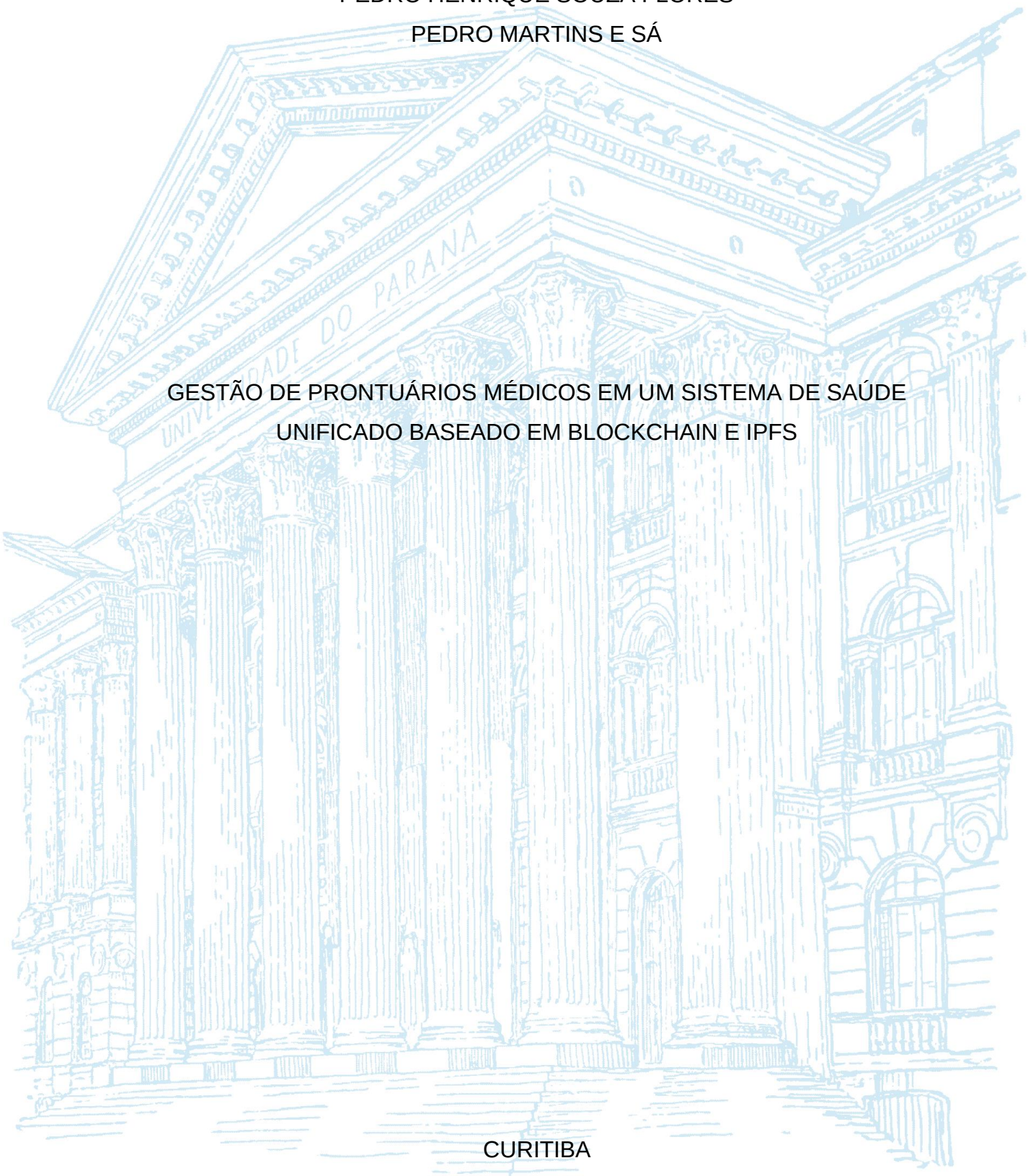
UNIVERSIDADE FEDERAL DO PARANÁ

PEDRO HENRIQUE SOUZA FLORES
PEDRO MARTINS E SÁ



GESTÃO DE PRONTUÁRIOS MÉDICOS EM UM SISTEMA DE SAÚDE UNIFICADO BASEADO EM BLOCKCHAIN E IPFS

CURITIBA
2023

PEDRO HENRIQUE SOUZA FLORES
PEDRO MARTINS E SÁ

GESTÃO DE PRONTUÁRIOS MÉDICOS EM UM SISTEMA DE SAÚDE UNIFICADO BASEADO EM BLOCKCHAIN E IPFS

Trabalho apresentado como requisito parcial à conclusão do Curso de Bacharelado em Ciência da Computação, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*

Orientador: Prof. Dr. Luiz Carlos Pessoa Albini

CURITIBA
2023

TERMO DE APROVAÇÃO

PEDRO HENRIQUE SOUZA FLORES
PEDRO MARTINS E SÁ

GESTÃO DE PRONTUÁRIOS MÉDICOS EM UM SISTEMA DE SAÚDE UNIFICADO BASEADO EM BLOCKCHAIN E IPFS

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

_____
Prof(a). Dr(a)./Msc. _____
Orientador(a) – Departamento _____, INSTITUIÇÃO

_____
Prof(a). Dr(a)./Msc. _____
Departamento _____, INSTITUIÇÃO

_____
Prof(a). Dr(a)./Msc. _____
Departamento _____, INSTITUIÇÃO

Curitiba, __ de _____ de 2023.

Mantenha essa página em branco para inclusão do termo/folha de aprovação assinado e digitalizado.

AGRADECIMENTOS

Eu, Pedro Flores, agradeço aos meus familiares pelo esforço e incentivo a trilhar um caminho nos estudos. Aos meus amigos pela companhia nos longos anos de faculdade e aos professores que contribuíram para minha formação.

Eu, Pedro e Sá, agradeço aos meus pais, Jorge e Vânia, por me darem todo o apoio e me incentivarem a buscar o conhecimento e valorizar a educação; à Lauri, por estar ao meu lado desde o Ensino Médio sendo minha companheira e parceira de vida e aos meus amigos que acompanharam minha jornada até aqui.

"To be young, gifted and black
Oh what a lovely precious dream"

(NINA SIMONE)

RESUMO

As redes de atenção à saúde têm como princípio a integralidade, visando atender as necessidades médicas da população desde o nível básico até o complexo. Para tanto, é necessária uma gestão eficiente de informações do paciente, a fim de traçar a sua jornada no sistema de saúde. A Blockchain surgiu como uma maneira descentralizada de realizar transações