é um marco importante no panorama da saúde brasileira, com o objetivo de acelerar a incorporação de inovações em Saúde Digital e promover melhorias nos processos de prevenção, diagnóstico e tratamento. Nesse contexto, é crucial entender os benefícios esperados dessa estratégia e os desafios que precisam ser superados para sua implementação efetiva [107].

A iniciativa visa fortalecer o setor de inovações e pesquisa em saúde no país, envolvendo a "aceleração da absorção de inovação em Saúde Digital por todo o sistema de saúde brasileiro" [107]. Essa abordagem tem como objetivo estimular o desenvolvimento de pesquisa translacional e a integração da ciência acadêmica com a prática da saúde, contribuindo para a melhoria dos serviços de saúde.

Além disso, a estratégia busca fortalecer o uso de estudos e evidências para a incorporação de inovações em saúde. Isso demonstra o compromisso em embasar as decisões no campo da saúde em dados concretos e pesquisas científicas, visando aprimorar a eficácia e a eficiência dos serviços de saúde no Brasil. [107]

A Rede Nacional de Dados em Saúde (RNDS) é uma iniciativa chave para a transformação digital do sistema de saúde no Brasil. A determinação de padrões de informática em saúde é essencial para possibilitar a interoperabilidade entre sistemas, garantir a segurança jurídica e farmacológica, assegurar a confidencialidade e privacidade das informações, além de permitir a automação de procedimentos e melhorar a atenção à saúde.

A RNDS não se restringe apenas à interoperabilidade, mas também visa promover a saúde, prevenir doenças e disponibilizar serviços digitais inovadores. A integração de informações coletadas em diferentes estabelecimentos de saúde na RNDS possibilita o desenvolvimento de modelos inovadores de promoção da saúde e prevenção de doenças, além de facilitar a tele saúde e a prestação de serviços digitais.

Para que a RNDS cumpra sua missão de ser o pilar central da Plataforma Nacional de Informações e Serviços de Saúde Digital, é crucial disseminar tecnologias, conceitos, padrões e modelos de informação entre os participantes do Espaço de Colaboração. A determinação de critérios éticos, propósitos de utilização e responsabilidades legais é essencial para garantir o acesso controlado e regulado à RNDS, em conformidade com a Visão de Saúde Digital [107].

Adicionalmente, a evolução da RNDS demanda a identificação dos atores e gestores do SUS, bem como a integração de dados e tecnologias cruciais para o atendimento remoto e a promoção da saúde da população. É imprescindível concentrar esforços na melhoria do

cuidado à saúde, na resolução das desigualdades de acesso e na utilização eficiente dos serviços de saúde no SUS [107].

Portanto, a RNDS não apenas fomenta a interoperabilidade e a segurança das informações de saúde, mas também impulsiona a inovação, a prevenção de doenças e a melhoria do cuidado à saúde, alinhada com os princípios da Saúde Digital no Brasil [107].

Além disso, a alocação de investimentos adequados e a definição de regulamentações claras são aspectos críticos a serem abordados. A disponibilidade de recursos financeiros e a conformidade com normas e padrões são fundamentais para viabilizar a colaboração entre os diversos atores envolvidos no processo de transformação digital da saúde no Brasil [107].

A garantia da conformidade com as normas estabelecidas e uma gestão eficiente dos recursos e processos são fatores determinantes para assegurar a qualidade e a segurança dos serviços de saúde digital oferecidos. A conformidade e a gestão eficaz são elementos-chave a serem considerados no desenvolvimento e implementação da Estratégia de Saúde Digital [107].

7.3.3 Desafios

Inovar no setor de tecnologia da saúde no Brasil é um desafio complexo e multifacetado. A diversidade geográfica e socioeconômica do país, a complexidade do SUS, e a necessidade de conformidade com regulamentações rigorosas são obstáculos significativos. Além disso, a infraestrutura de dados deficiente e a falta de uma cultura organizacional voltada para a inovação podem dificultar a implementação de soluções tecnológicas eficazes na área da saúde.

Um desses desafios está relacionado à formação e capacitação de profissionais de Tecnologia da Informação e Comunicação. É essencial investir na qualificação desses profissionais, garantindo que eles tenham “conhecimento, experiência e atitudes necessárias” para desempenhar um papel crucial na implementação das inovações em saúde [104] [107].

