



UNIVERSIDADE FEDERAL DE UBERLÂNDIA  
FACULDADE DE ENGENHARIA ELÉTRICA  
GRADUAÇÃO EM ENGENHARIA BIOMÉDICA

**MARIA LUIZA CAMARGOS BORGES CARNEIRO**

**PERSPECTIVA DA UTILIZAÇÃO DO *BLOCKCHAIN* EM  
PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)**

Uberlândia  
2023

**MARIA LUIZA CAMARGOS BORGES CARNEIRO**

**PERSPECTIVA DA UTILIZAÇÃO DO *BLOCKCHAIN* EM  
PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)**

Trabalho apresentado como requisito parcial de avaliação na disciplina Trabalho de Conclusão de Curso de Engenharia Biomédica da Universidade Federal de Uberlândia.

Orientador: Adriano Alves Pereira

---

Assinatura do Orientador

Uberlândia  
2023

## **AGRADECIMENTOS**

Gostaria de expressar minha sincera gratidão ao meu professor orientador, Adriano, pela sua orientação, apoio e, principalmente, por toda sua paciência durante o desenvolvimento deste trabalho. A caminhada não foi fácil, mas a sua compreensão e incentivo foram essenciais.

À minha família, gostaria de agradecer pelo apoio inabalável ao longo dessa jornada acadêmica. O amor, o incentivo e a compreensão de todos foram imensuráveis para a conclusão deste trabalho. Agradeço também por todo o apoio emocional e psicológico que me proporcionaram. Em momentos de desânimo ou incerteza, vocês estavam lá para me lembrar do meu potencial e me motivar a seguir em frente.

Gostaria de agradecer ao meu marido, Luis. Desde o início, você esteve ao meu lado, me incentivando a alcançar o meu melhor e acreditando em minhas capacidades. Sua confiança em mim e em meu potencial tem sido um combustível para superar desafios. Muito obrigada por estar ao meu lado nesta jornada.

Por fim, gostaria de dedicar um agradecimento especial as amigas que ganhei durante a graduação, que estiveram ao meu lado durante essa jornada acadêmica. Giovana, Luiza e Renata vocês foram uma fonte constante de motivação, compartilhando risadas, conselhos e desafios ao longo do caminho. Juntas, enfrentamos noites de estudo intensas, trabalhos em grupo, provas e momentos de pressão acadêmica. Através de tudo isso, pude contar com a amizade verdadeira e o apoio mútuo que nos fortaleceu.

A todas as pessoas que fizeram parte dessa minha jornada, meu mais sincero agradecimento. Vocês contribuíram de maneira significativa para o meu crescimento pessoal e acadêmico. Sou grata por ter tido a honra de compartilhar essa experiência com vocês. Que nossa jornada continue a ser repleta de aprendizado e sucesso.

## RESUMO

Os prontuários eletrônicos do paciente têm desempenhado um papel importante na transformação digital dos sistemas de saúde, permitindo o armazenamento e o acesso digital às informações médicas. No entanto, esses prontuários enfrentam desafios relacionados à segurança, privacidade e interoperabilidade. Nesse contexto, o *blockchain* tem sido explorado como uma solução potencial para melhorar esses prontuários. O *blockchain* é uma tecnologia distribuída e descentralizada que oferece segurança, transparência e imutabilidade aos registros armazenados. Este estudo tem como objetivo analisar a perspectiva da utilização do *blockchain* em prontuários eletrônicos do paciente, investigando os benefícios, desafios e implicações dessa tecnologia emergente. Espera-se fornecer uma visão abrangente sobre a aplicação do *blockchain* em prontuários eletrônicos, contribuindo para uma gestão mais segura, eficiente e interoperável das informações médicas. Desta forma, o estudo buscou realizar uma revisão sistemática sobre a perspectiva da utilização do *blockchain* em prontuários eletrônicos do paciente. Foram utilizadas as bases de dados BVS, Embase e PubMed/MEDLINE, com os descritores “*Blockchain*”, “Prontuário Eletrônico do Paciente”, “*Patient Electronic Records*”, “*Electronic Health Record*”, “*Electronic Medical Record*” e “*Electronic Patient Record*”. A busca foi refinada utilizando a metodologia PRISMA e PICOS e no final foram escolhidos 11 estudos. A conclusão do estudo revela que a utilização do *blockchain* em prontuário eletrônico do paciente tem sido considerada uma perspectiva promissora, já que o *blockchain* é uma tecnologia que pode oferecer maior segurança, privacidade e transparência aos dados de saúde dos pacientes.

## **ABSTRACT**

Electronic patient records have played a significant role in the digital transformation of healthcare systems, enabling the storage and digital access to medical information. However, these records face challenges related to security, privacy, and interoperability. In this context, blockchain has been explored as a potential solution to enhance these records. Blockchain is a distributed and decentralized technology that provides security, transparency, and immutability to stored records. This study aims to analyze the perspective of using blockchain in electronic patient records, investigating the benefits, challenges, and implications of this emerging technology. The study intends to provide a comprehensive view of blockchain application in electronic records, contributing to a more secure, efficient, and interoperable management of medical information. In this way, the study aimed to conduct a systematic review on the perspective of using blockchain in patient electronic health records. The databases BVS, Embase, and PubMed/MEDLINE were searched using the descriptors "Blockchain," "Patient Electronic Records," "Electronic Health Record," "Electronic Medical Record," and "Electronic Patient Record." The search was refined using the PRISMA and PICOS methodology, resulting in the selection of 11 studies. The study's conclusion reveals that the use of blockchain in patient electronic health records has been considered a promising perspective, as blockchain is a technology that can provide greater security, privacy, and transparency to patients' health data.

## LISTA DE ILUSTRAÇÕES

FIGURA 1 – Diagrama de fluxo PRISMA .....	22
---	----

## **LISTA DE TABELAS**

TABELA 1 – Estudos extraídos da revisão sistemática .....	24
TABELA 2 – Quadro comparativo dos estudos .....	37

## LISTA DE ABREVIATURAS E SIGLAS

BSF – Quadro de Segurança em *Blockchain*

EAS – Estabelecimento Assistencial de Saúde

Ecerts – Certificados de Inscrição

eID – Identificações de Inscrições Eletrônicas

EHR – Registros de Saúde Eletrônicos

IPFS – Sistema de Arquivos Interplanetário

Ipssec – *Internet Protocol Security*

HLF – *Hyperledger Fabric*

MIT – *Massachusetts Institute of Technology*

MSP – Provedor de Serviços de Adesão

PcBEHR – Registros de Saúde Eletrônicos Ativados por Blockchain e Controlado pelo Paciente

PEP – Prontuários Eletrônicos do Paciente

PIE – Troca de Informação de Pacientes

PHDMF – Quadro Federal de Gestão de Dados Pessoais de Saúde

PICOS – *Population, Intervention, Comparator, Outcome and Study*

PoA – Prova de autoridade

PoC – Prova de Conceito

PRE – Re-criptação por Procuração

PRISMA – *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*

SSL – *Secure Sockets Layer*

TLS – *Transport Layer Security*

VPN – *Virtual Private Network*

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b> .....	<b>11</b>
<b>1.1</b>	<b>OBJETIVOS</b> .....	<b>12</b>
<b>1.1.1</b>	<b>OBJETIVO GERAL</b> .....	<b>12</b>
<b>1.1.2</b>	<b>OBJETIVOS ESPECÍFICOS</b> .....	<b>12</b>
<b>2</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b> .....	<b>13</b>
<b>2.1</b>	<b>PRONTUÁRIOS DE PACIENTES</b> .....	<b>13</b>
<b>2.2</b>	<b>PROTOCOLO DE SEGURANÇA</b> .....	<b>16</b>
<b>2.3</b>	<b>BLOCKCHAIN</b> .....	<b>17</b>
<b>2.4</b>	<b>BLOCKCHAIN EM PRONTUÁRIOS ELETRÔNICOS DO PACIENTE</b> .....	<b>18</b>
<b>3</b>	<b>METODOLOGIA</b> .....	<b>20</b>
<b>3.1</b>	<b>DESENHO DE ESTUDO</b> .....	<b>20</b>
<b>3.2</b>	<b>ESTRATÉGIA DE BUSCA</b> .....	<b>20</b>
<b>3.3</b>	<b>IDENTIFICAÇÃO DA PERGUNTA DA PESQUISA</b> .....	<b>20</b>
<b>3.3.1</b>	<b>POPULAÇÃO</b> .....	<b>20</b>
<b>3.3.2</b>	<b>INTERVENÇÃO E COMPARAÇÃO</b> .....	<b>21</b>
<b>3.3.3</b>	<b>DESFECHO</b> .....	<b>21</b>
<b>3.3.4</b>	<b>TIPOS DE ESTUDO</b> .....	<b>21</b>
<b>3.4</b>	<b>CRITÉRIOS DE INCLUSÃO E EXCLUSÃO</b> .....	<b>21</b>
<b>3.5</b>	<b>ANÁLISE DE DADOS</b> .....	<b>21</b>
<b>4</b>	<b>RESULTADOS E DISCUSSÕES</b> .....	<b>23</b>
<b>5</b>	<b>CONCLUSÃO</b> .....	<b>42</b>
<b>6</b>	<b>REFERÊNCIAS</b> .....	<b>43</b>

## 1 INTRODUÇÃO

Os avanços tecnológicos têm desempenhado um papel fundamental na transformação dos sistemas de saúde, buscando melhorar a qualidade do atendimento, a eficiência dos processos e a segurança dos pacientes (Shortliffe, 2005). Nesse cenário, os prontuários eletrônicos do paciente (PEP) surgiram como uma solução promissora para substituir os antigos registros em papel, permitindo o armazenamento e o acesso digital às informações médicas. No entanto, apesar dos benefícios proporcionados pelos prontuários eletrônicos, eles também enfrentam desafios significativos, como questões de segurança, privacidade e interoperabilidade (Gans et al., 2005).

