

Arquitetura *Blockchain* para gestão de dados no contexto do SUS

Blockchain architecture for data management in the context of the Brazilian Unified Health System

Reginalda Santos Silva
<https://orcid.org/0000-0001-5409-1153>

Mestrado em Sistemas e Computação. Universidade Salvador (UNIFACS) – Brasil. reginalda012@gmail.com.

Paulo Caetano da Silva
<https://orcid.org/0000-0002-5038-2460>

PhD em Ciência da Computação (Universidade Federal de Pernambuco – UFPE), Pós-doutorado em Sistemas de Informações Financeiras (Rutgers Business School – USA). Universidade Salvador (UNIFACS) – Brasil. paulocaetano.dasilva@gmail.com.

Daniel José Díaz
<https://orcid.org/0000-0001-5459-1297>

Professor de Tecnologia da Informação. Universidad Nacional de Rosario (UNR) – Argentina. ddiaz@fcecon.unr.edu.ar

RESUMO

Dados de saúde são sensíveis a questões de segurança e privacidade. Normalmente, sistemas de registros médicos são centralizados, o que implica um ponto único de vulnerabilidade. A tecnologia *Blockchain* tem sido utilizada para ampliar a segurança por meio de suas características de descentralização e imutabilidade em um ambiente criptografado. Neste trabalho, propõe-se uma arquitetura baseada em *Blockchain* para armazenamento e intercâmbio de dados em sistemas de Registros Eletrônicos de Saúde (EHR). A pesquisa caracteriza-se como estudo de natureza técnica e exploratória, estruturado em duas etapas: a realização de três revisões sistemáticas da literatura e o desenvolvimento de uma proposta arquitetural. Este artigo apresenta a terceira revisão, sobre arquiteturas de sistemas EHR baseados em *Blockchain*, complementando duas revisões publicadas anteriormente pelos autores, que investigaram o estado da arte das plataformas *Blockchain* e o uso de sistemas de gerenciamento de registros médicos baseados nessa tecnologia. As três revisões fundamentaram a proposição de uma arquitetura conceitual voltada à integridade e à rastreabilidade de dados sensíveis de registros médicos, promovendo a interoperabilidade entre os diversos atores do setor. Como resultado, apresenta-se uma arquitetura conceitual que integra tecnologias destinadas a contribuir para a segurança e a governança dos dados. O estudo também inclui uma análise conceitual da aplicabilidade da proposta no contexto do Sistema Único de Saúde (SUS), discutindo seu potencial para aprimorar a gestão pública, contribuir para a conformidade com as leis de proteção de dados e fortalecer a confiança entre pacientes e profissionais de saúde. Entretanto, a proposta ainda não foi validada empiricamente.

Palavras-chave: *Blockchain*. *E-Health*. registro eletrônico de saúde. EHR. Segurança e privacidade.

ABSTRACT

Health data are sensitive and raise security and privacy concerns. Medical record systems are typically centralized, creating a single point of vulnerability. Blockchain technology has been used to enhance security through its decentralized and immutable characteristics within an encrypted environment. This study proposes a blockchain-based architecture for storing and exchanging data in Electronic Health Record (EHR) systems. The research is technical and exploratory in nature and is structured in two stages: three systematic literature reviews and the development of an architectural proposal. This paper presents the third review, which focuses on blockchain-based EHR system architectures and complements two reviews previously published by the authors, which investigated the state of the art of blockchain platforms and the use of blockchain-based medical record management systems. The three reviews provided the foundation for proposing a conceptual architecture aimed at ensuring the integrity and traceability of sensitive medical record data while promoting interoperability among the various stakeholders in the sector. The resulting conceptual architecture integrates technologies intended to contribute to data security and governance. The study also includes a conceptual analysis of the proposal's applicability within the context of Brazil's Unified Health System (SUS), discussing its potential to improve public management, contribute to compliance with data protection laws, and strengthen trust between patients and healthcare professionals. However, the proposal has not yet been empirically validated.

Keywords: Blockchain. E-Health. electronic health record. EHR. Security and privacy.

Recebido em 05/08/2025. Aprovado em 28/03/2026. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da APA.

<https://doi.org/10.22279/navus.v18.2178>

1 INTRODUÇÃO

A segurança e a privacidade dos dados de pacientes representam um dos maiores desafios na área da saúde. Com a crescente adoção de Registros Eletrônicos de Saúde (EHR), a vulnerabilidade a ataques cibernéticos e o risco de acesso não autorizado a informações sensíveis tornam-se cada vez mais evidentes. Modelos tradicionais de armazenamento centralizado frequentemente apresentam locais únicos de falha, comprometendo a integridade e a confidencialidade dos dados. Este cenário demanda o desenvolvimento de soluções que garantam a imutabilidade, a rastreabilidade e o controle granular de acesso aos dados de saúde, ao mesmo tempo em que promovem a interoperabilidade e a eficiência na troca de informações.

A infraestrutura na área da saúde é formada por distintas organizações, como hospitais, clínicas, postos de saúde e laboratórios. Cada uma dessas entidades gera dados relacionados ao histórico médico dos pacientes, que precisam ser armazenados e compartilhados em um ambiente protegido e confiável (Lavina, 2018). Os dados dos pacientes, por normalmente serem armazenados de forma centralizada, estão sujeitos a riscos de perda e manipulação, que podem comprometer a privacidade e a segurança. A tecnologia *Blockchain* pode mitigar esses riscos em razão de suas características de transparência, descentralização e imutabilidade (Kim *et al.*, 2022).

O uso da tecnologia *Blockchain* pode auxiliar na gestão dos dados médicos entre diferentes organizações de saúde. Por oferecer mecanismos de descentralização, rastreabilidade e integridade, essa tecnologia pode contribuir para a construção de uma base de dados mais segura e acessível (Lavina, 2018). A interoperabilidade entre os sistemas, proporcionada por essa tecnologia, possibilita a realização de transações entre distintas redes *Blockchain*, ou seja, possibilita o compartilhamento dos dados e a realização de transações envolvendo mais de uma organização (Liu *et al.*, 2019).

A motivação deste trabalho reside na vulnerabilidade dos atuais sistemas de saúde, cujos bancos de dados centralizados criam pontos únicos de falha e dependência de autoridades centrais. Como evidenciado por Mohurle e Patil (2017), incidentes globais de ransomware direcionados a instituições de saúde, como o ataque do WannaCry que paralisou hospitais do Serviço Nacional de Saúde (NHS) no Reino Unido e comprometeu o acesso a dados de pacientes, expõem a fragilidade dos Registros Eletrônicos de Saúde (EHR) em termos de privacidade e disponibilidade.

Diante desse cenário, a principal contribuição científica deste estudo consiste na proposição de uma arquitetura baseada em *Blockchain* projetada para uniformizar padrões e garantir a segurança no armazenamento e intercâmbio de dados. Ao utilizar *Smart Contracts* para monitorar o acesso, a arquitetura proposta oferece um modelo de governança capaz de modernizar a gestão no Sistema Único de Saúde (SUS). Essa solução visa converter a atual fragmentação em um ecossistema eficiente e transparente, assegurando a integridade dos registros e a conformidade regulatória, o que pode contribuir para a qualidade dos serviços prestados à população (Han *et al.*, 2022).

Nesse cenário, a tecnologia *Blockchain* apresenta-se como uma solução robusta para o armazenamento e compartilhamento de dados em sistemas EHR. No contexto do Sistema Único de Saúde (SUS), essa tecnologia pode contribuir para a modernização da gestão de registros ao garantir segurança, privacidade e interoperabilidade (Nunes *et al.*, 2021). A aplicação da arquitetura proposta reforça a transparência e a eficiência do sistema público brasileiro, promovendo, em última análise, a conformidade regulatória e uma maior qualidade nos serviços prestados à população.

Este trabalho se concentra, primordialmente, nas seguintes questões:

- QP1: Como a tecnologia *Blockchain* garante a privacidade e a segurança dos dados do paciente em prontuários eletrônicos de saúde (EHR)?

- QP2: Quais plataformas *Blockchain* são empregadas no gerenciamento de prontuários eletrônicos de saúde (EHR)?
- QP3: Existem propostas de aplicação para a integração da *Blockchain* em sistemas de prontuários eletrônicos de saúde (EHR)?
- QP4: Quais modelos de arquitetura de software são abordados nas pesquisas atuais sobre *Blockchain* na área da saúde?
- QP5: Qual padronização é adotada para o armazenamento de prontuários eletrônicos de saúde (EHR) na *Blockchain*?