bancárias, ou seja, sem a necessidade de um agente entre as partes; por meio da moeda digital Bitcoin. Conforme os avanços nos estudos do tema, outras implementações dela surgiram, o que trouxe maior flexibilidade para o uso da tecnologia. Uma delas foi o Ethereum, que permite a criação de contratos inteligentes para a automatização da rede, auxiliando no controle de acesso aos dados do paciente e no compartilhamento seguro de informações médicas entre diversas instituições através da integração com o Interplanetary File System (IPFS) para o armazenamento dos dados médicos. Além disso, a solução garante os pilares da segurança da informação com uma performance satisfatória. Ao final, a fim de aumentar a escalabilidade do sistema, pontua-se melhorias para trabalhos futuros, como o uso de cache e paginação para melhor eficiência no acesso aos dados.

Palavras-chave: Blockchain. Prontuários. Ethereum. Contrato Inteligente.

ABSTRACT

Healthcare networks have integrity as a principle, aiming to attend to the medical needs of the population from the basic to the complex level. This requires efficient management of patient information to trace the patient's journey through the healthcare system. Blockchain emerged as a decentralized way to perform banking transactions, without the need for an agent between the parts; through the digital currency Bitcoin. With advances in the studies of the theme, other implementations of it emerged, which brought more flexibility to the use of the technology. One of these was Ethereum, which allows the creation of smart contracts for in the network automation, helping with control access of patient data and securely share medical information among various healthcare institutions through integration with the Interplanetary File System (IPFS) for the storage the medical data. Furthermore, the solution ensures guarantees the pillars of information security with satisfactory performance. In order to increase the scalability of the system, improvements for future work are pointed out in the conclusion of this research, such as the use of caching and paging for better efficiency in data access.