A segurança dos prontuários eletrônicos é uma preocupação central, uma vez que a integridade e a confidencialidade das informações médicas são fundamentais para a relação médico-paciente e para a tomada de decisões clínicas adequadas (Kaufman, Perlman & Speciner, 2012). Além disso, a interoperabilidade entre os diferentes sistemas de prontuários eletrônicos ainda é um obstáculo, dificultando o compartilhamento eficiente e seguro de informações entre os prestadores de serviços de saúde (Menachemi & Collum, 2005).

Nesse contexto, a utilização do *blockchain* tem sido cada vez mais explorada como uma solução potencial para abordar os desafios enfrentados pelos PEP (Xi et al., 2022). O *blockchain*, originalmente desenvolvido para dar suporte às criptomoedas, é uma tecnologia distribuída e descentralizada que oferece segurança, transparência e imutabilidade aos registros armazenados (Nakamoto, 2008). Essas características podem contribuir para aumentar a confiança, a privacidade e a interoperabilidade dos prontuários eletrônicos, transformando a maneira como as informações médicas são gerenciadas e compartilhadas (Zhang et al., 2018).

A importância desse estudo reside na necessidade de compreender os benefícios e desafios da utilização da tecnologia *blockchain* em prontuários eletrônicos do paciente. Através dessa análise, é possível identificar oportunidades de melhoria nos sistemas existentes, fornecendo uma base sólida para a implementação adequada do *blockchain* na área da saúde. Além disso, este estudo contribuirá para o desenvolvimento de diretrizes e recomendações que orientem os profissionais de saúde e as instituições na adoção dessa tecnologia emergente.

## 1.1 Objetivos

### 1.1.1 Objetivo geral

O objetivo geral deste trabalho é analisar a perspectiva da utilização do *blockchain* em PEP.

### 1.1.2 Objetivos específicos

Os objetivos específicos do trabalho são:

- Analisar os conceitos fundamentais do *blockchain* e sua aplicabilidade em prontuários eletrônicos do paciente;
- Compreender os benefícios, desafios e impactos dessa tecnologia na segurança, privacidade e interoperabilidade dos registros de saúde;
- Analisar como a aplicação do *blockchain* pode contribuir para a confiabilidade e integridade dos prontuários eletrônicos, garantindo a imutabilidade e rastreabilidade das informações;
- Analisar os possíveis impactos na acessibilidade e compartilhamento seguro dos dados entre profissionais de saúde e estabelecimento assistencial de saúde (EAS);
- Analisar os desafios e limitações dos prontuários eletrônicos convencionais, incluindo questões de segurança, privacidade e interoperabilidade;
- Identificar os benefícios potenciais do uso do *blockchain* na gestão de prontuários eletrônicos, como a imutabilidade dos registros, a transparência e a descentralização;
- Contribuir para o avanço do conhecimento na área, fornecendo ideias e perspectivas sobre o uso do *blockchain* em prontuários eletrônicos e identificando possíveis áreas de pesquisa futura.

## 2 FUNDAMENTAÇÃO TEÓRICA

### 2.1 Prontuários de Pacientes

Os prontuários de pacientes remontam há muitos anos atrás, quando as informações dos pacientes começaram a ser registradas em papel. A primeira menção registrada de um prontuário médico data de 1302, quando o médico italiano Mondino dei Luzzi criou um livro de anotações sobre dissecação humana. Ao longo dos anos, os prontuários em papel se tornaram a norma na maioria das instituições de saúde (Di Matteo et al., 2017).

Os prontuários de pacientes são registros médicos que contêm informações sobre a saúde de um paciente, incluindo histórico médico, diagnósticos, resultados de exames, tratamentos, medicamentos prescritos, alergias e outras informações relevantes. Esses registros são mantidos por profissionais de saúde para ajudar a garantir a qualidade do atendimento prestado e para fins de documentação legal (Hersh, 2009).

Os prontuários de pacientes são importantes para garantir que os pacientes recebam o tratamento adequado e seguro. Eles também podem ser usados para pesquisas médicas e para monitorar tendências de saúde em uma determinada população. No entanto, a privacidade do paciente é uma preocupação importante ao lidar com prontuários médicos. As informações contidas nos prontuários devem ser mantidas em sigilo e só podem ser compartilhadas com autorização do paciente ou em casos em que é exigido por lei (Harrison & Palacio, 2006).

Além disso, é importante que os prontuários sejam precisos e atualizados regularmente, para garantir que os profissionais de saúde tenham acesso às informações mais atualizadas e precisas sobre a saúde do paciente. As instituições de saúde devem ter políticas e procedimentos claros para garantir que as informações sejam armazenadas e acessadas de forma segura e que a privacidade do paciente seja mantida em todos os momentos (Goodman, 2007).

Infelizmente, as falhas no gerenciamento e na segurança dos prontuários são preocupantes e podem ter consequências graves para a privacidade e segurança dos pacientes.

Segundo Khajouei, Abbasi & Mirzaee (2018), algumas das principais falhas podem incluir o acesso não autorizado, ou seja, se os prontuários não forem adequadamente protegidos, eles podem ser acessados por pessoas não autorizadas, como *hackers*,

funcionários mal-intencionados ou até mesmo membros da família do paciente que não têm autorização para acessar as informações. Isso pode resultar em roubo de identidade, fraude médica ou outras formas de abuso.

Outra falha importante a ser mencionada é o vazamento de informações, pois os prontuários de pacientes contêm informações altamente confidenciais e pessoais, como histórico médico, resultados de exames e medicamentos prescritos. Se essas informações vazarem, elas podem ser usadas para prejudicar o paciente, como na discriminação em seguro saúde ou emprego (Khajouei et al., 2018).

Erros e imprecisões, são falhas a serem consideradas também, pois se os prontuários não forem atualizados ou mantidos corretamente, podem ocorrer erros e imprecisões que podem afetar negativamente a qualidade do atendimento médico prestado ao paciente (Khajouei et al., 2018).

Segundo Halamka, Lippman, Ekblaw & Lippman (2018), para evitar essas falhas, as instituições de saúde devem implementar medidas de segurança adequadas, como o uso de senhas fortes, autenticação de dois fatores, criptografia de dados e monitoramento de acesso ao prontuário. Além disso, os profissionais de saúde devem ser treinados regularmente em práticas de segurança de dados e privacidade. As políticas e procedimentos de segurança de dados e privacidade devem ser revisados e atualizados regularmente para garantir que permaneçam eficazes e relevantes. Tais como:

- Autenticação forte: As instituições de saúde devem implementar mecanismos de autenticação forte para garantir que apenas pessoas autorizadas tenham acesso ao prontuário eletrônico do paciente. Isso pode incluir senhas fortes, autenticação de dois fatores ou biometria;
- Criptografia de dados: A criptografia é uma técnica de segurança que transforma as informações em um formato que só pode ser lido por pessoas com acesso autorizado. É importante que os dados do prontuário eletrônico sejam criptografados tanto em repouso (quando armazenados em servidores ou dispositivos) quanto em trânsito (quando transmitidos pela rede);
- Controles de acesso: Os sistemas de prontuário eletrônico devem ter controles de acesso rigorosos para garantir que apenas os profissionais de saúde que

precisam das informações do paciente tenham acesso a elas. Os sistemas também devem registrar quem acessou o prontuário eletrônico e quando;

- Monitoramento regular: As instituições de saúde devem monitorar regularmente as atividades de acesso aos prontuários eletrônicos do paciente para identificar atividades suspeitas ou não autorizadas;
- Treinamento de funcionários: Os profissionais de saúde devem ser treinados regularmente em práticas de segurança de dados e privacidade para garantir que compreendam suas responsabilidades e a importância da proteção dos prontuários eletrônicos do paciente;
- Políticas e procedimentos: As instituições de saúde devem ter políticas e procedimentos claros em vigor para garantir a segurança dos prontuários eletrônicos do paciente. Essas políticas devem ser revisadas regularmente e atualizadas conforme necessário para garantir que permaneçam eficazes e relevantes;

O uso de papel para gerenciar prontuários de pacientes pode ser ineficiente e caro, especialmente em grandes hospitais e clínicas. Isso ocorre porque o papel requer espaço físico para armazenamento, pode ser difícil de localizar, pode se deteriorar ao longo do tempo e pode ser perdido ou roubado. Além disso, o processo de arquivamento, recuperação e atualização de informações pode ser demorado e exigir muito trabalho manual (Goodman, 2007).

Felizmente, existem opções mais eficientes e econômicas para gerenciar prontuários de pacientes, os prontuários eletrônicos de pacientes se tornaram mais comuns nas últimas décadas. A primeira tentativa de criar um registro médico eletrônico foi feita na década de 1950, mas foi só na década de 1970 que a tecnologia necessária para criar sistemas eletrônicos de registro de pacientes começou a ser desenvolvida. A implementação generalizada de PEP só começou na década de 1990, quando as instituições de saúde começaram a investir em sistemas de informação de saúde (Fruhling & Talley, 2003).

Os sistemas PEP permitem que os profissionais de saúde armazenem, gerenciem e compartilhem informações do paciente de maneira eletrônica. Isso pode incluir histórico médico, resultados de exames, tratamentos, medicamentos prescritos e outras informações relevantes. Os PEP permitem que os profissionais de saúde acessem facilmente as

informações do paciente em tempo real, reduzindo o tempo gasto em tarefas administrativas e permitindo que eles se concentrem mais na prestação de cuidados de saúde (Gans et al., 2005).

Em resumo, os PEP são uma alternativa mais eficiente e econômica ao uso de papel para gerenciar prontuários de pacientes. Esses sistemas permitem que as informações do paciente sejam armazenadas eletronicamente, o que pode ser mais seguro, fácil de acessar e mais eficiente do que o uso de papel. A implementação de medidas de segurança adequadas, como criptografia de dados, autenticação forte, controles de acesso e treinamento de funcionários, podem ajudar a garantir que esses registros sejam protegidos contra acessos não autorizados ou vazamentos de informações.

## 2.2 Protocolo de Segurança

Um protocolo de segurança é um conjunto de regras e procedimentos que são usados para proteger a comunicação e os dados transmitidos entre dois ou mais dispositivos em uma rede. Esses protocolos são projetados para fornecer um nível de segurança apropriado para a rede e para garantir que as informações confidenciais não sejam interceptadas ou manipuladas durante a transmissão (Garfinkel, 2003).