O objetivo principal deste artigo é apresentar uma proposta conceitual de uma arquitetura para o armazenamento e intercâmbio de Registros Eletrônicos de Saúde (EHR), priorizando a segurança e a privacidade dos dados. A abordagem utiliza um ecossistema tecnológico composto por *Blockchain Hyperledger Fabric*, IPFS, *Zero Trust* e autenticação de dois fatores (2FA). Para isso foram realizadas três revisões da literatura, sendo a primeira avaliou-se comparativamente plataformas *Blockchain*, no que se refere a escalabilidade e consenso resultando na seleção do Hyperledger Fabric (Díaz et al., 2022). A segunda RSL pesquisou-se sobre a aplicação de *Blockchain* no domínio da saúde, com foco em requisitos de segurança e modelos de design (Caetano et al., 2025). Por fim, a terceira RSL é apresentada neste artigo. Espera-se que este trabalho aprofunde o entendimento sobre o potencial e os desafios dessas tecnologias na proteção de dados médicos, contribuindo para o fortalecimento da governança digital e da interoperabilidade segura no setor de saúde.

Nesta introdução, contextualizaram-se os problemas relacionados às questões de segurança de dados médicos que necessitam ser gerenciados. A Seção 2 apresenta a metodologia utilizada para o desenvolvimento deste trabalho; a Seção 3 discute os principais conceitos necessários para o entendimento do que é proposto neste artigo; a Seção 4 discute os trabalhos relacionados; a Seção 5 apresenta a arquitetura proposta e discute seus componentes; a Seção 6 apresenta um exemplo do processo de um *Smart Contract* em um atendimento médico; a Seção 7 discute a solução proposta no contexto do SUS; por fim, a Seção 8 apresenta as principais contribuições, limitações e as observações para pesquisas futuras.

2 METODOLOGIA

Esta pesquisa caracteriza-se como um estudo de natureza exploratória e qualitativa (Gil, 2002; Kitchenham & Charters, 2007), fundamentado em um rigoroso processo de Revisão Sistemática da Literatura (RSL) e no desenvolvimento de uma proposta arquitetural. A escolha metodológica justifica-se pela complexidade da integração de tecnologias emergentes, *Blockchain Hyperledger Fabric*, *Zero Trust*, IPFS e 2FA, no domínio sensível da saúde pública.

Embora o protocolo PRISMA seja amplamente reconhecido em revisões sistemáticas de saúde, esta pesquisa adotou as diretrizes de Kitchenham e Charters (2007), padrão consolidado para a Engenharia de Software e Sistemas de Informação. Esta escolha justifica-se pela necessidade de um protocolo que priorize a extração de requisitos técnicos e atributos arquiteturais de sistemas complexos (*Blockchain*, *Zero Trust*), indo além da síntese de evidências, típica do PRISMA. No entanto, o rigor de transparência foi mantido por meio do detalhamento das *strings*, bases de dados, critérios de inclusão e exclusão apresentados na Tabela 1 e critérios de qualidade apresentados na Tabela 2.

2.1 Processo de busca e critérios de seleção

A busca por artigos para realização da revisão da literatura foi realizada, no período de maio a junho de 2023, nas bases de dados *IEEE Xplore*, *PubMed*, *ScienceDirect* e *ACM Digital Library*. O protocolo de busca automática empregou a seguinte *string* de busca booleana aplicada igualmente em todas as bases de dados: ("*Blockchain*") AND ("*Architecture*" OR "*Software Architecture*") AND ("*E-Health*" OR "*Electronic Medical Record*" OR "*Electronic Medical Records*"). O fluxo de seleção seguiu quatro fases (Figura 1):

1. Identificação: Recuperação inicial de 199 artigos nas bases especificadas.
2. Triagem (Screening): Filtragem por título, resumo e palavras-chave baseada em critérios de inclusão (foco em segurança de EHR) e exclusão (estudos tangenciais sobre PHR ou E-Health genérico).
3. Inclusão e *snowballing*⁵: Aplicação da técnica de *snowballing* para capturar estudos relevantes não identificados na busca automática.
4. Avaliação de qualidade: aplicação dos critérios de qualidade e seleção dos artigos para análise.

Tabela 1

Inclusão e exclusão

Critérios de inclusão	
CI1	Trabalhos publicados no período de 2016 a 2023
CI2	O título deve conter pelo menos uma das palavras-chave do trabalho
CI3	Artigos publicados em congresso ou revista científica
CI4	Título, resumo e texto completo devem estar relacionados ao tema deste trabalho
Critérios de exclusão	
CE1	Trabalho duplicado
CE2	A solução proposta não foi delineada para EHR.
CE3	O texto completo não estava disponível em repositórios

Além dos critérios de seleção preliminares (Tabela 1) é fundamental executar uma avaliação de qualidade. Para isso, utilizou-se os critérios propostos por (Dybå & Dingsøyr, 2008) para investigar a qualidade apontada nos artigos e que atendessem no mínimo 70% das questões mostradas na Tabela 2.

Tabela 2

Critério de qualidade utilizado nesta dissertação.

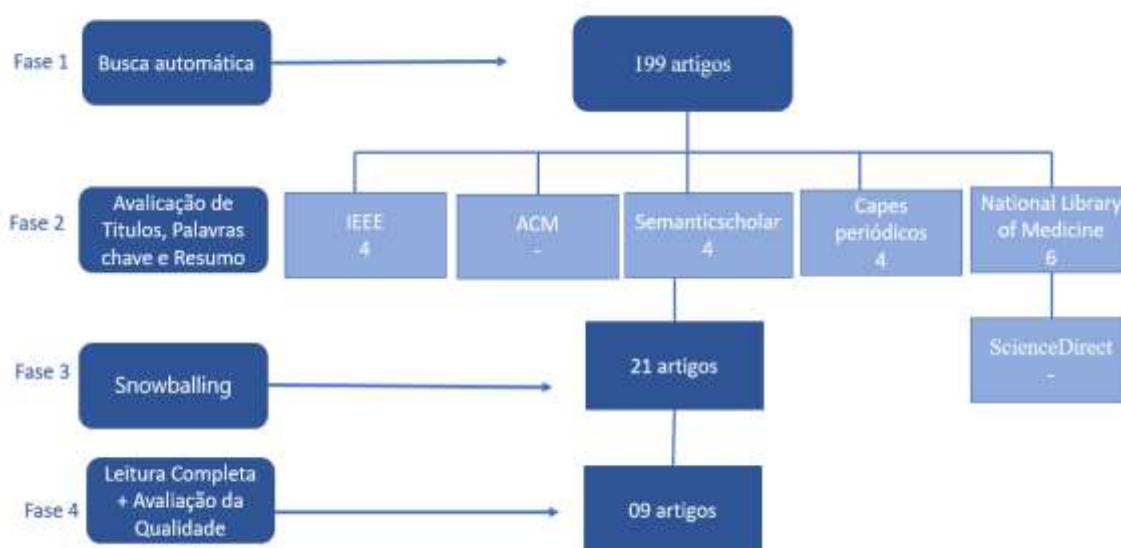
ID	Questionário	Aspectos
CQ1	A solução está claramente detalhada?	Rigidez
CQ2	Existe uma descrição clara do domínio da solução proposta?	Rigidez
CQ3	Os objetivos da pesquisa e a motivação estão claramente definidos?	Rigidez
CQ4	Os autores apresentaram um caso real?	Relevância
CQ5	Existe um processo de avaliação e validação, bem como uma declaração dos resultados alcançados?	Relevância
CQ6	O estudo identificou um cenário para avaliar a aplicação?	Relevância

CQ7	Os autores descrevem os principais problemas que podem ser solucionados com a <i>Blockchain</i> ?	Relevância
CQ8	O estudo tem valor para a pesquisa ou prática?	Credibilidade
CQ9	Os autores citam quais os benefícios foram alcançados com a aplicação da <i>Blockchain</i> nos sistemas EHR?	Credibilidade
CQ10	O estudo descreve que tipos de tecnologias <i>Blockchain</i> foram utilizadas?	Credibilidade

Nesta análise de qualidade, a cada artigo foi atribuída uma nota. Para cada resposta às perguntas do questionário, Tabela 7, foi dada a pontuação 1, quando satisfizesse totalmente a pergunta, nota 0,5 se satisfizesse parcialmente e zero se a resposta não fosse satisfatória. Essa análise foi conduzida por dois pesquisadores individualmente, no caso de pontuações divergentes o terceiro pesquisador participaria da discussão para se chegar ao consenso. Após finalizada essa atividade, os artigos que alcançaram nota mínima 7 foram considerados para ser inserido na revisão da literatura, a partir de leitura crítica dos três pesquisadores. Após a leitura de cada artigo os três pesquisadores se reuniam para discussão consensual. Os critérios de qualidade mais comuns que não foram satisfeitos foram a ausência de aplicações reais da tecnologia *Blockchain*, identificação clara dos problemas a serem solucionados com a tecnologia e a descrição adequada dos resultados alcançados, resultando em uma limitação do estudo.