Keywords: Blockchain. Medical Records. Ethereum. Smart Contracts.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AES	- Advanced Encryption Standard
API	- Application Programming Interface
CID	- Content Identifier
CRPAD	- Comissão Permanente de Revisão de Prontuários e Avaliação de Documento
DAG	- Merkle Directed Acyclic Graphs
DHT	- Distributed Hash Table
ETH	- Ether
EVM	- Ethereum Virtual Machine
HTTPS	- Hyper Text Transfer Protocol Secure
IOT	- Internet of Things
IPFS	- InterPlanetary File System
LGPD	- Lei Geral de Proteção de Dados
P2P	- Peer-to-Peer
PEP	- Prontuários Eletrônicos do Paciente
PoS	- Proof of Stack
PoW	- Proof of Work
REST	- Representational State Transfer
SI	- Sistemas de Informação
SPA	- Single Page Application
UML	- Unified Modeling Language

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTO E PROBLEMA

No tangente às redes de atenção à saúde, o conhecimento e gestão de informações de pacientes é um fator crítico para traçar sua jornada dentro do sistema. O principal objeto de registro deste percurso é o prontuário médico do paciente, o qual consiste em um documento único, gerado por um profissional da saúde, que reúne informações sobre histórico familiar, anamneses, descrição e evolução de sintomas e exames (CONSELHO FEDERAL DE MEDICINA, 1999).

As principais dificuldades enfrentadas no gerenciamento dos prontuários (tais quais ilegibilidade, confidenciabilidade, segurança da informação e duplicidade de dados) advêm do uso de documentos manuais ou da falta de interoperabilidade dos Sistemas de Informação (SI) utilizados nas redes de saúde (MASSAD *et al.,* 2003). Devido a tais desafios apresentados na gestão de prontuários, sejam eles manuais ou eletrônicos, muitas instituições de saúde possuem uma comissão permanente de revisão de prontuários e avaliação de documentos (CRPAD) a fim de unicamente cumprir as normas estabelecidas pelos conselhos de medicina (XAVIER, 2022). Além disso, estas instituições utilizam bases de dados centralizadas, contendo informações sensíveis dos pacientes, o que exclui a possibilidade de fornecer intercomunicação na rede de saúde, dar autonomia para o usuário gerir seus próprios documentos e deixando o sistema mais suscetível a ataques. Em 2021, aproximadamente 24,3 milhões de imagens médicas foram vazadas em 50 países (Li *et al.,* 2021), reforçando a fragilidade dos sistemas médicos ao redor do mundo.

Os prontuários possuem informações de caráter pessoal. Sendo assim, seu acesso é restrito ao paciente, ao seu responsável legal, às instituições e aos profissionais da área de saúde que necessitam do documento para obter uma visão completa do paciente. Segundo a Lei Geral de Proteção de Dados (LGPD), fica a caráter das instituições de saúde garantir respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem de uma pessoa, além de prover livre acesso a tais informações (BRASIL, 2023). Para tanto, fica evidente a necessidade de uma tecnologia que esteja em sincronia com as necessidades atuais da sociedade.

Com base no exposto, a presente monografia explora o uso de uma solução baseada em *Blockchain* e *Smart Contracts* visando aprimorar a gestão de informações

dentro do sistema de saúde. Contrapondo-se a problemas atuais, como bases de dados centralizadas trazendo risco à proteção de dados, dificuldade de cruzamento de dados em prontuários eletrônicos de formatos não padronizados, duplicidade de exames por falta de interoperabilidade de dados e falta de autonomia do paciente na gestão dos próprios dados.