Os protocolos de segurança são essenciais para proteger as redes e garantir a privacidade e a integridade das informações transmitidas. Eles trabalham em conjunto com outros mecanismos de segurança, como *firewalls* e sistemas de detecção de intrusão, para fornecer uma camada adicional de proteção contra ameaças de segurança. É importante que as organizações adotem e implementem protocolos de segurança adequados para proteger suas redes e dados, especialmente em setores sensíveis, como finanças e saúde (Stallings, 2017).

Segundo Boyd & Mathuria (2011), existem vários protocolos de segurança atuais que são amplamente utilizados para proteger informações confidenciais e garantir a privacidade e integridade de dados transmitidos através de redes de computadores. Alguns dos protocolos de segurança mais comuns incluem:

- *Transport Layer Security* (TLS): é um protocolo criptográfico utilizado para proteger a comunicação entre dois computadores em uma rede. O TLS é

amplamente utilizado em aplicativos da web, como sites de comércio eletrônico, serviços bancários online e outras transações sensíveis;

- *Secure Sockets Layer (SSL)*: é um protocolo de segurança semelhante ao TLS que também é usado para proteger a comunicação entre computadores em uma rede. Embora ainda seja amplamente utilizado, o SSL está sendo gradualmente substituído pelo TLS;
- *Virtual Private Network (VPN)*: é um protocolo de segurança que permite que usuários remotos se conectem a uma rede privada por meio de uma conexão segura. As VPNs são usadas principalmente para proteger a privacidade de dados transmitidos pela internet, como dados de login e senhas;
- *Internet Protocol Security (IPsec)*: é um conjunto de protocolos de segurança que é usado para proteger a comunicação entre computadores em uma rede privada. O IPsec é amplamente utilizado para fornecer segurança em redes corporativas;
- *Kerberos*: é um protocolo de autenticação usado para verificar a identidade de usuários e computadores em uma rede. O *Kerberos* é amplamente utilizado em redes corporativas e acadêmicas para garantir a segurança das informações e proteger contra ameaças externas;
- *Blockchain*: é frequentemente considerado um protocolo de segurança, pois possui várias características que o tornam altamente seguro e resistente a violações de segurança;

Esses são apenas alguns exemplos de protocolos de segurança atuais. Novos protocolos e tecnologias de segurança estão sendo desenvolvidos constantemente para combater as ameaças emergentes e manter a segurança da informação (Rahmani, Bayramov & Kalejahi, 2021).

## **2.3 Blockchain**

O *blockchain* é uma tecnologia relativamente nova que surgiu em 2008 com o lançamento da criptomoeda *Bitcoin*. Foi desenvolvido para fornecer um sistema seguro e

descentralizado para transações financeiras e desde então tem sido aplicado em uma ampla variedade de casos de uso (Nakamoto, 2008).

O conceito básico por trás do *blockchain* é criar um registro digital seguro e confiável que possa ser compartilhado entre várias partes sem a necessidade de um intermediário central. Isso é alcançado por meio de uma rede descentralizada de computadores que armazenam uma cópia idêntica do registro digital em cada um deles. Cada transação é validada por meio de um processo de consenso entre os nós da rede, o que significa que a maioria dos nós deve concordar que a transação é válida antes que ela seja registrada no *blockchain* (Tapscott & Tapscott, 2016).

O *blockchain* oferece várias vantagens em relação aos sistemas tradicionais de registro e transação. Uma das principais vantagens é a segurança, uma vez que o registro é criptografado e distribuído em toda a rede, tornando-o extremamente difícil de ser *hackeado* ou fraudado. Além disso, o *blockchain* é descentralizado, o que significa que não há um ponto único de falha, o que o torna mais resistente a ataques (Narayanan et al., 2016).

Outra vantagem do *blockchain* é a transparência. Como todos os nós da rede têm acesso ao registro completo, é possível rastrear todas as transações e verificar sua autenticidade. Isso pode ser particularmente útil em áreas como finanças, cadeias de suprimentos e votação eletrônica, onde a transparência e a confiabilidade são fundamentais (Wattenhofer, 2016).

O *blockchain* tem o potencial de transformar muitas indústrias, incluindo finanças, saúde, governança e logística. À medida que a tecnologia continua a evoluir, novos casos de uso estão surgindo e a adoção está aumentando em todo o mundo. Embora ainda haja desafios a serem superados, como escalabilidade e interoperabilidade, o *blockchain* está rapidamente se tornando uma tecnologia disruptiva que pode mudar a maneira como fazemos negócios e interagimos uns com os outros (Zheng et al., 2016).

## **2.4 Blockchain em prontuários eletrônicos do paciente**

O uso do *blockchain* na área da saúde é relativamente recente, com os primeiros projetos datando de cerca de 2014. No entanto, desde então, houve uma crescente adoção da tecnologia em diferentes aplicações na área da saúde (Ekblaw, 2014).

Um dos primeiros projetos de *blockchain* na saúde foi o MedRec, desenvolvido pelo *Massachusetts Institute of Technology* (MIT) em 2014. O MedRec foi projetado como um registro médico eletrônico baseado em *blockchain*, com o objetivo de fornecer uma plataforma segura para armazenar e compartilhar informações médicas entre diferentes organizações de saúde. Desde então, outros projetos semelhantes surgiram (Ekblaw, 2014).

Ao usar o *blockchain* para armazenar e gerenciar prontuários eletrônicos do paciente, os dados do paciente são armazenados em um registro digital seguro e distribuído entre várias partes, como hospitais, médicos e pacientes. Isso garante que os dados sejam acessados somente por pessoas autorizadas e que os registros de saúde do paciente possam ser compartilhados de maneira segura e eficiente entre diferentes organizações de saúde. Isso é especialmente importante em um cenário em que a privacidade dos dados do paciente é uma grande preocupação (Dhillon & Moores, 2019).

Em suma, o uso do *blockchain* como protocolo de segurança para prontuários eletrônicos do paciente é uma área de pesquisa promissora, que tem o potencial de transformar a maneira como os registros de saúde do paciente são armazenados, gerenciados e compartilhados entre diferentes organizações de saúde.

## 3 METODOLOGIA

### 3.1 Desenho de estudo

Para a realização do presente trabalho, foi feita uma revisão narrativa baseada no método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). As revisões sistemáticas, por meio da metodologia PRISMA, têm por objetivo aprimorar a qualidade dessas revisões, que são consideradas padrões de referência na área da saúde devido ao seu apoio em tomada de decisões clínicas e ao seu rigor metodológico (Moher et al., 2009).

A partir da definição da pergunta que guiou o presente trabalho, foi realizado um estudo com base na estratégia PICOS (*Population, Intervention, Comparator, Outcome and Study*).

A revisão sistemática foi conduzida em 6 etapas: busca na literatura, seleção de artigos, extração de informações dos estudos, avaliação dos estudos a serem incluídos na revisão, interpretação dos resultados e síntese da visão geral das informações obtidas.

### 3.2 Estratégia de busca

Para a busca e seleção dos artigos, foram escolhidas três bases de dados: BVS, Embase e PubMed/MEDLINE. Os descritores utilizados foram: “*Blockchain*”, “Prontuário Eletrônico do Paciente”, “*Patient Electronic Records*”, “*Electronic Health Record*”, “*Electronic Medical Record*” e “*Electronic Patient Record*”. As palavras foram combinadas com operadores booleanos AND e OR, formando a seguinte combinação: (BLOCKCHAIN) AND (((Patient Electronic Records) OR (Electronic Health Record) OR (Electronic Medical Record) OR (Electronic Patient Record) OR (Prontuário Eletrônico do Paciente))).

### 3.3 Identificação da pergunta da pesquisa

Qual é a perspectiva da utilização do *blockchain* como protocolo de segurança para estabelecimentos assistenciais de saúde que empregam prontuário eletrônico do paciente como ferramenta?

#### 3.3.1 População

A população consiste em pacientes que possuem seus dados relacionados à saúde registrados eletronicamente em EAS.

### 3.3.2 Intervenção e Comparação

Os estudos incluídos possuem o *blockchain* como protocolo de segurança no gerenciamento de sistemas eletrônicos destinados ao cuidado da saúde dos pacientes.

### 3.3.3 Desfecho

O desfecho principal dos artigos selecionados incluíram a informação da perspectiva da utilização do *blockchain* na segurança, privacidade e confiabilidade dos dados de saúde frente aos gerenciamentos tradicionais.

### 3.3.4 Tipos de Estudo

Os estudos selecionados aplicam *frameworks* e protótipos no intuito verificar a perspectiva da utilização do *blockchain* como protocolo de segurança nos PEP.