Ao final das fases de identificação e seleção inicial dos artigos, chegou-se a um total de 21 artigos elegíveis, dos quais 12 foram excluídos por não atingirem a nota 7, restando 9 para análise aprofundada. Esse processo é visualmente representado na Figura 1. Destaca-se que a etapa de eliminação de duplicidade, comum em revisões da literatura, foram conduzidas simultaneamente à Fase 2.

Figura 1
Estratégia de busca e resultados.



Com base na síntese das evidências encontradas nas revisões da literatura, procedeu-se à proposição da arquitetura. Os resultados obtidos nas três RSLs permitiram o mapeamento de desafios

éticos e técnicos, culminando no desenho de um framework que integra a descentralização da *Blockchain* com o rigor do modelo Zero Trust. A avaliação conceitual foi realizada por meio da modelagem e representação teórica do fluxo de atendimento médico por meio de um Smart Contract, examinando, em nível conceitual, a imutabilidade e o controle de acesso aos dados.

Dada a natureza estritamente conceitual deste trabalho, a avaliação fundamentou-se na análise qualitativa da arquitetura frente aos requisitos de segurança e interoperabilidade do SUS. Para ilustrar a aplicabilidade do modelo, descreveu-se um fluxo operacional de troca de informações médicas, evidenciando como a integração entre *Blockchain* e protocolos de autenticação (2FA/Zero Trust) mitigaria os pontos únicos de falha. Essa avaliação teórica sugere que a estrutura proposta é logicamente consistente e apta a guiar o desenvolvimento de protótipos futuros.

3 FUNDAMENTAÇÃO TEÓRICA

Nesta seção, são discutidos os principais conceitos relacionados a este trabalho: *Blockchain*, a plataforma *Hyperledger Fabric* e o *Interplanetary File System* (IPFS), organizados da seguinte forma: a Seção 3.1 apresenta uma visão geral a respeito da tecnologia *Blockchain* e os seus conceitos e termos mais importantes, discutem-se as características fundamentais da *Blockchain*, apresentam-se os protocolos de consenso e descrevem-se os contratos inteligentes; a Seção 3.2 discute a *Blockchain* permissionada *Hyperledger Fabric*; a Seção 3.3 descreve o *Interplanetary File System* (IPFS); a Seção 3.4 discute a arquitetura Zero Trust e a autenticação de dois fatores (2FA).

3.1 BLOCKCHAIN

A tecnologia *Blockchain* transcende sua origem financeira (Nakamoto, 2008) ao oferecer uma infraestrutura descentralizada e imutável, essencial para mitigar o "ponto único de falha" dos sistemas de saúde centralizados. No contexto de Registros Eletrônicos de Saúde (EHR), a literatura aponta que a principal lacuna não é apenas o armazenamento, mas a governança da confiança (Moura et al., 2020).

A cadeia de blocos é formada pelo encadeamento do bloco anterior por uma referência denominada *hash*¹. O bloco *Gênesis* inicia a cadeia de blocos que geram blocos seguintes, estes armazenam dados da transação atual e uma cópia do resumo criptográfico (*hash*) da transação anterior (Berghel, 2017). Enquanto bancos de dados tradicionais dependem de uma autoridade central, o uso de protocolos de consenso e encadeamento por *hashes* criptográficos garante que a integridade dos dados seja verificável por todos os nós² da rede, impedindo alterações retroativas (Zheng et al., 2019; Lavina, 2018; Gomes et al., 2022; Khan et al., 2021).

3.1.1 PROTOCOLO DE CONSENSO

Os protocolos de consenso constituem o cerne operacional das redes *Blockchain*, atuando como mecanismos de tolerância a falhas que asseguram a convergência de todos os nós em torno de um estado único e legítimo da rede. Diferentemente dos sistemas centralizados, onde a validade dos dados emana de uma autoridade única, no ambiente distribuído o consenso garante a existência de uma "única fonte de verdade" (*single source of truth*), essencial para a integridade de registros médicos sensíveis (Erdem et al., 2019). A literatura destaca que esses protocolos permitem que entidades distintas e potencialmente sem relação de confiança prévia (como diferentes hospitais,

1 Secure hash algorithm (*hash*) é o algoritmo usado para proteção criptográfica. É um algoritmo que tem como objetivo principal codificar dados para formar uma cadeia de caracteres exclusiva.

2 Nó: Um nó de rede de computadores pode ser um equipamento de comunicação de dados (DCE), como um modem, hub ou switch, ou um equipamento terminal de dados (DTE), como dois ou mais computadores e impressoras. Em uma rede *Blockchain*, um nó é um computador que faz parte da rede.

clínicas e laboratórios no SUS) ordenem transações de forma cronológica e imutável (Li et al., 2021). Sob a perspectiva da segurança, o consenso mitiga ataques de manipulação de dados: uma vez que um bloco é validado e encadeado, qualquer tentativa de alteração arbitrária invalidaria o *hash* correspondente e todos os blocos subsequentes, tornando a fraude detectável por toda a rede (Berghel, 2017; Khan et al., 2021; Mohurle & Patil, 2017).

3.1.2 Contratos inteligentes

Diferente de repositórios estáticos, a arquitetura proposta utiliza *Smart Contracts* para automatizar a lógica de negócio e o controle de acesso. Segundo Kemmoe et al. (2020), a capacidade de autoexecução desses códigos permite que regras de privacidade e direitos de acesso sejam aplicados sem intervenção humana, garantindo a observabilidade e verificabilidade do prontuário médico. Esta funcionalidade é o que viabiliza a transição de um sistema passivo para um ecossistema de saúde ativo e auditável (Muneeb et al., 2022).

3.2 HYPERLEDGER FABRIC

A escolha pelo *Hyperledger Fabric* justifica-se pela necessidade de conformidade com regulamentações rigorosas como a LGPD no Brasil e a Health Insurance Portability and Accountability Act (HIPAA)³. Ao contrário de redes públicas, o *Hyperledger Fabric* introduz modularidade e o Membership Service Provider (MSP), permitindo que apenas entidades de saúde identificadas participem da rede.

A utilização de canais privados e políticas de endosso mitiga um dilema clássico das redes distribuídas na saúde: a transparência estrutural versus a privacidade do paciente. Cabe ressaltar que a *Blockchain*, em sua essência, fornece integridade e rastreabilidade. A confidencialidade e a proteção do dado em repouso na arquitetura proposta não derivam diretamente do bloco, mas sim da criptografia aplicada aos dados antes de seu envio ao IPFS, combinada a uma gestão de chaves robusta e ao controle estrito de acesso. Essa estrutura permite que o sistema segmente a visibilidade de acordo com a necessidade clínica, protegendo informações sensíveis de nós não autorizados (Shakhbulatov et al., 2020).

3.3 Interplanetary file system (IPFS)

O armazenamento de grandes volumes de dados médicos (por exemplo, exames de imagem) diretamente na *Blockchain* é tecnicamente inviável devido ao custo computacional e problemas de escalabilidade. A arquitetura soluciona essa limitação por meio do Interplanetary File System (IPFS) (Sun et al., 2020).

- Densidade Analítica: O IPFS atua como uma camada de armazenamento off-chain onde o arquivo é identificado pelo seu conteúdo (content-addressing) e não pela localização.
- Relação com a Proposta: Ao registrar apenas o hash do IPFS dentro da *Blockchain*, a arquitetura garante a integridade do exame médico enquanto mantém a eficiência da rede P2P, aliviando a sobrecarga de armazenamento na cadeia principal. Contudo, como o IPFS nativamente não assegura a disponibilidade permanente dos arquivos, a persistência dos dados nesta arquitetura deve ser garantida por meio da adoção de serviços de *pinning* (fixação de arquivos) e pela manutenção de nós consorciados, gerenciados pelas entidades de saúde, dedicados a replicar e reter os registros continuamente (Sun et al., 2020).