Outro desafio relevante é o engajamento dos diversos atores do setor de saúde para a criação conjunta de mecanismos de fortalecimento da base produtiva em saúde. A colaboração entre governo, instituições de pesquisa, empresas de tecnologia e profissionais de saúde é essencial para impulsionar a inovação e o desenvolvimento tecnológico no setor da saúde.

Existem também alguns outros entraves significativos que precisam ser superados. A desigualdade regional na distribuição de iniciativas inovadoras, a falta de compreensão

aprofundada dos problemas do sistema de saúde, a burocracia pública, a fragmentação dos ecossistemas de inovação, os desafios de escalabilidade, a infraestrutura de dados deficiente e a falta de uma cultura organizacional voltada para a inovação são alguns dos principais obstáculos que dificultam a tomada de decisões informadas e a definição de prioridades para a inovação e melhora dos sistemas [104].

A burocracia excessiva e pouco preparada para lidar com iniciativas inovadoras também se destaca como um obstáculo significativo. Conforme mencionado por um ex-gestor de Ciência, Tecnologia e Inovação do Estado de São Paulo [104]:

> "Se você não sabe o que está resolvendo e não sabe onde mexer para resolver, é grande a chance de que você institua uma iniciativa que mais atrapalha do que ajuda. Veja o exemplo de um hospital que não tem fluxos básicos definidos, mas compra um aparelho de cirurgia robótica: você acaba de sobrecarregar o time, ampliar a necessidade de treinamento, aumentar os custos de giro e qual problema relevante foi resolvido? Nenhum." (apud AGUILLAR et al, 2021)

A inovação muitas vezes pode ser desvinculada de problemas amplos e reconhecidos, o que pode comprometer a eficácia das soluções propostas.

O SUS, como entidade pública, enfrenta desafios intrínsecos relacionados à sua dependência de financiamento governamental, que é sujeito a flutuações conforme as diretrizes políticas vigentes. Essa volatilidade se manifesta em decisões como a exemplo da proposta de redução orçamentária para o DATASUS que representaria um corte de 58% nos recursos previstos para 2023, reduzindo o orçamento de R$330 milhões para R$140,2 milhões [108]. Tal medida teria implicações diretas na integridade e eficiência do sistema, além de potencializar os desafios já existentes na gestão da saúde pública.

7.3.4 Blockchain e DID como solução.

No âmbito da saúde brasileira, a inovação tecnológica se faz crucial para superar obstáculos, conforme abordado previamente. Nesta perspectiva, as identidades descentralizadas emergem como uma solução promissora para fomentar a inovação tecnológica na área da saúde no país.

As tecnologias de identidade descentralizadas apresentam suas vantagens de maneira técnica, ou seja, todos os aspectos envolvidos na sua implementação possuem seus prós e contras, independentemente do contexto em que são inseridos. Portanto, quais benefícios e desafios específicos da realidade brasileira essa tecnologia pode impactar?

A adoção de identidades descentralizadas no setor de saúde pode criar um ecossistema colaborativo, envolvendo o SUS, instituições de saúde, empresas de tecnologia e centros acadêmicos, para compartilhar dados e inovações, respeitando sempre a ética e a legislação. Isso não só impulsiona a inovação, mas também permite a avaliação criteriosa de novas soluções tecnológicas.

Essas tecnologias podem contribuir para garantir um acesso controlado e regulado à RNDS, em conformidade com os critérios éticos, alinhados com os critérios de utilização e responsabilidades legais estabelecidos na Estratégia de Saúde Digital.

Elas também podem auxiliar na conformidade com a LGPD ao proporcionar maior controle e consentimento aos titulares dos dados, assegurar privacidade e segurança, promover a minimização de dados, facilitar a rastreabilidade e auditoria, e permitir a transferência segura de informações. Essas tecnologias criptográficas avançadas auxiliam as organizações a proteger os dados pessoais, atender aos requisitos de segurança e transparência da LGPD e facilitar o compartilhamento seguro de dados entre entidades.