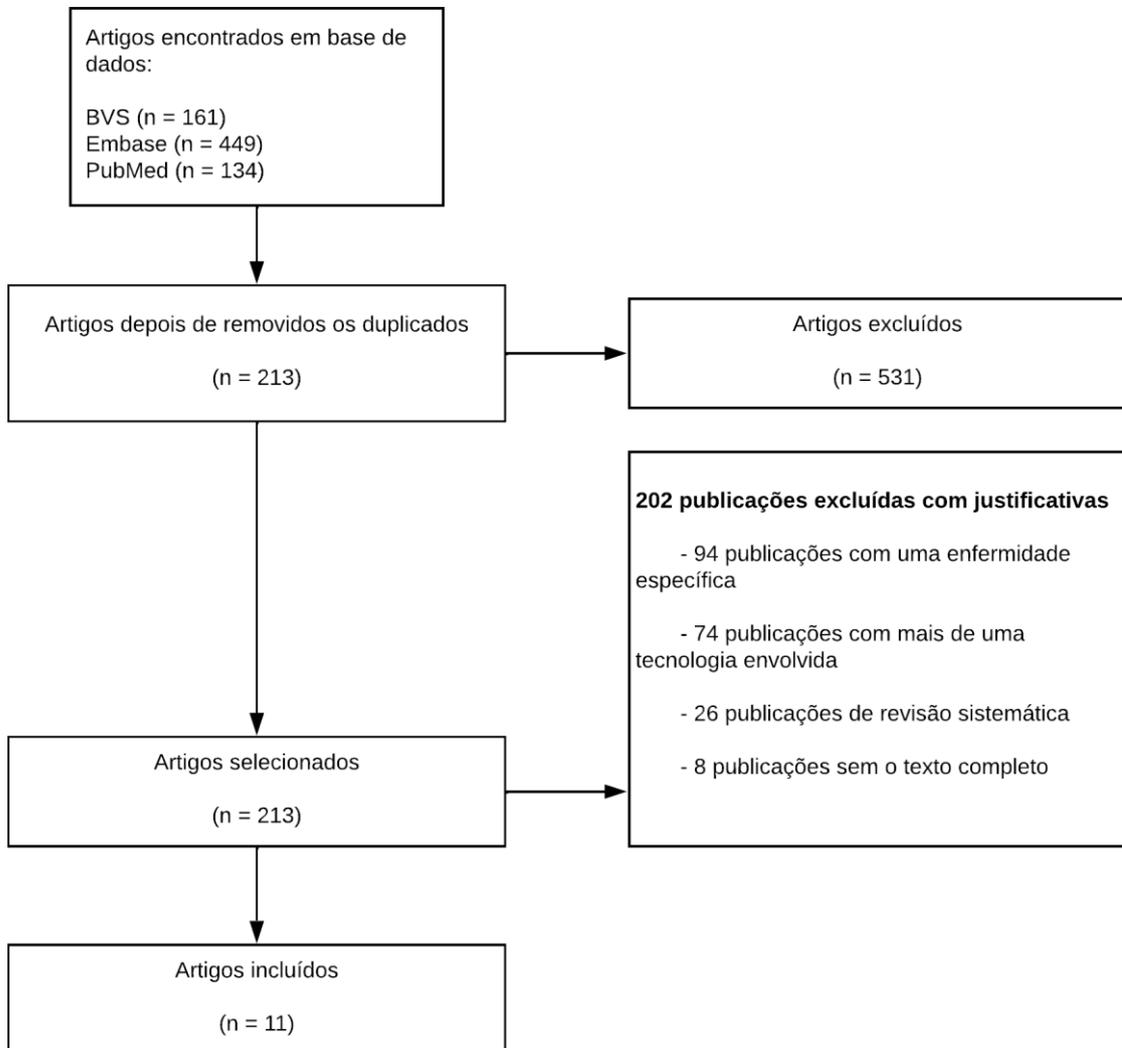
## 3.4 Critérios de inclusão e exclusão

Foram considerados artigos no período de 2009 a 2022, período após o surgimento do *Blockchain*. Foram desconsiderados os artigos que não tinham seu texto completo disponível, artigos de revisões de literatura ou meta-análises, estudos com foco em uma enfermidade específica e publicações que correlacionava *blockchain* com outros protocolos de segurança.

## 3.5 Análise de dados

A partir da seleção dos artigos, foi feita a avaliação de informações por meio da leitura integral de todos os estudos. Os itens selecionados para serem compreendidos na tabela foram: estudo, ano, país, desenvolvimento de um *framework* e/ou protótipo, teste com voluntários e a perspectiva da utilização. Todo o processo de seleção foi resumido no diagrama de fluxo PRISMA (Figura 1).

Figura 1 – Diagrama de fluxo PRISMA



Fonte: Autoria própria (2023)

## 4 RESULTADOS E DISCUSSÕES

Neste tópico, apresenta-se os resultados e discussões sobre os estudos selecionados que relatam o uso da tecnologia *blockchain* como alternativa para gerenciamento dos dados eletrônicos dos pacientes frente aos gerenciamentos atuais. O estudo teve como população apenas os pacientes, não verificando a visão dos profissionais de saúde. Durante a busca, percebeu-se que o assunto vem tornando-se popular nos últimos anos e que a tendência é que a tecnologia seja mais discutida e aplicada em diversos âmbitos.

Durante a busca, encontrou-se 744 artigos e foram removidos 531 estudos devido a duplicação. Foi realizada a busca também na base Cochrane, mas não foi obtido nenhum artigo a partir da combinação de palavras e conectivos utilizadas. Após isso, foi realizado uma filtragem com a leitura dos títulos, resumos e leitura integral dos textos no intuito de eleger os artigos de acordo com os critérios de seleção estabelecidos durante a revisão, resultando em 11 artigos finais. A interpretação dessas informações foi resumida de forma organizada na Tabela 1.

Tabela 1 – Estudos extraídos da revisão sistemática

ESTUDO	AUTOR	TÍTULO
Estudo 1	(Hylock & Zeng, 2019)	<i>A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study</i>
Estudo 2	(Beinke, Fitte & Teuteberg, 2019)	Towards a Stakeholder-Oriented <i>Blockchain</i> -Based Architecture for Electronic Health Records: Design Science Research Study
Estudo 3	(Tith et. al, 2020)	Application of <i>Blockchain</i> to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability
Estudo 4	(Tith et. al, 2020)	Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on <i>Blockchain</i> Technology
Estudo 5	(Cernian, Tiganoaia, Sacala, Pavel & Iftemi, 2020)	PatientDataChain: A <i>Blockchain</i> -Based Approach to Integrate Personal Health Records
Estudo 6	(Cadoret, Kailas, Velmovitsky, Morita & Igboeli, 2020)	Proposed Implementation of <i>Blockchain</i> in British Columbia's Health Care Data Management
Estudo 7	(Abunadi & Kumar, 2021)	BSF-EHR: <i>Blockchain</i> Security Framework for Electronic Health Records of Patients
Estudo 8	(Xiao, XU, Jiang & Wu, 2021)	The HealthChain <i>Blockchain</i> for Electronic Health Records: Development Study
Estudo 9	(Rai, 2022)	PcBEHR: patient-controlled <i>blockchain</i> enabled electronic health records for healthcare 4.0
Estudo 10	(Ma et. al, 2022)	PHDMF: A Flexible and Scalable Personal Health Data Management Framework Based on <i>Blockchain</i> Technology
Estudo 11	(Lee, Kim, Kwon, Kim & Cho, 2022)	Privacy Preservation in Patient Information Exchange Systems Based on <i>Blockchain</i> : System Design Study

Fonte: Autoria própria (2023)

## Conteúdo dos estudos selecionados

- **Estudo 1**

A pesquisa de número um chama-se “*A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study*”. O autor principal, Ray Hales, é da Faculdade de Ciências da Saúde da Universidade da Carolina do Leste na cidade de Greenville, Carolina do Norte, Estados Unidos. O texto foi publicado em 2019, no *Journal of medical Internet research*.

Neste artigo, os autores propõem uma nova estrutura de *blockchain* centrada no paciente chamada *HealthChain*, para melhorar o envolvimento do paciente, a curadoria de dados e a divulgação regulamentada da informação acumulada num ambiente seguro e interoperável. A estrutura utiliza normas de interoperabilidade, contratos inteligentes e identidades criptográficas para trocar com segurança dados de pacientes com os provedores e regular o acesso.

O quadro proposto aborda as principais barreiras à adesão do *blockchain* nos cuidados de saúde, incluindo segurança da informação, interoperabilidade, integridade dos dados, validação da identidade e escalabilidade. O documento descreve também um *blockchain* misto para apoiar o registo imutável e os bloqueios de pacientes com capacidade de rediscricção, bem como a utilização de re-criptação por procuração (PRE) para partilhar informação através de contratos revogáveis e inteligentes, assegurando a preservação da privacidade e confidencialidade.

O documento oferece várias melhorias PRE para melhorar o desempenho e a segurança. Foi desenvolvida uma ferramenta de código aberto e prova de conceito para avaliar o desempenho dos novos componentes de blocos de pacientes e configurações do sistema. A ferramenta foi utilizada para testar a estrutura proposta numa variedade de cenários, envolvendo um número variável de registos existentes e importados.

Os resultados do documento indicam que o *blockchain* é uma tecnologia potente e viável para o acesso e troca de informações de saúde centradas no paciente. O quadro proposto *HealthChain* apresenta pacientes e provedores com acesso a registos médicos consistentes e abrangentes. Os autores testaram 16 configurações da estrutura e encontraram várias configurações de alto desempenho e baixa largura de banda, embora não sejam as mais fortes do ponto de vista criptográfico. O algoritmo mais eficiente depende, em última análise,

das necessidades específicas do utilizador. Os autores sugerem que a encriptação avançada de dados com chaves estáticas, armazenamento incremental do servidor, e nenhuma encriptação adicional do lado do servidor são as mais rápidas e menos intensivas em largura de banda, enquanto que os dados encriptados por *proxy* com chaves dinâmicas, armazenamento incremental do servidor, e encriptação adicional do lado do servidor são o melhor desempenho das configurações mais fortes.

- **Estudo 2**

O estudo de número dois tem como título “*Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study*” e foi publicado no ano de 2019, no *Journal of medical Internet research*. O artigo tem como autor principal Jan Heinrich Beinke, do Departamento de Sistema de Informação da Universidade de Osnabrueck, e Contabilidade, na cidade de Osnabrueck, Alemanha.

A metodologia utilizada neste trabalho é o paradigma da Pesquisa Científica em Design (DSR). Esta abordagem envolve o desenvolvimento de artefatos inovadores para abordar problemas de relevância humana e contribuir com novos conhecimentos para a comunidade científica. O paradigma do DSR é adequado para desenvolver uma arquitetura de PEP baseada em *blockchain*. As partes interessadas foram envolvidas na fase de desenvolvimento para promover sua conscientização e compreensão da tecnologia. O desenvolvimento de uma solução é influenciado pelo meio ambiente e pelo corpo de conhecimento existente.

O artigo propõe uma arquitetura baseada em *blockchain* para PEP para tratar de questões de segurança de dados. Os autores identificaram três grandes grupos de interessados e 34 respectivos requisitos para a arquitetura proposta. Eles desenvolveram uma arquitetura de cinco camadas e a avaliaram através de *workshops* com 15 participantes. O estudo identificou 12 benefícios-chave e 12 desafios-chave de uma arquitetura baseada em *blockchain* para os PEP. Os autores sugerem que a tecnologia de *blockchain* tem o potencial de melhorar a segurança, rastreabilidade e automação dos dados através de contratos inteligentes nos prontuários eletrônicos.