3 HIPAA: Disponível em: <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>. Acesso em 13/02/2024.

3.4 ARQUITETURA ZERO TRUST E AUTENTICAÇÃO DE DOIS FATORES (2FA)

A lacuna científica identificada em muitos modelos de EHR baseados em *Blockchain* é a negligência com o "perímetro de acesso". A integração do modelo *Zero Trust Architecture* (ZTA) neste trabalho estabelece que a confiança nunca é implícita, independentemente da localização do usuário na rede (Syed et al., 2022). A proposta da arquitetura contribui ao combinar ZTA com 2FA. A arquitetura proposta cria camadas de defesa em profundidade. Enquanto a *Blockchain* protege o dado "em repouso" e sua rastreabilidade, o binômio ZTA/2FA protege o dado "em trânsito" e o "ponto de acesso", mitigando riscos de credenciais roubadas ou dispositivos comprometidos (Sultana et al., 2020).

No contexto da arquitetura proposta, a escolha do protocolo de consenso é determinante para a escalabilidade do sistema. Enquanto redes públicas utilizam métodos de alto custo energético (por exemplo, *Proof of Work*), redes permissionadas voltadas à saúde, como a delineada neste trabalho, priorizam algoritmos de consenso mais eficientes (como o Raft ou PBFT), que oferecem maior vazão de transações e finalidade imediata, requisitos críticos para o acesso em tempo real a prontuários de emergência no sistema público de saúde.

4 TRABALHOS CORRELATOS

Esta seção apresenta uma revisão da literatura sobre arquiteturas baseadas em *Blockchain* para sistemas EHR. O trabalho proposto por Sultana et al. (2020) apresenta um sistema para combater fragilidades de segurança de dados médicos sensíveis, no qual usa as definições de princípios *Zero Trust Architecture* (ZTA) e a tecnologia *Blockchain Ethereum*, que usa o mecanismo de consenso de Prova de Trabalho (POW) para validar os nós e o armazenamento de dados no *InterPlanetary File System* - IPFS (Sultana et al., 2020).

Shen et al. (2019) propõem um esquema de compartilhamento de dados, denominado *MedChain*. O esquema proposto utiliza dois tipos isolados de redes descentralizadas, uma rede *Blockchain* e uma rede de armazenamento ponto a ponto (P2P). A sua finalidade é oferecer aos pacientes um controle sobre seus dados de saúde e limitar a fragmentação de dados (Shen et al., 2019).

A proposta de Nguyen et al. (2019) é um modelo de compartilhamento de EHRs combinando a *Blockchain* e o IPFS em uma plataforma de nuvem. O objetivo dessa estrutura é fornecer um mecanismo de controle de acesso confiável, baseado unicamente em um *Smart Contract* para gerenciar o acesso do usuário e assegurar que organizações autorizadas (como prestadores de cuidados de saúde) recuperem os EHRs na nuvem, e, desta forma, dificulte o acesso não autorizado aos sistemas de EHRs (Nguyen et al., 2019).

Para solucionar problemas de segurança e privacidade, Uddin et al. (2021) propõem uma arquitetura baseada na *Blockchain Hyperledger Fabric*, uma *Blockchain* de consórcio para o gerenciamento dos sistemas EHRs. No sistema proposto a arquitetura fornece um ambiente seguro, transparente e imutável para armazenar, compartilhar e trocar EHRs entre entidades médicas na saúde (Uddin et al., 2021).

Nishi et al. (2022) propõem uma arquitetura que fornece segurança e gerenciamento dos dados do paciente. O sistema proposto visa proporcionar aos usuários alcançar simultaneamente os dados, preservando o armazenamento seguro de dados, determinando acessos especiais para usuários, além de oferecer a transferência segura de registros médicos de pacientes (Nishi et al., 2022).

Capece e Lorenzi (2020) apresentam a *Medicalchain* um sistema que opera com provedores de saúde para executar registros médicos baseados em *Blockchain*. A vantagem da *Medicalchain* do

ponto de vista médico é que os pacientes têm acesso aos seus prontuários no decorrer de uma consulta de telemedicina, possibilitando que os médicos tenham uma visão mais extensa e investigativa da situação do paciente, tornando-se útil para o paciente e médico (Capece & Lorenzi, 2020).

Xia *et al.* (2017) propõem uma arquitetura para armazenamento e compartilhamento de dados com a aplicação da *Blockchain* denominada *MeDShare*. A arquitetura oferece auditoria e controle de acesso para dados médicos compartilhados de serviços em nuvem. A arquitetura proposta utiliza *Smart Contracts* e mecanismos de controle de acesso para rastrear os dados, assim como anular o acesso a regras e permissões violadas (Xia *et al.*, 2017).

Mani *et al.* (2021) apresentam a gestão de dados de saúde focada no paciente, *Patient-Centric Healthcare Data Management* (PCHDM). O modelo proposto possibilita às partes interessadas confiança na parceria e compartilhamento dos registros de saúde (Mani *et al.*, 2021).

Sonkamble *et al.* (2023) apresentam um sistema de gerenciamento de dados de saúde centrado no paciente *Patient-Centric Healthcare Data Management* (PCHDM) baseada na tecnologia *Blockchain*. A arquitetura proposta engloba o sistema de arquivos interplanetário (IPFS) para o armazenamento externo à *Blockchain* (*off-chain*) e a plataforma *Blockchain Hyperledger Fabric* para o armazenamento na *Blockchain* (*on-chain*), i.e., armazenamento na *Blockchain* (Sonkamble *et al.*, 2023).

Esses trabalhos adotaram o uso da tecnologia *Blockchain* fundamentada em *Smart Contracts* e IPFS. Identificou-se uma quantidade bem limitada de pesquisas que consideraram a utilização da tecnologia *Blockchain* e os princípios de confiança zero. Diante desse contexto, este trabalho apresenta uma arquitetura baseada na tecnologia *Blockchain* que integre os princípios *Zero Trust Architecture* (ZTA) para garantir que nenhum indivíduo dentro ou fora da rede deva ser confiável, a menos que sua identidade tenha sido totalmente investigada; adicionalmente utiliza o IPFS para garantir a escalabilidade dos dados de saúde, em que somente os hashes dos registros de saúde no IPFS são armazenados na *Blockchain*, enquanto os dados médicos são armazenados no IPFS; também é usado o mecanismo criptográfico *Zero-Knowledge Proof* (ZKP) para validar a identidade do usuário e ao mesmo tempo proteger detalhes pessoais.

5 ARQUITETURA PARA SISTEMAS E-HEALTH BASEADA NA *BLOCKCHAIN*

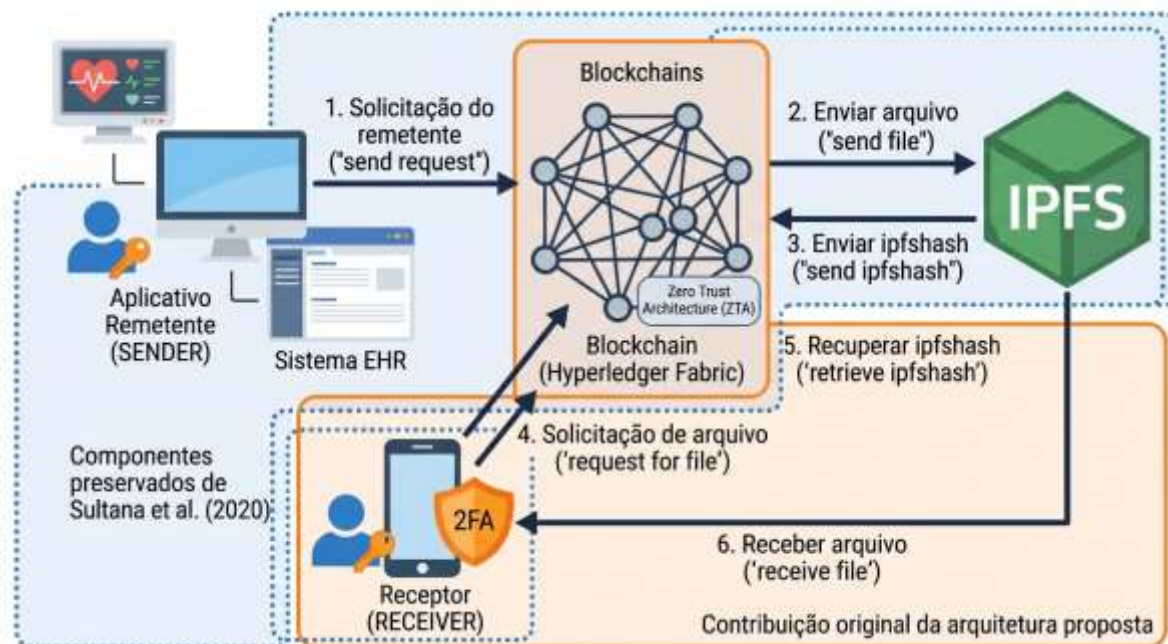
Nesta seção a arquitetura proposta para o ambiente de intercâmbio de dados médicos é mostrada na Figura 2. O modelo arquitetural proposto é baseado naquele desenvolvido por Sultana *et al.* (2020). Em relação ao modelo original, foram preservados o uso do IPFS para armazenamento *off-chain* e o fluxo básico entre os aplicativos remetente e receptor. A contribuição original e as inovações desta arquitetura consistem na substituição da rede Ethereum pela Hyperledger Fabric, garantindo governança permissionada e adequação à privacidade de dados, e na introdução mandatória das camadas de arquitetura Zero Trust (ZTA) e autenticação multifator (2FA) nos aplicativos clientes. De acordo com a análise realizada por Pancari *et al.* (2023) a *Hyperledger Fabric* tem melhor desempenho que a *Blockchain Ethereum* em termos de velocidade de validação de transações e escalabilidade (Pancari *et al.*, 2023). Por outro lado, sendo uma plataforma baseada no conceito de *Blockchain* permissionada, diferencia-se da *Ethereum* pela capacidade de implementar processos intrínsecos de identificação de usuários, sem necessidade de recorrer ao desenvolvimento de *Smart Contracts* para esta função.