Essas tecnologias também têm o potencial de desempenhar um papel crucial na mitigação das desigualdades regionais em saúde. Por meio delas, os pacientes podem acessar e controlar seus próprios registros de saúde de forma segura, o que é especialmente importante em regiões com acesso limitado a serviços de saúde. Além disso, a telemedicina e consultas remotas podem ser potencializadas, permitindo que pacientes em áreas remotas recebam atendimento médico de qualidade, contribuindo para a redução das disparidades no acesso aos cuidados de saúde.

A colaboração e pesquisa em saúde podem ser incentivadas, permitindo que pesquisadores e profissionais compartilhem dados de forma segura e colaborem em estudos e projetos que beneficiem comunidades em regiões menos assistidas.

O empoderamento dos pacientes é outro benefício das identidades descentralizadas, pois eles podem controlar suas próprias informações de saúde, o que promove a autogestão do mesmo. Isso pode resultar em uma melhor adesão ao tratamento, prevenção de doenças e promoção de estilos de vida saudáveis.

Em suma, as identidades descentralizadas têm o potencial de promover o acesso equitativo aos cuidados de saúde, a colaboração entre profissionais e pesquisadores, e o empoderamento dos pacientes, desempenhando um papel fundamental na redução da desigualdade regional em saúde.

8. CONCLUSÃO E TRABALHOS FUTUROS

Este estudo investigativo mergulhou no universo da identidade descentralizada e da tecnologia blockchain, com intuito de realizar uma revisão sistemática da literatura, que revelou áreas inexploradas e sublinhou a urgência de inovação neste segmento tecnológico, e, foi colocada em uma correlação com as problemáticas brasileiras com intuito de responder a pergunta de pesquisa proposta: "Qual é a natureza da identidade descentralizada e da identidade auto-soberana, e como essas tecnologias podem contribuir para a resolução dos problemas do sistema de saúde brasileiro?".

A resposta desta pergunta foi obtida através das seguintes perguntas secundárias:

1. Quais os termos técnicos mais frequentes no contexto de blockchain, identidade descentralizada e identidade auto-soberana no setor de saúde?
2. Como a identidade descentralizada, blockchain e identidade auto-soberana podem ser aplicadas no setor de saúde?
3. Quais os desafios enfrentados pela aplicação dessas tecnologias no contexto de saúde?

Os achados desta pesquisa não só enriquecem o acervo de conhecimentos atual, mas também pavimentam o caminho para futuras investigações sobre tecnologias descentralizadas no cenário brasileiro. O estudo também ressalta a necessidade de estabelecer padrões, acumular experiência prática e aprofundar o entendimento sobre identidade descentralizada e blockchain. Este trabalho aspira a ser uma contribuição referencial, incentivando novas pesquisas e análises nesta área.

As situações críticas identificadas reforçam a necessidade de superar desafios com soluções tecnológicas avançadas e inovadoras. Ao destacar as possíveis aplicações e consequências da identidade descentralizada e da blockchain, o estudo busca estimular avanços e fomentar uma cultura de inovação diante dos desafios únicos do Brasil.

A complexidade e a inovação inerentes a essas tecnologias exigem um estudo contínuo e aprofundado para superar os desafios técnicos, éticos e legais associados à sua implementação

A partir do que foi feito, algumas possibilidades de trabalhos futuros surgiram:

- Estudo de caso e pilotos em hospitais
- Desenvolvimento de protocolos de segurança

- Desenvolver um projeto de integração com sistemas hospitalares legados
- Realizar um aprofundamento do estudo do caso com mais comparativos
- Propor uma solução/framework para uso de identidades descentralizadas desenvolvidas com os pilares técnicos das necessidades dos sistemas brasileiros.

Este resumo enfatiza a relevância da pesquisa, suas contribuições para o conhecimento prévio e seu impacto potencial em futuras pesquisas e avanços tecnológicos no domínio das tecnologias descentralizadas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CANNY, J. A Computational Approach to Edge Detection. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. PAMI-8, n. 6, p. 679–698, nov. 1986.

[2] STATISTA. **Total EHR market size worldwide 2024** forecast. Disponível em: <https://www.statista.com/statistics/938799/ehr-market-size-forecast-globally/>.

[3] STATISTA. **Digital health tech to improve patient care 2020.** Disponível em: <https://www.statista.com/statistics/1198387/digital-health-tech-to-improve-patient-care/>.