As limitações deste trabalho são que os autores não puderam entrevistar representantes de cada grupo identificado de partes interessadas, tais como companhias de seguros ou institutos de pesquisa. Além disso, não foi incluída a opinião das partes interessadas mais importantes para a adoção dos PEP, ou seja, os pacientes. A atitude pessoal

em relação às inovações tecnológicas é altamente subjetiva e depende da idade, afinidade tecnológica e pré-experiências.

Os autores discutem alguns dos principais benefícios e desafios desta abordagem, o que poderia ter implicações nestas áreas. Por exemplo, o uso da tecnologia de *blockchain* poderia melhorar a segurança e a privacidade dos dados, o que tem implicações éticas e sociais. O uso de contratos inteligentes também poderia automatizar certos processos, o que poderia ter implicações econômicas. Entretanto, os autores sugerem que são necessárias mais pesquisas para compreender plenamente as implicações da implementação de um sistema de PEP baseado em *blockchain*.

- **Estudo 3**

O terceiro estudo selecionado é intitulado “*Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability*” e a autora principal, Dara Tith, é do Instituto de Pesquisa e Inovação, do Instituto de Tecnologia de Tokio, na cidade de Yokohama, Japão. O artigo foi publicado em 2020, na *Healthcare informatics research*.

Neste artigo, os autores propõem um sistema baseado em *blockchain* para a gestão dos dados dos pacientes nos cuidados de saúde. O sistema utiliza um provedor de serviços de adesão (MSP) para emitir identificações de inscrições eletrônicas (eID) aos pacientes, que são utilizadas como identificações de pacientes no sistema. Cada transação no livro de registros contém uma eID, que é acelerada após ser concatenada com um dado aleatório chamado *salt*. O sistema também utiliza endossadores para simular a proposta de transferência de dados de um paciente e fornecer-lhe as suas assinaturas digitais após validação do formato da proposta e execução bem sucedida do *chaincode* do pedido.

O MSP visa abstrair todos os mecanismos e protocolos criptográficos por trás da emissão e validação de certificados, e autenticação de utilizadores. Há dois tipos de MSP, canal e local. Um MSP de canal fornece um método para validar certificados de inscrição (ECerts) entre diferentes organizações do canal, enquanto um MSP local oferece um método para verificar a identidade de um utilizador numa organização. Já o *chaincode* é um programa de aplicação executado por pares para facilitar, verificar ou impor a negociação e o acordo entre utilizadores. Um *chaincode* é também conhecido como um contrato inteligente em outras plataformas de *blockchain*, como o *Ethereum*. Um *chaincode* tem muitas funções de

programação nele, e normalmente lê e atualiza o estado do livro razão com toda a lógica empresarial contida nas funções internas.

Os autores implementaram um protótipo do sistema e o testaram com cinco *chaincodes* contendo funções de lógica empresarial. Os resultados mostraram que o sistema foi capaz de lidar com mais de 3.500 transações por segundo e ele pode proporcionar aos pacientes um maior controle sobre os seus registros médicos, permitindo-lhes controlar quem acessou os seus dados e assegurar que cada transferência de dados é feita em conformidade com o seu consentimento. O sistema pode também reduzir o risco de violação de dados e de acesso não autorizado aos dados dos pacientes, utilizando um registo descentralizado e à prova de adulteração para armazenar e gerir registros médicos. Além disso, o sistema pode fornecer às instituições de saúde uma forma mais eficiente de gerir os dados dos pacientes, reduzindo a necessidade de intermediários e racionalizando o processo de intercâmbio de dados.

O artigo não menciona explicitamente quaisquer limitações do sistema proposto. Contudo, é importante notar que a implementação do sistema num contexto real pode enfrentar desafios, tais como a necessidade de padronização dos formatos de dados em diferentes instituições de saúde, a necessidade de conformidade regulamentar e o potencial de erros na introdução de dados. Além disso, o sistema pode exigir recursos computacionais significativos para lidar com um grande volume de transações, o que pode não ser viável para instituições de cuidados de saúde de menor dimensão. Em suma, o artigo conclui que o sistema proposto tem o potencial de melhorar a segurança e eficiência da gestão de dados de saúde.

- **Estudo 4**

O quarto artigo selecionado intitula-se “*Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on Blockchain Technology*” e a autora principal, Dara Tith, pertence ao Instituto de Pesquisa e Inovação, do Instituto de Tecnologia de Tokio, na cidade de Yokohama, Japão. O artigo foi publicado em 2020, na *Healthcare informatics research*.

O artigo propõe um novo sistema de consentimento eletrônico para que os pacientes possam gerir os seus dados de consentimento de forma mais elaborada. O sistema baseia-se na tecnologia de *blockchain* e utiliza um esquema de controle de acesso baseado em objetivos. Espera-se que o sistema proposto proporcione aos pacientes um maior controle sobre os seus dados, melhore a eficiência, a transparência e a rastreabilidade no tratamento do

consentimento para assegurar que os dados dos pacientes estão sendo compartilhados adequadamente entre os prestadores de cuidados de saúde.

Além disso, é apresentado brevemente o *Hyperledger Fabric* (HLF), seguido do conceito do seu sistema e do seu funcionamento. O HLF consiste em um *blockchain* e banco de dados estaduais. O primeiro é um diário de transações, enquanto o segundo contém os valores atuais dos estados do livro razão. Devido ao banco de dados de estados, o programa obtém prontamente valores sem atravessar todo o log de transações. As transações são coletadas para formar um bloco que é anexado sequencialmente ao último bloco do *blockchain*, que é imutável uma vez que é feito.

No entanto, o artigo não fornece quaisquer resultados experimentais ou avaliação do sistema proposto. Por conseguinte, são necessárias maiores investigações e testes para determinar a eficácia e praticabilidade do sistema proposto.

- **Estudo 5**

A pesquisa de número 5 chama-se "*PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records*" e foi publicada na Revista Científica *Sensors* no ano de 2020. A autora principal, Alexandra Cernian, é da Faculdade de Controle Automação e Computação da Universidade Politécnica de Bucareste, Romênia.

O estudo descreve o projeto, a implementação e a validação experimental de um sistema baseado em *blockchain* chamado *PatientDataChain* para integrar registros pessoais de saúde de várias fontes em um sistema unificado e descentralizado de PEP. A metodologia utilizada no trabalho inclui a realização de uma prova de conceito (PoC) em uma clínica médica em Bucareste, utilizando um conjunto de dados de 100 pacientes e 1144 transações ao longo de um período de três meses, integrando-se com o sistema PEP existente na clínica, chamado BizMedica.

A PoC foi realizada coletando dados específicos dos registros médicos dos pacientes usando sensores de vários dispositivos, que podem ser usados para interligar diferentes provedores de saúde e integrar os dados coletados em um sistema PEP unitário e permitir que os pacientes sejam os proprietários de seus dados. Com isso, é possível fornecer o acesso seguro aos registros médicos e alavancar a natureza descentralizada da tecnologia de

*blockchain* para criar um sistema seguro, flexível e confiável de compartilhamento e troca de dados.

O artigo não menciona explicitamente quaisquer limitações do sistema proposto. Entretanto, como em qualquer nova tecnologia, pode haver desafios na implementação e dimensionamento do sistema em cenários do mundo real. Além disso, o artigo não aborda potenciais questões regulatórias ou legais relacionadas ao uso da tecnologia de *blockchain* na saúde.

A conclusão do estudo é que o *PatientDataChain*, um sistema PEP baseado no *blockchain*, melhora o armazenamento descentralizado dos registros médicos e o intercâmbio de dados entre os prestadores de serviços de saúde. O sistema oferece aos pacientes e médicos um registro imutável, seguro, flexível e confiável de prontuários eletrônicos e a arquitetura do *PatientDataChain*, tendo o paciente em seu núcleo e colocando o paciente no controle de seus dados médicos, aproveita um sistema PEP contendo uma versão única e unitária dos prontuários médicos do paciente.

O estudo de validação provou que o *PatientDataChain* cria o contexto adequado para a interoperabilidade e troca de informações médicas entre os agentes de saúde. Além disso, o sistema pode ser escalável para um grande número de usuários e tem o potencial de revolucionar a indústria da saúde, fornecendo uma infraestrutura confiável para a troca e armazenamento de dados médicos.

- **Estudo 6**

O sexto estudo selecionado é intitulado "*Proposed Implementation of Blockchain in British Columbia's Health Care Data Management*", publicado em 2020 no *Journal of medical Internet research*. A autora principal, Danielle Cadoret, é do Programa de Ciência e Negócios da Faculdade de Ciência, da Universidade de Waterloo, Canadá.

Neste estudo, os autores realizaram uma análise da atual infraestrutura de gestão de dados de saúde na província Colúmbia Britânica do Canadá para identificar possíveis lacunas e ineficiências no sistema Canadense de gestão de dados de saúde. Eles exploraram o potencial da utilização da tecnologia do *blockchain* como solução para superar as lacunas existentes nas soluções de PEP no sistema de cuidados de saúde da província. Os autores construíram a infraestrutura de dados de cuidados de saúde da Colúmbia Britânica e o fluxo de

informação sanitária com base em informação disponível ao público e em parceria com um perito da indústria familiarizado com a rede de tecnologia de informação dos sistemas de saúde das Autoridades Provinciais de Serviços de Saúde da Colômbia Britânica. Eles analisaram as lacunas, inconsistências e ineficiências do fluxo de informação.

Foram identificados, de acordo com o artigo, vários desafios na atual infraestrutura de gestão de dados de saúde na província, incluindo silos de informação, potencial para erros médicos, falta de interoperabilidade e falhas de segurança. Os autores descobriram que uma solução baseada em *blockchain* tem o potencial de resolver a maioria destes desafios na gestão de dados de cuidados de saúde da população Canadense.

A solução baseada em *blockchain* oferece armazenamento descentralizado para aumentar a segurança para fornecer aos pacientes e às instalações de cuidados de saúde acesso seguro aos registos médicos, e mais importante ainda, interoperabilidade para permitir a transferência de registos médicos a qualquer pessoa que tenha permissão e necessite acessar aos mesmos. As conclusões deste documento podem ser utilizadas pelos políticos Canadenses e prestadores de cuidados de saúde para melhorar a atual infraestrutura de gestão de dados de saúde e para explorar o potencial da utilização de tecnologia *blockchain* na gestão de dados de cuidados de saúde.