As principais características da arquitetura proposta são explicadas a seguir.
Componentes da Arquitetura:

1. **Aplicativo Remetente (Sender):** as duas primeiras camadas de segurança são executadas neste aplicativo. A primeira camada verifica o nome de usuário e as credenciais de login do usuário, que pode ser um médico ou pessoal de saúde autorizado (enfermeiros, gerentes de laboratório e outros). A segunda camada de segurança verifica se o dispositivo no qual as informações são enviadas possui os mais recentes mecanismos de segurança instalados. Isso torna possível garantir que o dispositivo em questão não seja invadido ou comprometido. Uma vez passadas pelas duas camadas de segurança, o aplicativo remetente é responsável por criptografar as informações do prontuário médico usando a chave criptográfica do destinatário final (receptor). Desta forma, ao final de todo o processo apenas o destinatário final da informação poderá decifrar a mensagem com sua chave. A Figura 2 apresenta, no fluxo 1, "send request", o envio da solicitação à rede. É importante ressaltar que a comunicação com o armazenamento externo é mediada por esta camada de aplicação: o aplicativo envia o prontuário criptografado ao IPFS, recebe o hash (*ipfshash*) de volta, e apenas submete o hash na transação enviada à *Blockchain*. Destaca-se que a opção de usar a plataforma *Hyperledger Fabric* no sistema, permite adicionar mais uma camada de segurança vinculada à identidade dos usuários, fornecida pela própria plataforma, ou substituir a camada de segurança do Aplicativo Remetente.
2. **Blockchain (*Hyperledger Fabric*):** uma vez que o Aplicativo Remetente transfere as informações para a *Blockchain*, elas são processadas por um Smart Contract que gerenciará apenas o seu registro na *Blockchain*. Como os *chaincodes* exigem execução determinística, eles não realizam chamadas externas diretas. Toda a informação criptografada do prontuário é armazenada previamente no repositório IPFS pela camada de aplicação. O Smart Contract recebe e registra definitivamente no *ledger* apenas o *hash* criptográfico (*ipfshash*) atrelado à transação. Desta forma, ao final deste processo será registrado o seguinte:
 - a) No repositório IPFS: o arquivo criptografado do prontuário.
 - b) Na *Blockchain*, o código criptografado *hash* (*ipfshash*) gerado pelo repositório IPFS. Esse *hash* é o que será usado para localizar o registro médico armazenado no IPFS e recuperá-lo.

Figura 2

Arquitetura do ecossistema E-Health baseada na Blockchain



Nota. Adaptada de Sultana et al. (2020).

3. **Repositório IPFS: os registros** médicos criptografados pelo Aplicativo Remetente, são armazenados no IPFS pelo *Smart Contract* da *Hyperledger Fabric*. O armazenamento no IPFS é identificado por um código *hash* gerado pelo IPFS e devolvido ao *Smart Contract* que o insere no bloco da transação em execução. O valor desse *hash* corresponde a um endereço de arquivo no IPFS. Isto é ilustrado na Figura 2 pelo fluxo 3 (*send ipfshash*).
4. **Receptor (receiver):** Este aplicativo é utilizado pelo médico ou pessoal de saúde autorizado para consultar as informações do prontuário do paciente. Na arquitetura é proposta uma autenticação de dois fatores da mesma forma que no Aplicativo Remetente. O Receptor é responsável por enviar o pedido de acesso ao prontuário médico, por meio do *Smart Contract* que é executado na plataforma *Hyperledger Fabric*. A Figura 2 apresenta esse processo no fluxo 4 (*request for file*). O Receptor consulta a *Blockchain* por meio de uma chamada ao *Smart Contract* para obter o *ipfshash* associado ao paciente. De posse do *hash*, o próprio Aplicativo Receptor acessa o repositório IPFS para baixar o arquivo de registros médicos (fluxo 5, *retrieve ipfshash*). Em seguida, o prontuário criptografado será decifrado com a chave correspondente, tornando as informações disponíveis para o usuário. A Figura 2 apresenta esse processo no fluxo 6 (*receiver file*), concluindo assim todo o processo de comunicação.

A *Hyperledger Fabric* fornece um bom desempenho quando modelada corretamente. Ao combinar a plataforma com o *Zero Trust* e a 2FA, é possível gerar redes *Blockchain* bastante seguras e confiáveis. Vale ressaltar que ao implementar medidas de segurança como o *Zero Trust* e a 2FA, é necessário analisar o impacto no desempenho da rede. É indispensável obter um equilíbrio entre segurança e desempenho, estabelecendo os parâmetros da rede e optando por tecnologias pertinentes.

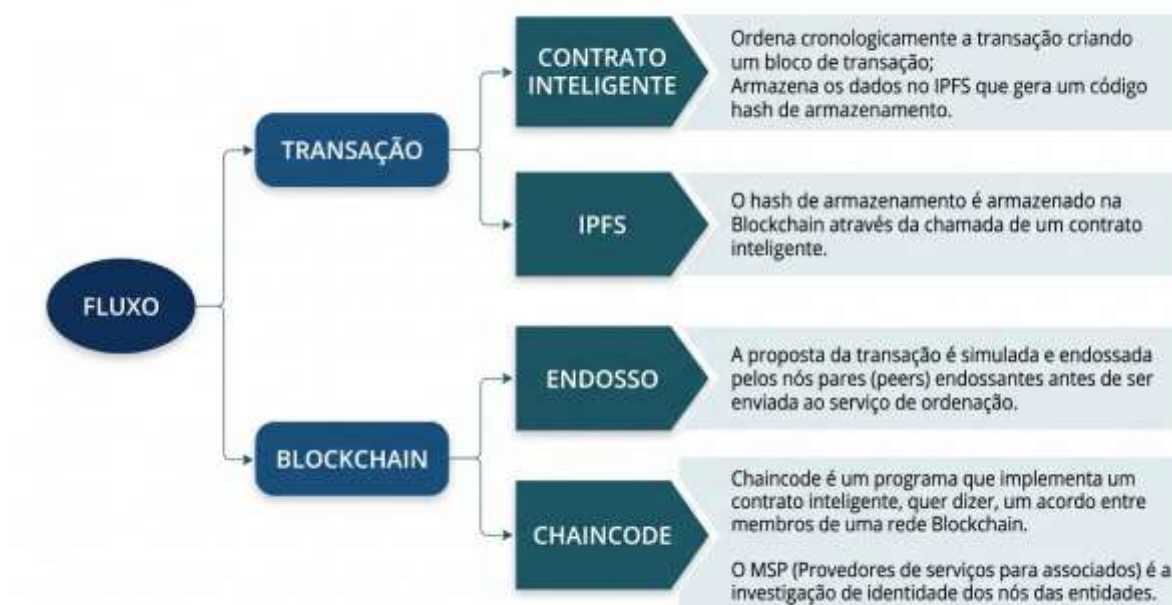
6 EXEMPLO DE USO DA ARQUITETURA PROPOSTA EM UM ATENDIMENTO MÉDICO

Nesta seção é descrito o funcionamento da arquitetura proposta gerenciado por um *Smart Contract* em um atendimento entre o médico e seu paciente em uma organização hospitalar.