[4] ZHANG, P. et al. **Blockchain Technology Use Cases in Healthcare**. Advances in Computers, v. 111, p. 1–41, 2018.

[5] STATISTA. **Health workers' issues with digital patient data 2020.** Disponível em:<https://www.statista.com/statistics/1198190/health-workers-issues-with-digital-patient-data/>.

[6] KAMEDA, K.; PAZELLO, **M. E-Saúde e desafios à proteção da privacidade no Brasil.** São Paulo: Instituto Saúde, 2015.

[7] G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal.** Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>.

[8] UOL. **7 em cada 10 brasileiros dependem do SUS para tratamento, diz IBGE.** Disponível em: <https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2020/09/04/7-em-cada-10-brasileiros-dependem-do-sus-para-tratamento-diz-ibge.htm>.

[9] RAUCHS, M. et al. **Distributed Ledger Technology Systems: A Conceptual Framework.** SSRN Electronic Journal, 2018.

[10] DESHPANDE, A. et al. **Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards Prepared for the British Standards Institution (BSI).** Disponível em: <https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf>.

[11] EL IOINI, N.; PAHL, C. **A Review of Distributed Ledger Technologies. Lecture Notes in Computer Science**, 2018.

[12] THEODOULI, A. et al. **On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing.** Disponível em: <https://ieeexplore.ieee.org/document/8456059>.

[13] HARSHINI, V. M. et al. **Health Record Management through Blockchain Technology.** 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), abr. 2019.

[14] MAZONKA, **O. Blockchain: Simple Explanation.** Research Gate, 2016.

[15] GUO, Y.; LIANG, C. **Blockchain Application and Outlook in the Banking Industry.** Financial Innovation, v. 2, n. 1, dez. 2016.

[16] WALID FDHILA et al. **Methods for Decentralized Identities: Evaluation and Insights. Lecture notes in business information processing**, p. 119–135, 1 jan. 2021.

[17] GOODELL, G.; ASTE, T. **A Decentralized Digital Identity Architecture.** Frontiers in Blockchain, v. 2, 5 nov. 2019.

[18] DIB, O.; TOUMI, K. **Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions.** Annals of Emerging Technologies in Computing, v. 4, n. 5, p. 19–40, 20 dez. 2020.

[19] ZHOU, Y. et al. **Application of Distributed Ledger Technology in Distribution Networks.** Proceedings of the IEEE, p. 1–13, 2022.

[20] TOTH, K. C.; ANDERSON-PRIDDY, A. **Self-Sovereign Digital Identity: A Paradigm Shift for Identity.** IEEE Security & Privacy, v. 17, n. 3, p. 17–27, maio 2019.

[21] BAHYA NASSR EDDINE; AAFAF OUADDAH; ABDELLATIF MEZRIOUI. **Exploring blockchain-based Self Sovereign Identity Systems: challenges and comparative analysis**. IEEE, 27 set. 2021.

[22] MICROSOFT. **Solução de identidade descentralizada** | Segurança da Microsoft. Disponível em: <https://www.microsoft.com/pt-br/security/business/solutions/decentralized-identity>.

[23] ZHANG, P.; SCHMIDT, D.; LENZ, G. **Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare.** Disponível em: <https://www.dre.vanderbilt.edu/~schmidt/PDF/PLoP-2017-blockchain.pdf>.

[24] KITCHENHAM, B. A. **Systematic review in software engineering. Proceedings of the 2nd international workshop on Evidential assessment of software technologies** - EAST '12, 2012.

[25] SHLOMI LINOY et al. **Authenticated Range Querying of Historical Blockchain Healthcare Data using Authenticated Multi-Version Index. Distributed Ledger Technologies Research and Practice**, 6 out. 2023.

[26] CLAVIN, J. et al. **Blockchains for Government. Digital Government: Research and Practice**, v. 1, n. 3, dez. 2020.

[27] OAKLEY, J. et al. **Scrybe: A Secure Audit Trail for Clinical Trial Data Fusion.** Digital Threats: Research and Practice, 29 out. 2021.

[28] AMIRI, M. J.; AGRAWAL, D.; EL ABBADI, A. **Permissioned Blockchains: Properties, Techniques and Applications. Proceedings of the 2021 International Conference on Management of Data**, 9 jun. 2021.