- **Estudo 7**

O artigo de número sete chama-se “*BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients*” e tem como autor principal Ibrahim Abunadi. O estudo foi publicado na Revista Científica *Sensors*, no ano de 2021. O autor principal pertence a Faculdade de Ciência da Informação e Computação da Universidade de Prince Sultan, Arábia Saudita.

O estudo propõe um quadro de segurança em *blockchain* (BSF) para armazenar e gerir com segurança os registos de saúde eletrônicos (EHR). A estrutura é concebida para equilibrar a confidencialidade dos dados, a procura dos pacientes e a interação constante com os dados do provedor. A metodologia envolve a utilização de tecnologia *blockchain* para distribuir informação de forma transacional e descentralizada. O artigo apresenta também resultados de simulação que mostram a eficácia do quadro proposto na proteção dos dados de EHR.

Ao utilizar a BSF-EHR, o paciente é capaz de gerir, descarregar e compartilhar os seus dados EHR de forma independente. Os resultados experimentais mostram que a BSF-EHR consegue uma partilha de dados segura entre os seus utilizadores. Mais importante ainda, o sistema de controle de acesso BSF-EHR é capaz de proteger importantes tentativas de ataques externos aos dados eletrônicos de saúde do paciente.

No entanto, o estudo não discute a implementação do quadro proposto num cenário do mundo real. Além disso, não compara o quadro proposto com outras soluções de segurança EHR existentes. Além do mais, o documento não aborda as potenciais questões de escalabilidade que podem surgir durante a implementação do quadro proposto num sistema de saúde de grande escala.

- **Estudo 8**

O oitavo estudo selecionado foi publicado no ano de 2021 no *Journal of medical Internet research* e tem como título “*The HealthChain Blockchain for Electronic Health Records: Development Study*”. Seu autor principal Yonggang Xiao é da Faculdade de Ciência da Computação da Universidade de Ciência e Tecnologia de Hubei, da cidade de Xianning, China.

A pesquisa propõe um *blockchain* experimental para PEP chamada *HealthChain*. Ela é construída utilizando a tecnologia de *blockchain* de consórcio, onde três organizações (hospitais, provedores de seguros e agências governamentais) formam um consórcio que funciona sob um modelo de governação. A *HealthChain* armazena os PEP num livro-razão distribuído e os partilha entre diferentes participantes. O protocolo de consenso adotado na *HealthChain* chama-se prova de autoridade (PoA), que verifica a identidade de quem executa o pedido de PEP e quem embala as transações de PEP num bloco. Os dois parâmetros de tempo limite do grupo e tamanho do grupo têm um impacto elevado no desempenho da *HealthChain*.

A *HealthChain* supera as desvantagens dos sistemas tradicionais de PEP e atinge requisitos funcionais e não funcionais, como o armazenamento dos PEP. Ela também demonstra características superiores, tais como preservação da privacidade, segurança e elevado rendimento. A tecnologia de *blockchain* proposta pelo consórcio e o algoritmo de consenso podem ser utilizados como referência para a construção de sistemas semelhantes no futuro.

O artigo identifica uma limitação do protótipo *HealthChain*, que é o único ponto de falha causado pelo único solicitante. Se o solicitante falhar, as transações PEP não podem ser encomendadas num bloco, causando a falha de todo o sistema. No entanto, o artigo sugere uma solução para este problema através da implementação de um serviço de solicitações que consiste num conjunto de nós de serviço de encomendas e um agrupamento *Kafka* com o seu conjunto *ZooKeeper*. Isto ajudará não só a construir um sistema tolerante a falhas, mas também a aumentar o desempenho devido ao equilíbrio de carga.

Por fim, o artigo conclui que a adoção da *HealthChain* ou de sistemas semelhantes pode melhorar a exatidão e a integridade dos registos de saúde, levando a melhores cuidados e resultados para os pacientes.

- **Estudo 9**

O estudo de número nove é intitulado “*PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0*” e seu único autor Bipin Kumar Rai, pertence ao Departamento de Tecnologia da Informação do Instituto de Tecnologia ABES, na cidade de Ghaziabad, Índia. O artigo foi publicado no ano de 2022 na revista *Health Services and Outcomes Research Methodology*.

O estudo propõe um sistema de Registros de Saúde Eletrônicos Ativados por *Blockchain* e Controlado pelo Paciente (PcBEHR) para dar aos pacientes o controle sobre os seus dados médicos. O sistema tem três camadas: camada de interface do utilizador, camada de *blockchain* e camada de acesso aos dados. Os participantes podem interagir com o sistema através de qualquer dispositivo de PC e registar-se através da aplicação do cliente. Uma chave privada com uma identificação única é gerada pelo administrador a fim de alistar o membro. A técnica proposta utiliza o armazenamento de ficheiros Interplanetário Descentralizado. Os dois principais critérios de desempenho utilizados para avaliar as soluções sugeridas são o custo e a precisão.

O sistema proposto é descentralizado, imutável, transparente, rastreável e digno de confiança. O documento conclui que esse sistema pode proporcionar aos pacientes um controle seguro sobre os seus dados médicos. A utilização de tecnologia de *blockchain* pode fornecer soluções para questões como privacidade, segurança da informação e autenticação no setor da saúde. No entanto, o estudo não fornece uma análise detalhada da escalabilidade e desempenho do sistema sob cargas pesadas. Além disso, o documento não discute os

potenciais desafios da implementação do sistema proposto em ambientes de cuidados de saúde do mundo real.

Os principais desafios associados aos atuais sistemas de PEP são o fato de não proporcionarem aos pacientes uma rastreabilidade, confiabilidade e segurança sobre os seus dados médicos, criando sérios riscos de segurança. Além disso, a maioria das atuais técnicas e sistemas PEP estão centralizados, o que dificulta a partilha de dados médicos e aumenta o perigo de um único ponto de falha. Os PEP controlado pelo paciente a partir da tecnologia *blockchain* podem abordar estas questões, proporcionando aos pacientes um controle seguro sobre os seus dados, descentralizado, imutável, transparente, rastreável e digno de confiança. A utilização da tecnologia *Blockchain* pode permitir uma computação confiável, transparente e auditável na indústria dos estabelecimentos assistenciais de saúde, utilizando uma rede descentralizada de pares e uma razão pública.

- **Estudo 10**

O décimo estudo selecionado tem como título “*PHDMF: A Flexible and Scalable Personal Health Data Management Framework Based on Blockchain Technology*” e seus autores são de Universidades e Laboratórios da China. O artigo foi publicado no ano de 2022 na revista *Frontiers in Genetics*.

O documento apresenta um quadro federal de gestão de dados pessoais de saúde (PHDMF) que utiliza tecnologia de *blockchain* para estabelecer um consórcio de dados sobre múltiplas instituições médicas. A estrutura proporciona um ambiente seguro e de confiança para a supervisão e circulação de dados de saúde, o que facilita o estabelecimento do consórcio sobre as instituições médicas e ajuda a alcançar o valor da partilha e extração de dados.

A utilização de tecnologia de armazenamento distribuído permite que os dados pessoais de saúde sejam armazenados nas suas instituições médicas originais, reduzindo a necessidade de transferência massiva de dados. A tecnologia de registo distribuído regista o valor *hash* dos dados, o que pode identificar modificações maliciosas dos dados. A tecnologia de contrato inteligente gerencia o acesso dos utilizadores e o funcionamento dos dados, tornando o processo de transação de dados rastreável e resolvendo o problema da proveniência dos dados. É fornecido um ambiente informático confiável para meta-análise com informação estatística em vez de dados originais.

O documento não menciona quaisquer limitações específicas do quadro proposto. Contudo, é importante notar que a implementação de tal quadro pode enfrentar desafios relacionados com a privacidade, segurança e interoperabilidade dos dados entre diferentes instituições médicas. Além disso, a adoção de tecnologia de *blockchain* na indústria da saúde está ainda nas suas fases iniciais e será necessário maiores investigações para avaliar a sua eficácia e escalabilidade na gestão de dados pessoais de saúde.

- **Estudo 11**

A última pesquisa selecionada é intitulada “*Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study*” e seu autor principal é do Departamento de Ciência da Computação e Engenharia, da Universidade de Hanyang, República da Coreia. O estudo foi publicado no *Journal of medical Internet research* no ano de 2022.

Este documento propõe um sistema de troca de informação de pacientes (PIE) descentralizada baseada em *blockchain* que pode partilhar prontuários eletrônicos de forma segura e eficiente. O sistema proposto utiliza uma rede em *blockchain* para gerir e partilhar PEP entre pacientes, hospitais e outros utilizadores. O sistema utiliza criptografia de dados e controle de acesso para proteger a privacidade e segurança dos PEP dos pacientes durante o processo de intercâmbio de dados. Além disso, é utilizado um esquema distribuído de partilha de dados para proporcionar escalabilidade e partilha rápida de PEP, independentemente da sua dimensão ou tipo.

Os modelos de simulação foram implementados utilizando *Hyperledger Fabric*, uma estrutura de *blockchain* de código aberto, para testar o desempenho e a segurança do sistema proposto. A simulação consistiu em dois médicos, um paciente, um consórcio médico, e uma rede de sistema de arquivos interplanetário (IPFS) pública participando na rede de *blockchain* como a unidade mínima para a partilha de um PEP. O documento avaliou o desempenho do sistema PIE proposto medindo o tempo necessário para o processo de partilha de PEP e o tempo de execução do contrato inteligente para a partilha de chaves de re-criptação. A simulação foi realizada utilizando vários dados, desde o formato de texto até imagens médicas.

Os resultados mostraram que o sistema proposto pode partilhar rapidamente PEP, independentemente do seu tamanho ou tipo, com uma média de 0,01014 segundos para descarregar 1 MB de PEP no sistema PIE proposto. A análise de segurança também confirmou

que o mecanismo de segurança proposto pode proteger eficazmente os PEP dos utilizadores contra falsificações e ameaças de fugas de privacidade e fornecer integridade de dados. Em suma, o documento conclui que o sistema PIE proposto pode gerir e partilhar PEP de forma segura, superando os problemas do sistema médico existente baseado em *blockchain*.