No atendimento entre o médico e um paciente é gerado um registro médico (EHR). Esse registro médico pode incluir o histórico médico, diagnóstico, resultados de exames laboratoriais, imagens médicas, cuidados de enfermagem e dados relacionados ao histórico de medicamentos. Cada EHR corresponde a uma transação. As transações são armazenadas em blocos na *Blockchain*. Então, o médico envia uma solicitação da transação EHR para a rede. Ressalta-se que o médico necessita autenticar suas credenciais no sistema de controle de acesso. A rede recebe a solicitação da transação por meio de um *Smart Contract*, ordena-as cronologicamente e cria um bloco de transações. Os dados são armazenados no IPFS, gerando um código *hash* do EHR armazenado (*hash* de armazenamento). O *hash* gerado no IPFS, i.e. endereço de armazenamento, e os metadados da transação (como identificadores pseudonimizados do paciente, especialidade do atendimento, identificador do médico e *timestamps*) são armazenados na *Blockchain* por meio de um *Smart Contract*. Visando a estrita conformidade com a Lei Geral de Proteção de Dados (LGPD) e o princípio da minimização, dados sensíveis e diretamente identificáveis, e.g. como nome, CPF, data de nascimento, endereço e laudos clínicos, são criptografados e mantidos exclusivamente *off-chain* no IPFS, garantindo que o direito à exclusão e a privacidade não entrem em conflito com a imutabilidade da cadeia de blocos.

O fluxo de transação na *Hyperledger Fabric* adota o modelo *Execute-Order-Validate*. Primeiramente, o aplicativo do médico submete uma proposta de transação. Esta proposta é recebida pelos nós pares (*peers*) endossantes, que simulam a execução do *chaincode* e verificam sua validade sem alterar o registro. Após o endosso por um número suficiente de *peers* (conforme as políticas da rede), as respostas são devolvidas ao aplicativo cliente, que as encaminha ao serviço de ordenação (*Ordering Service*). O serviço de ordenação agrupa cronologicamente as transações validadas em um novo bloco. Em seguida, o bloco é distribuído a todos os *peers* da rede, que realizam a validação final (checagem de conflitos) e o *commit* (gravação definitiva) no *ledger*. Durante todo o processo, a autenticação estrutural é gerida pelo *Membership Service Provider* (MSP), que atua como autoridade certificadora para atestar criptograficamente as identidades e permissões das organizações e de seus respectivos nós (Leng et al., 2021). A Figura 3 reflete os elementos essenciais deste ciclo.

Figura 3
Processo da transação



O que torna a *Hyperledger Fabric* diferenciada de outras *Blockchains*, por exemplo, *Ethereum* ou *Bitcoin*, são as políticas de endosso. As políticas de endosso são essenciais para atestar a integridade e a segurança das transações na *Blockchain*. Essas políticas indicam quais organizações ou nós devem endossar uma transação para que ela seja classificada como válida e seja adicionada à *Blockchain*. Nesses sistemas, transações válidas podem ser geradas por algum nó da rede (Gaba et al., 2022).

7 BLOCKCHAIN APLICADA EM SISTEMAS EHR NO CONTEXTO BRASILEIRO (SUS)

A aplicação da tecnologia *Blockchain* no Sistema Único de Saúde (SUS) significa uma evolução na busca por um sistema de saúde mais eficaz, seguro e transparente. A imutabilidade e a descentralização características da *Blockchain* fornecem diversos benefícios que podem transformar a gestão de dados de saúde no Brasil.

Conforme o Ministério da Saúde (MS)⁴, a Rede Nacional de Dados em Saúde (RNDS) é um programa do Governo Federal desenvolvido para a mudança digital da saúde no Brasil. A rede é formada por uma camada de troca de dados, na qual, por meio de um barramento de serviços os dados são intercambiados por várias aplicações de Saúde Digital⁵, como o "Prontuário Eletrônico do Paciente, Sistemas de Gestão Hospitalar e de Laboratórios, portais e aplicações em celular". A execução dessas aplicações de Saúde Digital ocorre em um ambiente heterogêneo. Embora a implementação atual da RNDS ocorra precipuamente por meio da disponibilização de contêineres virtuais em nuvem geridos pelo DATASUS, a aplicação da tecnologia *Blockchain* vem sendo amplamente investigada e proposta na literatura científica como a evolução natural para esse ecossistema, dadas as suas características de segurança descentralizada e imutabilidade. O DATASUS é

4 Ministério da Saúde (MS): Disponível em: <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds>. Acesso em 16 de dezembro de 2024.

5 Saúde Digital: Disponível em: <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds/solucao-tecnologica>. Acesso em 16 de dezembro de 2024.

responsável pela aquisição, instalação e manutenção desses contêineres. O propósito do programa é facilitar a troca de dados entre o ecossistema da Rede de Atenção à Saúde, facilitando a integração e comunicação nos setores públicos e privados, permitindo o compartilhamento dos resultados de exames de Covid-19; dos registros de vacinas administradas contra a Covid-19 e na campanha de multivacinação; bem como dos registros de atendimentos, internações hospitalares e medicamentos dispensados. Estes serviços oferecidos pelo programa são baseados no padrão *Fast Healthcare Interoperability Resources* - Recursos rápidos de interoperabilidade em saúde (FHIR).

Segundo Barbalho et al. (2022), o Conecte SUS é um exemplo de aprimoramento da integração de dados usados pelos usuários (cidadão/paciente). O Conecte SUS foi desenvolvido objetivando centralizar as informações, possibilitando o acesso à saúde, a continuidade do cuidado, a transparência e a segurança dos dados para cidadãos, profissionais de saúde e gestores. O Conecte SUS é uma plataforma nacional de saúde baseada em registros de assistência médica no SUS e serviços privados (por exemplo, exames, consultas, vacinas e dispensação de medicamentos) (Barbalho et al., 2022).

Nesse cenário, no Brasil existem diversos problemas relacionados à interoperabilidade, como a quantidade de sistemas de informação em saúde desatualizados. Uma situação crítica é o caso do Sistema de Informação de Agravos de Notificação (SINAN) que não está à disposição da RNDS, como também não é integrado aos sistemas desenvolvidos pelo Ministério da Saúde (MS) brasileiro. Nesse sentido, essa situação torna-se grave, pois o atual modelo para o Sistema Integrado de Saúde (SIS), constantemente não identifica o estado da infraestrutura tecnológica. Outro fator é a constante mudança política do país. Essa mudança pode levar à suspensão de políticas e programas que obtiveram sucesso, por exemplo, a mudança na forma como os dados são coletados. Além disso, existe a necessidade de empregos estáveis para profissionais de tecnologia da informação (Barbalho et al., 2022).

Um sistema descentralizado de dados médicos adaptável à Lei Geral de Proteção de Dados (LGPD) com a aplicação da tecnologia *Blockchain*, repositório externo IPFS e o uso da criptografia *Pretty Good Privacy* (OpenPGP) que funciona por meio de chaves assimétricas foi proposto (Brasil, 2018; Nunes et al., 2021). Porém, esse trabalho trata-se de um estudo relacionado ao modelo tecnológico vigente do SUS, no qual é analisado o banco de dados do sistema de saúde brasileiro. Os autores apresentam uma proposta, mas sem a discussão sobre a arquitetura a ser implementada. Diante desse contexto, o diferencial do ecossistema proposto neste trabalho é o uso da plataforma *Hyperledger Fabric* com um sistema para o gerenciamento do controle de acesso e dos dados médicos, armazenando os registros de saúde no IPFS para acesso por todas as partes envolvidas (por exemplo, pacientes, profissionais de saúde, clínicas, hospitais); o papel do IPFS na arquitetura é garantir a escalabilidade dos dados de saúde, em que somente os hashes dos registros de saúde são armazenados na *Blockchain*, enquanto os dados são armazenados no IPFS. Essas tecnologias tornariam segura a integração de dados e sistemas para o SUS, o que pode favorecer a proteção e a integração das informações da população atendida.