[29] SHUAIB, K. et al. **Secure decentralized electronic health records sharing system based on blockchains.** Journal of King Saud University - Computer and Information Sciences, maio 2021.

[30] KARMAKAR, A. et al. **ChainSure: Agent free insurance system using blockchain for healthcare 4.0. Intelligent Systems with Applications**, fev. 2023.

[31] LIN, G. et al. **A blockchain-based fine-grained data sharing scheme for e-healthcare system.** Journal of Systems Architecture, nov. 2022.

[32] CLIM, A.; ZOTA, R. D.; CONSTANTINESCU, R. **Data exchanges based on blockchain in m-Health applications.** Procedia Computer Science, 2019.

[33] BRUNESE, L. et al. **A Blockchain Based Proposal for Protecting Healthcare Systems through Formal Methods**. Procedia Computer Science, 2019.

[34] CHONDROGIANNIS, E. et al. **Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations.** Blockchain: Research and Applications, jun. 2022.

[35] KUMAR, M. et al. **Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems**, 1 jan. 2023.

[36] ROEHRS, A. et al. **Analyzing the performance of a blockchain-based personal health record implementation. Journal of Biomedical Informatics**, abr. 2019.

[37] CUNHA, S. et al. **Permissioned Blockchain Approach using Open Data in Healthcare.** Procedia Computer Science, 1 jan. 2022.

[38] KUMAR, P. et al. **A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system.** Journal of Parallel and Distributed Computing, 1 fev. 2023.

[39] MAHER, M.; KHAN, I.; PRIKSHAT, V. **Monetisation of digital health data through a GDPR-compliant and blockchain enabled digital health data marketplace: A proposal to enhance patient's engagement with health data repositories. International Journal of Information Management Data Insights**, abr. 2023.

[40] LI, Y.; TANG, M. **Blockchain-powered Distributed Data Auditing Scheme for Cloud-edge Healthcare System.** Cyber Security and Applications, abr. 2023.

[41] KAMAL, R.; EZZ EL-DIN HEMDAN; NAWAL EL-FISHWAY. **Care4U: Integrated healthcare systems based on blockchain.** 1 jul. 2023.

[42] ZHANG, Y. et al. **Blockchain-Enabled decentralized Attribute-Based access control with policy hiding for smart healthcare**. Journal of King Saud University - Computer and Information Sciences, 1 nov. 2022.

[43] AIT BENNACER, S. et al. **Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study.** Informatics in Medicine Unlocked, 2022.

[44] UPPAL, S. et al. **HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system.** Healthcare Analytics, nov. 2023.

[45] FOY, M. et al. **Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis.** Procedia Computer Science, 2022.

[46] BALISTRI, E. et al. **BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten**. ICT Express, ago. 2021.

[47] GAO, Y. et al. **Blockchain-based Multi-hop Permission Delegation Scheme with Controllable Delegation Depth for Electronic Health Record Sharing.** High-Confidence Computing, out. 2022.

[48] AZBEG, K.; OUCHETTO, O.; JAI ANDALOUSSI, S. **BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security.** Egyptian Informatics Journal, fev. 2022.

[49] DONG, Y.; SEONG KI MUN; WANG, Y. **A blockchain-enabled sharing platform for personal health records.** Heliyon, 1 jul. 2023.

[50] BARBARIA, S.; MAHJOUBI, H.; RAHMOUNI, H. B. **A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case.** Procedia Computer Science, 2023.

[51] WANG, G.; ALDIAN NURCAHYO. **Designing Personalized Integrated Healthcare Monitoring System through Blockchain and IoT. Procedia Computer Science**, 1 jan. 2023.

[52] SHARMA, Y.; BALAMURUGAN, B. **Preserving the Privacy of Electronic Health Records using Blockchain.** Procedia Computer Science, 2020.

[53] KOSHECHKIN, K. A. et al. **Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation. Procedia Computer Science**, 2018.

[54] GUIMARÃES, T. et al. **Blockchain Analytics - Real-time Log Management in Healthcare.** Procedia Computer Science, 2022.

[55] ZHUANG, Y. et al. **Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology.** Computers in Biology and Medicine, 1 maio 2023.