No entanto, existe algumas limitações descritas no estudo como a maturidade tecnológica dos sistemas médicos baseados em *blockchain* ainda permanecem ao nível do protótipo. Os formatos de dados médicos utilizados por diferentes países ou instituições variam consideravelmente, o que torna difícil a partilha de dados médicos. E para criar com sucesso o ambiente médico da próxima geração através de um sistema médico baseado em *blockchain*, várias e complexas questões, tais como o *backlash* do campo médico, ramificações legais relacionadas com cuidados médicos, limitações técnicas, e normas de dados, devem ser abordadas.

Os artigos foram resumidos de forma organizada na tabela 2. Os itens selecionados para serem compreendidos na tabela foram: estudo, ano, país, desenvolvimento de um *framework* e/ou protótipo, testes desses *frameworks* e/ou protótipos desenvolvidos e avaliação com voluntários ou em EAS e a perspectiva da utilização.

Tabela 2 – Quadro comparativo dos estudos

ESTUDO	ANO	PAÍS	Desenvolvimento de um protótipo ou framework?	Realizado teste do protótipo?	Avaliação com EAS ou voluntários?	Perspectiva da utilização do <i>Blockchain</i>
1	2019	ESTADOS UNIDOS	SIM	SIM	NÃO	O <i>blockchain</i> é uma tecnologia potente e viável para o acesso e troca de informações de saúde centradas no paciente
2	2019	ALEMANHA	SIM	SIM	SIM	A tecnologia de <i>blockchain</i> tem o potencial de melhorar a segurança, rastreabilidade e automação dos dados através de contratos inteligentes nos EHRs
3	2020	JAPÃO	SIM	SIM	NÃO	O sistema proposto com o <i>blockchain</i> tem o potencial de melhorar a segurança e eficiência da gestão de dados de saúde
4	2020	JAPÃO	SIM	NÃO	NÃO	O artigo não fornece quaisquer resultados experimentais ou avaliação do sistema proposto
5	2020	ROMÊNIA	SIM	SIM	SIM	O sistema oferece aos pacientes e médicos um registro imutável, seguro, flexível e confiável de prontuários eletrônicos
6	2020	CANADÁ	SIM	NÃO	NÃO	Uma solução baseada em <i>blockchain</i> tem o potencial de resolver desafios na gestão de dados de cuidados de saúde da população
7	2021	ARÁBIA SAUDITA	SIM	SIM	NÃO	O sistema baseado em <i>blockchain</i> consegue uma partilha de dados segura e é capaz de proteger importantes tentativas de ataques externos aos dados eletrônicos de saúde do paciente
8	2021	CHINA	SIM	SIM	NÃO	A adoção de sistemas em <i>blockchain</i> pode melhorar a exatidão e a integridade dos registos de saúde, levando a melhores cuidados e resultados para os pacientes
9	2021	ÍNDIA	SIM	NÃO	NÃO	A utilização da tecnologia <i>Blockchain</i> pode permitir uma computação confiável, transparente e auditável na indústria dos estabelecimentos assistenciais de saúde
10	2022	CHINA	SIM	NÃO	NÃO	A adoção de tecnologia de <i>blockchain</i> na indústria da saúde está ainda nas suas fases iniciais e será necessário maiores investigações para avaliar a sua eficácia e escalabilidade na gestão de dados pessoais de saúde
11	2022	COREIA DO SUL	SIM	SIM	SIM	O sistema proposto pode partilhar rapidamente os dados eletrônicos dos pacientes e pode proteger eficazmente esses dados

Fonte: Autoria própria

## Discussão sobre os estudos

Existem diversos problemas atuais relacionados ao método de gerenciamento dos dados dos pacientes, que podem ser agravados em contextos de saúde pública. Dentre os principais problemas, podemos destacar a falta de padronização, pois os dados dos pacientes são armazenados em diferentes sistemas e formatos, o que dificulta a integração e compartilhamento de informações entre diferentes prestadores de serviços de saúde. Isso pode levar a erros de diagnóstico e tratamento, além de atrasar a tomada de decisão. A falta de segurança também é um fator importante devido ao uso de sistemas centralizados para armazenar e gerenciar dados dos pacientes aumentando o risco de violações de segurança e privacidade. Isso pode levar a acessos não autorizados, roubo de identidade, perda de dados e outros tipos de fraude.

A dificuldade no acesso aos dados é também um dos problemas, pois os pacientes muitas vezes têm dificuldade em acessar seus próprios dados de saúde, o que pode prejudicar a sua capacidade de gerenciar sua própria saúde e tomar decisões informadas sobre tratamentos e procedimentos. Além disso, a manutenção e gestão dos sistemas tradicionais de gerenciamento de dados de saúde podem ser muito caros, especialmente em relação a atualizações e integrações de sistemas. E por fim, a falta de transparência, pois muitas vezes os pacientes não têm conhecimento sobre quem tem acesso aos seus dados de saúde, como eles são usados e compartilhados, o que pode levar a desconfiança e falta de transparência no sistema de saúde.

Em resumo, o método de gerenciamento atual dos dados dos pacientes enfrenta diversos problemas relacionados à falta de padronização, segurança, acesso, custos elevados e transparência. Esses problemas podem ser agravados em situações de saúde pública, destacando a necessidade de soluções mais seguras e eficientes para o gerenciamento de dados de saúde.

No estudo proposto, foi realizada a busca de artigos que faz o uso da tecnologia *blockchain* para aprimorar o método de gerenciamento eletrônico de dados dos pacientes em estabelecimentos assistenciais de saúde. Entre os estudos selecionados, observa-se que todos desenvolveram uma arquitetura de protótipo ou *framework* no intuito de tentar realizar testes para comprovar a viabilidade do uso desse sistema frente aos gerenciamentos tradicionais. No entanto, entre os onze artigos, somente sete puderam testar a eficácia de seus

protótipos desenvolvidos e somente três fizeram uma avaliação em EAS com dados de voluntários.

Dentre os estudos selecionados que realizaram testes de eficácia foi possível visualizar a viabilidade do uso da tecnologia em diferentes aspectos. O primeiro a ser destacado é a segurança, pois o uso da tecnologia *blockchain* pode trazer diversos benefícios em relação a segurança no armazenamento e gerenciamento de PEP. Isso ocorre devido às características da tecnologia, como a descentralização e a criptografia.

A descentralização é um dos principais benefícios da tecnologia *blockchain*. Em um sistema de gestão de prontuários eletrônicos baseado em *blockchain*, as informações são armazenadas em uma rede distribuída de computadores, em vez de em um único servidor centralizado. Isso significa que não há um único ponto de falha, o que aumenta a segurança dos dados. Além disso, a descentralização garante que os dados não possam ser alterados ou excluídos sem o conhecimento dos participantes da rede.

Outra característica importante da tecnologia *blockchain* é a criptografia. A tecnologia usa algoritmos criptográficos para proteger os dados dos pacientes. Isso garante que as informações dos pacientes permaneçam confidenciais e seguras, mesmo em caso de violações de segurança. Além disso, a criptografia garante que apenas pessoas autorizadas possam acessar os dados do paciente.

Além do mais, a tecnologia *blockchain* pode ajudar a aumentar a transparência e a rastreabilidade dos dados do paciente. Cada transação realizada na rede *blockchain* é registrada em um registro imutável e auditável, o que garante a integridade dos dados. Isso permite que os pacientes possam rastrear quem acessou seus dados e quando, o que aumenta a transparência e a confiança no sistema de saúde.

Outro aspecto que viabiliza o uso da tecnologia *blockchain* é em relação a agilidade e eficácia no gerenciamento de prontuários eletrônicos de pacientes. Uma das principais vantagens da tecnologia *blockchain* é que ela permite a integração e compartilhamento de dados de forma mais eficiente e segura. Como os dados são armazenados em uma rede distribuída, eles podem ser acessados de forma mais rápida e fácil, eliminando a necessidade de procurar informações em diferentes sistemas e formatos.

Isso significa que os profissionais de saúde podem ter acesso imediato às informações dos pacientes, o que pode ser especialmente importante em casos de emergência. Por exemplo, se um paciente viaja para outro país e precisa de atendimento médico, os profissionais de saúde podem acessar o prontuário eletrônico do paciente por meio de uma rede *blockchain*, o que pode ajudar a garantir que o tratamento seja consistente e baseado em informações precisas. Além do mais, o compartilhamento de informações em uma rede *blockchain* pode reduzir a duplicação de exames e procedimentos, o que pode economizar tempo e recursos.

A tecnologia também pode ser utilizada para automatizar processos, como a autorização de tratamentos e procedimentos. Isso pode ajudar a reduzir a burocracia e a aumentar a eficiência do sistema de saúde. Por exemplo, em vez de esperar por aprovações manuais, um sistema baseado em *blockchain* poderia permitir que os profissionais de saúde autorizem tratamentos automaticamente, com base em regras predefinidas.

Outra vantagem da tecnologia *blockchain* é a possibilidade de criar contratos inteligentes, que são acordos digitais que se autoexecutam quando as condições especificadas são atendidas. Isso pode ser usado para automatizar o processo de pagamentos e reembolsos, o que pode ajudar a reduzir erros e fraudes.

Em relação à confiabilidade, a tecnologia *blockchain* usa um sistema de validação distribuída que permite que as transações sejam validadas por múltiplos nós de rede, em vez de depender de um único servidor centralizado. Isso significa que é muito difícil para um invasor comprometer o sistema ou alterar os dados, o que aumenta a confiabilidade dos prontuários eletrônicos. Além da criptografia que foi mencionada, também pode ser utilizado autenticação digital para aumentar a confidencialidade e a privacidade das informações.

Por fim, em termos de flexibilidade, os estudos sugerem que a tecnologia *blockchain* permite que os prontuários eletrônicos sejam acessados de forma mais fácil e segura em diferentes locais e dispositivos. Isso pode ser especialmente útil para pacientes que precisam ser atendidos em diferentes clínicas ou hospitais, ou que mudam de cidade ou país.