O atendimento do SUS executa um grande volume de dados referentes ao atendimento dos pacientes em hospitais, clínicas, postos de saúde e farmácias. Segundo o Ministério da Saúde⁶ o “SUS é o único sistema de saúde pública do mundo que atende mais de 190 milhões de pessoas”. Em 2022, foram realizados pelo SUS 12,5 milhões de procedimentos hospitalares e quatro bilhões de atendimentos ambulatoriais. Devido a esse grande volume de dados é necessária a adoção de um

6 Ministério da Saúde: Disponível em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2021/setembro/maior-sistema-publico-de-saude-do-mundo-sus-completa-31-anos>. Acesso em 17 de dezembro de 2024.

repositório externo como o IPFS para armazenar os dados, pois esse alto volume de dados impacta na escalabilidade da *Blockchain*. Com isso, os dados do prontuário seriam armazenados no repositório IPFS, enquanto o resumo criptográfico (*hash* de armazenamento) é registrado na *Blockchain* por um *Smart Contract* que gerenciará o registro na *Blockchain* e o armazenamento no IPFS. Iniciativas recentes no âmbito estadual, a exemplo dos estudos e projetos vinculados à Rede Mineira de Dados em Saúde (RDS-MG), demonstram o esforço contínuo de instituições acadêmicas e governamentais para viabilizar prontuários unificados embasados na tecnologia *Blockchain* no Brasil⁷. Diante desse contexto, a aplicação da tecnologia *Blockchain* pode ser uma solução viável de segurança para o armazenamento e compartilhamento dos dados no SUS.

A fundamentação desta arquitetura considera as particularidades do cenário brasileiro, especialmente as diretrizes da Rede Nacional de Dados de Saúde (RNDS) e a estratégia de Saúde Digital (MS, 2020)⁸. As revisões sistemáticas integraram estudos nacionais que discutem os desafios de governança e a fragmentação de dados no Sistema Único de Saúde (SUS), identificando na tecnologia *Blockchain* uma solução para o barramento de serviços de interoperabilidade conforme os estudos do Ministério da Saúde (2020) e as diretrizes de Novoa (2019).

A avaliação conceitual da arquitetura foi realizada por meio da análise de um cenário de uso que simula o fluxo de intercâmbio de dados entre uma Unidade Básica de Saúde (UBS) e um hospital de alta complexidade. O mapeamento lógico deste cenário segue as seguintes premissas e etapas operacionais:

- Geração e Criptografia: Um paciente é atendido na UBS, onde seus dados clínicos (laudos preliminares) são gerados. O Aplicativo Remetente da UBS autentica o médico via 2FA, verifica a conformidade do dispositivo (ZTA) e criptografa o arquivo do prontuário.
- Armazenamento e Hashing: O arquivo criptografado é enviado ao IPFS, que retorna um hash único de localização (*ipfshash*). O *Smart Contract* registra apenas este hash e os metadados pseudonimizados na *Blockchain* (*Hyperledger Fabric*), garantindo a conformidade com a LGPD.
- Solicitação de Acesso: Semanas depois, o paciente sofre um agravo e dá entrada no hospital de alta complexidade. O médico plantonista solicita acesso ao histórico da UBS. A requisição passa pelos mesmos protocolos ZTA e 2FA do Aplicativo Receptor.
- Recuperação e Decifragem: O *Smart Contract* valida as credenciais e permissões do hospital. Sendo autorizado, o aplicativo recebe o *ipfshash*, busca o arquivo no IPFS e o decifra localmente para leitura do plantonista.

Esse mapeamento lógico ilustrou como a arquitetura proposta se alinha aos padrões de segurança exigidos pela RNDS, oferecendo um *framework* robusto para a modernização da gestão de dados públicos e a garantia da soberania do paciente sobre suas informações médicas.

8 CONCLUSÃO

Este artigo apresentou uma proposta de arquitetura conceitual voltada ao fortalecimento da segurança e privacidade em sistemas de Registros Eletrônicos de Saúde (EHR). Diante da vulnerabilidade crítica dos *modelos centralizados*, a solução proposta integrou de forma articulada a *Blockchain Hyperledger Fabric*, o IPFS e a arquitetura *Zero Trust* (ZTA) com autenticação multifator (2FA), estabelecendo uma arquitetura robusta para a governança de dados sensíveis.

7 Disponível em: <https://www.unirio.br/comunicacaosocial/isc/minas-gerais-cria-o-primeiro-prontuario-unificado-com-blockchain-para-atendimentos-no-sus>. Acesso em 24 de janeiro de 2025.

8 Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 31 de março de 2026.

Para consolidar os achados desta pesquisa, a Tabela 3 sintetiza as respostas para as questões de pesquisa (QP1 a QP5) levantadas na introdução, correlacionando-as com as evidências extraídas da literatura e o design da arquitetura proposta.

Tabela 3

Matriz de Resultados das Questões de Pesquisa

Questão de Pesquisa (QP)	Evidência Analisada na Literatura	Resposta Alcançada pela Pesquisa e Arquitetura
QP1: Como a tecnologia <i>Blockchain</i> garante a privacidade e a segurança dos dados do paciente em prontuários eletrônicos de saúde (EHR)?	A literatura demonstra que redes descentralizadas evitam pontos únicos de falha. A segurança baseia-se em criptografia e protocolos de consenso (Moura et al., 2020; Zheng et al., 2019).	A segurança é garantida pela imutabilidade e rastreabilidade dos <i>hashes</i> na <i>Blockchain</i> . A privacidade é assegurada pelo armazenamento dos dados sensíveis fora da rede (off-chain no IPFS), combinados com o controle rigoroso de acesso via <i>Zero Trust Architecture</i> (ZTA) e 2FA.
QP2: Quais plataformas <i>Blockchain</i> são empregadas no gerenciamento de prontuários eletrônicos de saúde (EHR)?	Trabalhos correlatos apontam o uso de redes públicas (Ethereum) (Sultana et al., 2020) e permissionadas (Hyperledger Fabric) (Uddin et al., 2021; Sonkamble et al., 2023).	Plataformas permissionadas, especificamente a Hyperledger Fabric, são mais adequadas por possuírem Membership Service Provider (MSP) para identificação de usuários, canais privados e maior escalabilidade em transações de saúde.
QP3: Existem propostas de aplicação para a integração da <i>Blockchain</i> em sistemas de prontuários eletrônicos de saúde (EHR)?	Sim, autores como Nguyen et al. (2019) e Capece & Lorenzi (2020) propuseram modelos com IPFS, nuvem e Smart Contracts, mas muitos negligenciam o perímetro de acesso.	Existem diversas propostas em desenvolvimento. Esta pesquisa avança ao propor um modelo de integração que combina a Hyperledger Fabric com ZTA e 2FA, cobrindo a lacuna de controle no perímetro de acesso às informações médicas.
QP4: Quais modelos de arquitetura de software são abordados nas pesquisas atuais sobre <i>Blockchain</i> na área da saúde?	Os estudos concentram-se no uso de redes descentralizadas isoladas (Shen et al., 2019) e arquiteturas híbridas on-chain/off-chain gerenciadas por Smart Contracts.	O modelo adotado e validado teoricamente por esta pesquisa é a arquitetura híbrida. O gerenciamento do acesso (log, regras de negócio e identificadores) ocorre on-chain (Hyperledger), enquanto os arquivos pesados dos EHRs ficam off-chain (IPFS).
QP5: Qual padronização é adotada para o armazenamento de prontuários eletrônicos de saúde (EHR) na	O uso de identificadores criptográficos (hashes) é o padrão técnico principal. No Brasil, o SUS fomenta padrões de interoperabilidade em	A padronização ocorre pelo armazenamento estrito do hash do IPFS na <i>Blockchain</i> , protegendo os dados em repouso e viabilizando a integração futura com padrões

Questão de Pesquisa (QP)	Evidência Analisada na Literatura	Resposta Alcançada pela Pesquisa e Arquitetura
<i>Blockchain?</i>	saúde digital (Ministério da Saúde, 2020).	semânticos de saúde exigidos pela RNDS (como o HL7 FHIR).

A discussão evidenciou a alta relevância dessa arquitetura para o Sistema Único de Saúde (SUS) e sua conformidade teórica com a Rede Nacional de Dados de Saúde (RNDS). Por meio de uma avaliação conceitual do cenário de uso, considerou-se que a descentralização do registro e o armazenamento *off-chain* via IPFS oferecem uma resposta escalável à heterogeneidade do sistema público brasileiro. O modelo apresenta potencial para mitigar riscos de manipulação e acessos não autorizados, promovendo a soberania do paciente e a confiança mútua entre os atores do ecossistema de saúde digital.