[56] SABU, S. et al. I**mplementation of A Secure and Privacy-Aware E-Health Record and IoT Data Sharing using Blockchain.** Global Transitions Proceedings, 13 ago. 2021.

[57] ANTWI, M. et al. **The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications. Blockchain: Research and Applications**, maio 2021.

[58] REHMAN, A. et al. **A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique.** Computers in Biology and Medicine, nov. 2022.

[59] NASER ALSUQAIH, H. et al. **An efficient privacy-preserving control mechanism based on blockchain for E-health applications.** Alexandria Engineering Journal, 15 jul. 2023.

[60] JAYANTHY, D. S. et al. **Secured Health Data Sharing System using IPFS and Blockchain with Beacon Proxy. Procedia Computer Science**, 1 jan. 2023.

[61] GARRIDO, A.; RAMÍREZ LÓPEZ, L. J.; ÁLVAREZ, N. B. **A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions. Informatics in Medicine Unlocked**, 2021.

[62] GUO, R. et al. **Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems.** IEEE Access, 2018.

[63] TANG, F. et al. **An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records**. IEEE Access, 2019.

[64] WANG, S.; ZHANG, D.; ZHANG, Y. **Blockchain-based personal health records sharing scheme with data integrity verifiable.** IEEE Access, 2019.

[65] NIU, S. et al. **Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain.** IEEE Access, 2020.

[66] ISMAIL, L.; MATERWALA, H.; ZEADALLY, S. **Lightweight Blockchain for Healthcare.** IEEE Access, 2019.

[67] NGUYEN, D. C. et al. **Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems.** IEEE Access, 2019.

[68] RAJPUT, A. R. et al. **EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain.** IEEE Access, 2019.

[69] SHAHNAZ, A.; QAMAR, U.; KHALID, A. **Using Blockchain for Electronic Health Records.** IEEE Access, 2019.

[70] AKKAOUI, R.; HEI, X.; CHENG, W. **EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange.** IEEE Access, 2020.

[71] TOMAZ, A. E. B. et al. **Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain**. IEEE Access, 2020.

[72] RAHMAN, M. A. et al. **Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach.** IEEE Access, 2020.

[73] HOUTAN, B.; HAFID, A. S.; MAKRAKIS, D. **A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare.** IEEE Access, 2020.

[74] ZAROUR, M. et al. **Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records.** IEEE Access, 2020.

[75] JAIMAN, V.; UROVI, V. **A Consent Model for Blockchain-Based Health Data Sharing Platforms. IEEE Access**, 2020.

[76] XIANG, X.; WANG, M.; FAN, W. **A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems.** IEEE Access, 2020.

[77] ZHUANG, Y. et al. **A Patient-Centric Health Information Exchange Framework Using Blockchain Technology.** IEEE Journal of Biomedical and Health Informatics, ago. 2020.

[78] ZGHAIBEH, M. et al. **SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities.** IEEE Access, 2020.

[79] MUSAMIH, A. et al. **A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain.** IEEE Access, 2021.

[80] LEE, D.; SONG, M. **MEXchange: A Privacy-preserving Blockchain-based Framework for Health Information Exchange using Ring Signature and Stealth Address.** IEEE Access, 2021.

[81] SUBRAMANIAN, G.; SREEKANTAN THAMPY, A. **Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations.** IEEE Access, 2021.

[82] YONGJOH, S. et al. **Development of an Internet-of-Healthcare System Using Blockchain.** IEEE Access, 2021.

[83] LIU, Y. et al. **Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Perspective.** IEEE Access, 2022.

[84] BAWANY, N. Z. et al. **Integrating Healthcare Services using Blockchain-based Telehealth Framework**. IEEE Access, 2022.

[85] ALZAHRANI, A. G.; ALHOMOUD, A.; WILLS, G. **A Framework of the Critical Factors for Healthcare Providers in Data-Sharing Using Blockchain.** IEEE Access, 2022.

[86] PANG, Z. et al. **Electronic Health Records Sharing Model based on Blockchain with Checkable State PBFT Consensus Algorithm.** IEEE Access, 2022.

[87] HEGDE, M.; RAO, R. R.; NIKHIL, B. M. **DDMIA: Distributed Dynamic Mutual Identity Authentication for Referrals in Blockchain-Based Health Care Networks.** IEEE Access, 2022.