Embora a tecnologia *blockchain* possa trazer muitos benefícios para o gerenciamento de prontuários eletrônicos de pacientes, há desafios significativos que devem ser enfrentados para que a implementação dessa tecnologia seja bem-sucedida.

Um dos principais desafios é a interoperabilidade entre diferentes sistemas de saúde. Como a tecnologia *blockchain* é relativamente nova, ainda não existe um padrão universal para o armazenamento e o compartilhamento de dados de saúde na rede *blockchain*. Isso significa que diferentes sistemas de saúde podem ter formatos de dados diferentes e podem usar diferentes plataformas de *blockchain*, o que pode dificultar a integração e a interoperabilidade entre eles.

Outro desafio é a privacidade dos dados do paciente. Embora a tecnologia *blockchain* seja altamente segura e confiável, ainda existem preocupações com a privacidade dos dados do paciente. Por exemplo, se as informações do paciente forem armazenadas em uma rede pública de *blockchain*, qualquer pessoa com acesso à rede pode ver os dados. Isso pode ser problemático para pacientes que desejam manter suas informações de saúde privadas e confidenciais.

Além disso, a tecnologia *blockchain* também pode enfrentar desafios em relação à escalabilidade e desempenho. Como as informações são armazenadas em uma rede distribuída, pode ser mais difícil para a rede processar um grande volume de transações simultâneas. Isso pode levar a atrasos e interrupções no processamento de transações, o que pode afetar a eficiência e a agilidade do sistema de gerenciamento de prontuários eletrônicos.

## 5 CONCLUSÃO

A tecnologia *blockchain* tem sido cada vez mais explorada em diferentes setores e áreas, incluindo na saúde e, principalmente, na gestão de prontuários eletrônicos de pacientes. A sua principal característica é a descentralização, que garante maior segurança, transparência e confiabilidade nos registros e transações realizados.

No contexto da gestão de prontuários eletrônicos, o uso da tecnologia *blockchain* pode trazer diversas vantagens em relação aos sistemas tradicionais. Dentre elas, podemos destacar:

- **Maior segurança:** A descentralização garante que os dados não possam ser alterados ou excluídos sem o conhecimento dos participantes da rede. Além disso, a criptografia utilizada na tecnologia *blockchain* garante a proteção dos dados sensíveis dos pacientes.
- **Transparência:** Como a tecnologia *blockchain* permite que os dados sejam acessados por diferentes participantes da rede, ela promove maior transparência e confiança no processo de gestão dos prontuários eletrônicos.
- **Agilidade:** A tecnologia *blockchain* permite a execução de transações de forma rápida e segura, o que pode agilizar o processo de atualização e compartilhamento de informações dos prontuários eletrônicos.
- **Redução de custos:** O uso da tecnologia *blockchain* pode reduzir os custos com a manutenção e armazenamento dos prontuários eletrônicos, uma vez que não é necessário um servidor centralizado para gerenciar as informações.

No entanto, é importante mencionar que o uso da tecnologia *blockchain* em prontuários eletrônicos ainda enfrenta alguns desafios, como a necessidade de padronização e integração com outros sistemas de saúde existentes. Além disso, é preciso garantir a privacidade dos dados dos pacientes e a conformidade com as leis de proteção de dados em vigor.

Portanto, apesar dos desafios, a tecnologia *blockchain* é uma opção viável e promissora para a gestão de prontuários eletrônicos de pacientes, sobretudo em relação à segurança, transparência, agilidade e redução de custos.

## 6 REFERÊNCIAS

Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. *Sensors (Basel, Switzerland)*, 21(8), 2865. <https://doi.org/10.3390/s21082865>.

Beinke, J. H., Fitte, C., & Teuteberg, F. (2019). Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study. *Journal of medical Internet research*, 21(10), e13585. <https://doi.org/10.2196/13585>.

Boyd, C., & Mathuria, A. (Eds.). (2011). *Protocols for authentication and key establishment*. Springer.

Cadoret, D., Kailas, T., Velmovitsky, P., Morita, P., & Igboeli, O. (2020). Proposed Implementation of Blockchain in British Columbia's Health Care Data Management. *Journal of medical Internet research*, 22(10), e20897. <https://doi.org/10.2196/20897>.

Cernian, A., Tiganoaia, B., Sacala, I., Pavel, A., & Iftemi, A. (2020). PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records. *Sensors (Basel, Switzerland)*, 20(22), 6538. <https://doi.org/10.3390/s20226538>.

Dhillon, G., & Moores, T. T. (2019). Digital ledger technology and blockchain. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1*, 103-128.

Di Matteo, B., Tarabella, V., Filardo, G., Mosca, M., Lo Presti, M., Viganò, A., Tomba, P., & Marcacci, M. (2017). Art in Science: Mondino de' Liuzzi: The Restorer of Anatomy. *Clinical orthopaedics and related research*, 475(7), 1791–1795. <https://doi.org/10.1007/s11999-016-5213-5>.

Ekblaw, A. C. (2014). *MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis*. MIT Media Lab Research.

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*. John Wiley & Sons.

Fruhling, A. L., & Talley, P. C. (2003). *Electronic health records: Understanding and using computerized medical records (2nd ed.)*. Upper Saddle River, NJ: Prentice Hall.

Gans, D., Kralewski, J., Hammons, T., & Dowd, B. (2005). Medical groups' adoption of electronic health records and information systems. *Health affairs (Project Hope)*, 24(5), 1323–1333. <https://doi.org/10.1377/hlthaff.24.5.1323> .

Garfinkel, S. L. (2003). Design principles and patterns for computer systems that are simultaneously secure and usable. Ph.D. Thesis, Massachusetts Institute of Technology.

Goodman K. W. (2010). Ethics, information technology, and public health: new challenges for the clinician-patient relationship. *The Journal of law, medicine & ethics : a journal of the American Society of Law, Medicine & Ethics*, 38(1), 58–63. <https://doi.org/10.1111/j.1748-720X.2010.00466.x>.

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and structural biotechnology journal*, 16, 224–230. <https://doi.org/10.1016/j.csbj.2018.06.003>.

Halamka, J., Lippman, A., Ekblaw, A., & Lippman, J. (2018). The potential for *blockchain* to transform electronic health records. *Harvard Business Review*, 3.

Harrison, J. P., & Palacio, C. (2006). The role of clinical information systems in health care quality improvement. *The health care manager*, 25(3), 206–212. <https://doi.org/10.1097/00126450-200607000-00003>.

Hersh W. (2009). A stimulus to define informatics and health information technology. *BMC medical informatics and decision making*, 9, 24. <https://doi.org/10.1186/1472-6947-9-24>.

Hillestad, R., Bigelow, J., Bower, A., Giroso, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health affairs (Project Hope)*, 24(5), 1103–1117. <https://doi.org/10.1377/hlthaff.24.5.1103>.

Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. *Journal of medical Internet research*, 21(8), e13592. <https://doi.org/10.2196/13592>.

Kaufman, C., Perlman, R., & Speciner, M. (2012). *Network security: Private communication in a public world*. Prentice Hall.

Lee, S., Kim, J., Kwon, Y., Kim, T., & Cho, S. (2022). Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study. *Journal of medical Internet research*, 24(3), e29108. <https://doi.org/10.2196/29108>.

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018). BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. *Em 2018 IEEE Global Communications Conference (GLOBECOM). GLOBECOM 2018 - 2018 IEEE Global Communications Conference. IEEE*. <https://doi.org/10.1109/glocom.2018.8647713>.

Ma, L., Liao, Y., Fan, H., Zheng, X., Zhao, J., Xiao, Z., Zheng, G., & Xiong, Y. (2022). PHDMF: A Flexible and Scalable Personal Health Data Management Framework Based on Blockchain Technology. *Frontiers in genetics*, 13, 877870. <https://doi.org/10.3389/fgene.2022.877870>.

Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk management and healthcare policy*, 4, 47–55. <https://doi.org/10.2147/RMHP.S12985>.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS medicine*, 6(7), e1000097. <https://doi.org/10.1371/journal.pmed.1000097>.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. [Bitcoin.org](http://Bitcoin.org).

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Rahmani, A. M., Bayramov, S., & Kiani Kalejahi, B. (2021). Internet of Things Applications: Opportunities and Threats. *Em Wireless Personal Communications (Vol. 122, Issue 1, p. 451–476)*. Springer Science and Business Media LLC. <https://doi.org/10.1007/s11277-021-08907-0>.

Rai, B.K., (2022). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Serv Outcomes Res Method* 23, 80–102. <https://doi.org/10.1007/s10742-022-00279-7>.

Shortliffe E. H. (1999). The evolution of electronic medical records. *Academic medicine : journal of the Association of American Medical Colleges*, 74(4), 414–419. <https://doi.org/10.1097/00001888-199904000-00038>.

Sittig, D. F., & Singh, H. (2012). Electronic health records and national patient-safety goals. *The New England journal of medicine*, 367(19), 1854–1860. <https://doi.org/10.1056/NEJMs1205420>.

Stallings, W. (2017). *Cryptography and network security: Principles and practice (7th ed.)*. Pearson.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohshima, N. (2020). Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability. *Healthcare informatics research*, 26(1), 3–12. <https://doi.org/10.4258/hir.2020.26.1.3>.

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohshima, N. (2020). Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on Blockchain Technology. *Healthcare informatics research*, 26(4), 265–273. <https://doi.org/10.4258/hir.2020.26.4.265>.

Wattenhofer, R. (2016). *The science of the blockchain*. *Lecture Notes in Computer Science*, 9604, 1-14.

Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A Review of Blockchain-Based Secure Sharing of Healthcare Data. *Applied Sciences*, 12(15), 7912. <https://doi.org/10.3390/app12157912>.

Xiao, Y., Xu, B., Jiang, W., & Wu, Y. (2021). The HealthChain Blockchain for Electronic Health Records: Development Study. *Journal of medical Internet research*, 23(1), e13556. <https://doi.org/10.2196/13556>.

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. *Health informatics journal*, 24(2), 121-128.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 13(4), 352-375.