Em suma, a convergência dessas tecnologias representa um avanço propositivo na proteção de dados de saúde. Embora o estudo apresente natureza estritamente conceitual, ele oferece subsídios para o desenvolvimento de infraestruturas mais resilientes, alinhadas às exigências da LGPD e às crescentes demandas por integridade da informação em redes complexas.

8.1 Limitações e trabalhos futuros

Como limitação principal, destaca-se a ausência de validação empírica por meio de implementação em ambiente de produção, o que restringe a análise de métricas de desempenho em tempo real. Visando expandir as contribuições deste estudo, elencam-se as seguintes sugestões para trabalhos futuros:

- Desenvolvimento de Prova de Conceito (PoC): Implementar a arquitetura em ambiente controlado utilizando a *Blockchain Hyperledger Fabric* para mensurar a latência e a vazão de transações sob carga;
- Análise de Desempenho: Investigar o impacto computacional da sobreposição das camadas de segurança (ZTA e 2FA) no tempo de resposta das consultas aos EHRs;
- Integração de Padrões: Avaliar a interoperabilidade técnica da arquitetura com o padrão HL7 FHIR, visando a integração nativa com o barramento da RNDS;
- Estudos de Usabilidade: Realizar testes com profissionais de saúde para avaliar a percepção de eficiência e segurança do fluxo de trabalho proposto.

REFERÊNCIAS

- Barbalho, I. M. P., Fernandes, F., Barros, D. M. S., Paiva, J. C., Henriques, J., Moraes, A. H. F., Coutinho, K. D., Coelho Neto, G. C., Chioro, A., & Valentim, R. A. M. (2022). Electronic health records in Brazil: Prospects and technological challenges. *Frontiers in Public Health*, 10. <https://doi.org/10.3389/fpubh.2022.963841>
- Berghel, H. (2017). Equifax and the Latest Round of Identity Theft Roulette. *Computer*, 50(12), 72–76. <https://doi.org/10.1109/MC.2017.4451227>
- Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União.
- Caetano da Silva, P., Santos Silva, R., & Diaz, D. J. (2025). Managing medical records with blockchain. *Contabilidad Y Negocios*, 10–47. <https://doi.org/10.18800/contabilidad.2025ESP.001>
- Capece, G., & Lorenzi, F. (2020). Blockchain and Healthcare: Opportunities and Prospects for the EHR. *Sustainability*, 12(22), 9693. <https://doi.org/10.3390/su12229693>
- Diaz, D. J., Santos Silva, R., & Caetano da Silva, P. (2022). Plataformas blockchains: Uma visão comparativa. *19th CONTECSI International Conference on Information Systems and Technology Management*. <https://doi.org/10.5748/19CONTECSI/PSE/ITM/7003>
- Dybå, T., & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology*, 50(9–10), 833–859. <https://doi.org/10.1016/j.infsof.2008.01.006>
- Erdem, A., Yıldırım, S. Ö., & Angin, P. (2019). Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art. In *Security, Privacy and Trust in the IoT Environment* (pp. 97–122). Springer. https://doi.org/10.1007/978-3-030-18075-1_6
- Gaba, P., Raw, R. S., Mohammed, M. A., Nedoma, J., & Martinek, R. (2022). Impact of Block Data Components on the Performance of Blockchain-Based VANET Implemented on Hyperledger Fabric. *IEEE Access*, 10, 71003–71018. <https://doi.org/10.1109/ACCESS.2022.3188296>
- Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (4ª ed.). Atlas.
- Gomes, N. B. P., Franco, S. de C., & Salvador, L. do N. (2022). ONTOVID - Uma Abordagem para Construção de Grafos de Conhecimento Semântico com Enfoque em Notificações e Óbitos Relacionados ao Novo Coronavírus (COVID-19). *Anais Do XXII Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2022)*, 425–436. <https://doi.org/10.5753/sbcas.2022.222723>
- Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, 19(23), 15577. <https://doi.org/10.3390/ijerph192315577>
- Kemmoe, V. Y., Stone, W., Kim, J., Kim, D., & Son, J. (2020). Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access*, 8, 117782–117801. <https://doi.org/10.1109/ACCESS.2020.3005020>
- Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, 11(20), 9372. <https://doi.org/10.3390/app11209372>

- Kim, J. W., Kim, S. J., Cha, W. C., & Kim, T. (2022). A Blockchain-Applied Personal Health Record Application: Development and User Experience. *Applied Sciences*, 12(4), 1847. <https://doi.org/10.3390/app12041847>
- Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Keele University and Lincoln University.
- Lavina, M. E. (2018). Validação do uso da tecnologia Blockchain para o tráfego seguro de dados na área da saúde. *Unisul*, 1(2), 1–16.
- Leng, Z., Tan, Z., & Wang, K. (2021). Application of Hyperledger in the Hospital Information Systems: A Survey. *IEEE Access*, 9, 128965–128987. <https://doi.org/10.1109/ACCESS.2021.3112608>
- Li, D., Han, D., Weng, T. H., Zheng, Z., Li, H., Liu, H., Castiglione, A., & Li, K. C. (2021). Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. *Soft Computing*, 26(9), 4423–4440. <https://doi.org/10.1007/s00500-021-06496-5>
- Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE Access*, 7, 118943–118953. <https://doi.org/10.1109/ACCESS.2019.2937685>
- Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics*, 10(23), 3003. <https://doi.org/10.3390/electronics10233003>
- Ministério da Saúde. (2020). *Estratégia de Saúde Digital para o Brasil 2020-2028*. Ministério da Saúde do Brasil.
- Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5). <https://doi.org/10.26483/IJARCS.V8I5.4021>
- Moura, L. M. F. de, Brauner, D. F., & Janissek-Muniz, R. (2020). Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática. *Revista de Administração Contemporânea*, 24(3), 259–274. <https://doi.org/10.1590/1982-7849rac2020190171>
- Muneeb, M., Raza, Z., Haq, I. U., & Shafiq, O. (2022). SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management. *IEEE Access*, 10, 23687–23699. <https://doi.org/10.1109/ACCESS.2021.3135562>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamoto Institute.
- Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access*, 7, 66792–66806. <https://doi.org/10.1109/ACCESS.2019.2917555>
- Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., & Saini, D. K. (2022). Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. *Journal of Sensors*, 2022, 1–22. <https://doi.org/10.1155/2022/7299185>
- Novoa, C. G. (2019). *Fundamentos de gestão e informática em saúde*. ResearchGate. ISBN 978-85-62377-41-9.

Nunes, C. C., Ma, S., & Filho, M. S. T. (2021). Armazenamento descentralizado no Sistema Único de Saúde brasileiro (SUS) usando Interplanetary File System (IPFS) e Blockchain. *Revista de Direito*, 13(01), 01–25. <https://doi.org/10.32361/2021130111695>

Pancari, S., Rashid, A., Zheng, J., Patel, S., Wang, Y., & Fu, J. (2023). A Systematic Comparison between the Ethereum and Hyperledger Fabric Blockchain Platforms for Attribute-Based Access Control in Smart Home IoT Environments. *Sensors*, 23(16), 7046. <https://doi.org/10.3390/s23167046>

Shakhbulatov, D., Medina, J., Dong, Z., & Rojas-Cessa, R. (2020). How Blockchain Enhances Supply Chain Management: A Survey. *IEEE Open Journal of the Computer Society*, 1, 230–249. <https://doi.org/10.1109/OJCS.2020.3025313>

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. *IEEE Access*, 7, 120234–120245. <https://doi.org/10.1109/ACCESS.2019.2952942>

Sonkamble, R. G., Bongale, A. M., Phansalkar, S., Sharma, A., & Rajput, S. (2023). Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics*, 12(4), 1015. <https://doi.org/10.3390/electronics12041015>

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, 20(1), 256. <https://doi.org/10.1186/s12911-020-01275-y>

Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. *IEEE Access*, 8, 59389–59401. <https://doi.org/10.1109/ACCESS.2020.2982964>

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, 10, 57143–57179. <https://doi.org/10.1109/ACCESS.2022.3174679>

Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. *Computers, Materials & Continua*, 68(2), 2377–2397. <https://doi.org/10.32604/cmc.2021.015354>

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access*, 5, 14757–14767. <https://doi.org/10.1109/ACCESS.2017.2730843>

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). NutBaaS: A Blockchain-as-a-Service Platform. *IEEE Access*, 7, 134422–134433. <https://doi.org/10.1109/ACCESS.2019.2941905>