[88] BAE, Y. S. et al. **Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test.** IEEE Access, 2022.

[89] ALNUAIMI, A. et al. **Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs.** IEEE Access, 2022.

[90] SAIDI, H. et al. **DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data.** IEEE Access, 2022.

[91] GOHAR, A.; ABDELGABER, S.; SALAH, M. **A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability based on Blockchain, Cloud, and IoT.** IEEE Access, 2022.

[92] PINTO, R. P.; SILVA, B. M. C.; INÁCIO, P. R. M. **A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain.** IEEE Access, 2022.

[93] AKASH, S. S.; FERDOUS, M. S. **A Blockchain Based System for Healthcare Digital Twin.** IEEE Access, 2022.

[94] COSTA, L. D. et al. **Sec-Health: A Blockchain-Based Protocol for Securing Health Records.** IEEE Access, 2023.

[95] T HARITHA; A ANITHA. **Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System.** IEEE Access, 1 jan. 2023.

[96] ABHISHEK BISHT et al. **Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain and IPFS. IEEE open journal of the Communications Society**, 1 jan. 2023.

[97] SIDDHANT THAPLIYAL et al. **Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications.** IEEE Access, 1 jan. 2023.

[98] AYSHA ALNUAIMI et al. **Trustworthy Healthcare Professional Credential Verification using Blockchain Technology**. IEEE Access, 1 jan. 2023.

[99] SMITH, T. et al. **Blockchain to Blockchains in Life Sciences and Health Care.** Deloitte, 2018.

[100] CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. **Brasil sobe cinco posições e chega ao 49 lugar no Índice Global de Inovação.** Disponível em:

<https://www.gov.br/inpi/pt-br/central-de-conteudo/noticias/brasil-sobe-cinco-posicoes-e-chega-ao-49o-lugar-no-indice-global-de-inovacao>.

[101] G1. **Sistema de dados do Ministério da Saúde completa um mês com instabilidades**. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2022/01/10/sistema-de-dados-do-ministerio-da-saude-completa-um-mes-com-instabilidades.ghtml>. Acesso em: 5 mar. 2024.

[102] BRASIL DE FATO. **TCU abre investigação sobre diretor que migrou DataSUS para Amazon e agora trabalha na empresa**. Disponível em: <https://www.brasildefato.com.br/2022/04/01/tcu-abre-investigacao-sobre-diretor-que-migrou-datasus-para-amazon-e-agora-trabalha-na-empresa>. Acesso em: 5 mar. 2024.

[103] FOLHA DE SÃO PAULO. **Saúde admite falha em dados sobre vacinados, e transição planeja nova secretaria no SUS**. Disponível em: <https://www1.folha.uol.com.br/equilibrioesaude/2022/12/saude-admite-falha-em-dados-sobre-vacinados-e-transicao-planeja-nova-secretaria-no-sus.shtml>. Acesso em: 5 mar. 2024.

[104] AGUILLAR, A. et al. **Panorama IEPS: Inovação em Saúde no Brasil.** Brasil: IEPS, 2021.

[105] ANGÉLICA BAPTISTA SILVA; JOSÉ, F. Lei Geral de Proteção de Dados e o controle social da saúde. Editora Rede Unida, 10 jun. 2023.

[106] CONSELHO FEDERAL DE MEDICINA. **Após amplo debate, CFM regulamenta prática da Telemedicina no Brasil** |. Disponível em: <https://portal.cfm.org.br/noticias/apos-amplo-debate-cfm-regulamenta-pratica-da-telemedicina-no-brasil>. Acesso em: 5 mar. 2024.

[107] MINISTÉRIO DA SAÚDE. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Brasil: Editora MS, 2020.

[108] FÓRUM DE DIREITO DE ACESSO A INFORMAÇÕES PÚBLICAS. **Proposta de corte de 58% no orçamento do DataSUS compromete direito à saúde, à informação e à proteção de dados, alerta Fórum**. Disponível em: <https://informacaopublica.org.br/leia/proposta-de-corte-de-58-no-orcamento-do-datasus-compromete-direito-a-saude-a-informacao-e-a-protecao-de-dados-alerta-forum/>. Acesso em: 10 mar. 2024.