1.2 OBJETIVOS

1.2.1 Objetivo geral

Objetiva-se elaborar uma abordagem para a integração das informações de prontuários médicos entre as diversas redes de saúde. Para isso, durante a pesquisa visamos criar uma rede descentralizada *Blockchain* baseada em *Ethereum*, na qual serão produzidos contratos inteligentes para automatização, autenticação e armazenamento das referências dos prontuários médicos no sistema. Será desenvolvida uma *Application Programming Interface* (API) que fará a integração entre a *Blockchain*, os contratos inteligentes e os arquivos no IPFS, salvando, recuperando e dando acesso aos registros que serão disponibilizados ao usuário final, seja ele médico ou paciente. Através dela os hospitais poderão fazer a integração da sua interface com a rede completa de saúde.

1.2.2 Objetivos específicos

a) Desenvolver um contrato inteligente para gerenciamento dos médicos e pacientes do sistema, bem como salvar as referências dos arquivos no IPFS;
b) Armazenar os dados no IPFS garantindo a recuperação com segurança e rapidez;
c) Criar uma comunicação padronizada entre o contrato inteligente na *Blockchain*, o IPFS e o sistema consumidor;
d) Desenvolver uma API *proxy* para a integração dos sistemas do hospital com a rede e garantir o gerenciamento das informações;

1.3 JUSTIFICATIVA

Conforme supracitado na seção de contextualização do problema, fica evidente a necessidade de superar as adversidades mencionadas utilizando a tecnologia como suporte. A área da saúde é um dos pilares fundamentais da sociedade, logo qualquer atuação nela precisa estar alinhada com as práticas e exigências governamentais. Segundo o Ministério da Saúde, dois dos pilares do Plano de Ação de Saúde Digital para o Brasil entre os anos de 2020 e 2028 são a informatização dos 3 Níveis de Atenção, buscando incentivar a utilização de Prontuários Eletrônicos do Paciente (PEP) para a gestão hospitalar integradora e a criação de um Ambiente de Interconectividade que pretende impulsionar o uso da Rede Nacional de Dados em Saúde em tecnologias postas em prática (BRASIL, Ministério da Saúde, 2020). Complementando o raciocínio, Patrício *et al.* (2011, p. 124) descrevem em seu estudo as vantagens na utilização de PEP:

> Percebe-se, portanto, que inúmeras são as vantagens e possibilidades advindas da utilização do PEP, tais como: acesso mais veloz ao histórico de saúde e às intervenções às quais o paciente foi submetido; disponibilidade remota; uso simultâneo por diversos serviços e profissionais de saúde; flexibilidade do layout dos dados; legibilidade absoluta das informações; eliminação da redundância de dados e de pedidos de exames complementares; fim da redigitação das informações; integração com outros sistemas de informação; processamento contínuo dos dados, deixando-os imediatamente disponíveis para todos os atores envolvidos no cuidado ao paciente.

A utilização da solução objetivo desta pesquisa servirá como um incremento tecnológico aos PEP. Ao aproveitar-se da característica descentralizada da *Blockchain*, as informações dos pacientes poderiam ser acessadas por qualquer agente de saúde que o paciente deseje, provendo através do IPFS uma base de dados escalável e segura para os dados sensíveis. Assim posto, o presente trabalho justifica-se através de sua sincronia com o planejamento governamental, propondo uma implementação melhorada para a gestão de informação médica através do uso de tecnologias como *Blockchain*, *Smart Contracts* e IPFS cuja estrutura teórica estará descrita ao longo da monografia.

Inicialmente, será realizada uma contextualização das tecnologias usadas para criação do sistema. Em seguida, serão apresentadas as especificações da aplicação, os casos de uso e seus fluxos de execução, e por fim, será efetuada uma

análise do programa onde serão abordadas questões relacionadas a implementação, segurança e performance da solução proposta.

2 REVISÃO TEÓRICA

Este capitulo introduz uma contextualização das bases temáticas que circundam e possibilitam o desenvolvimento da aplicação. Iniciando pelo conceito da *Blockchain*, na sequência será apresentado o funcionamento dos *smart contracts,* a rede Ethereum, que permite a criação de grandes sistemas, por conta de sua escalabilidade. Por fim, é exposta a arquitetura e a comunicação do IPFS, local onde é armazenado os prontuários médicos.

2.1 BLOCKCHAIN

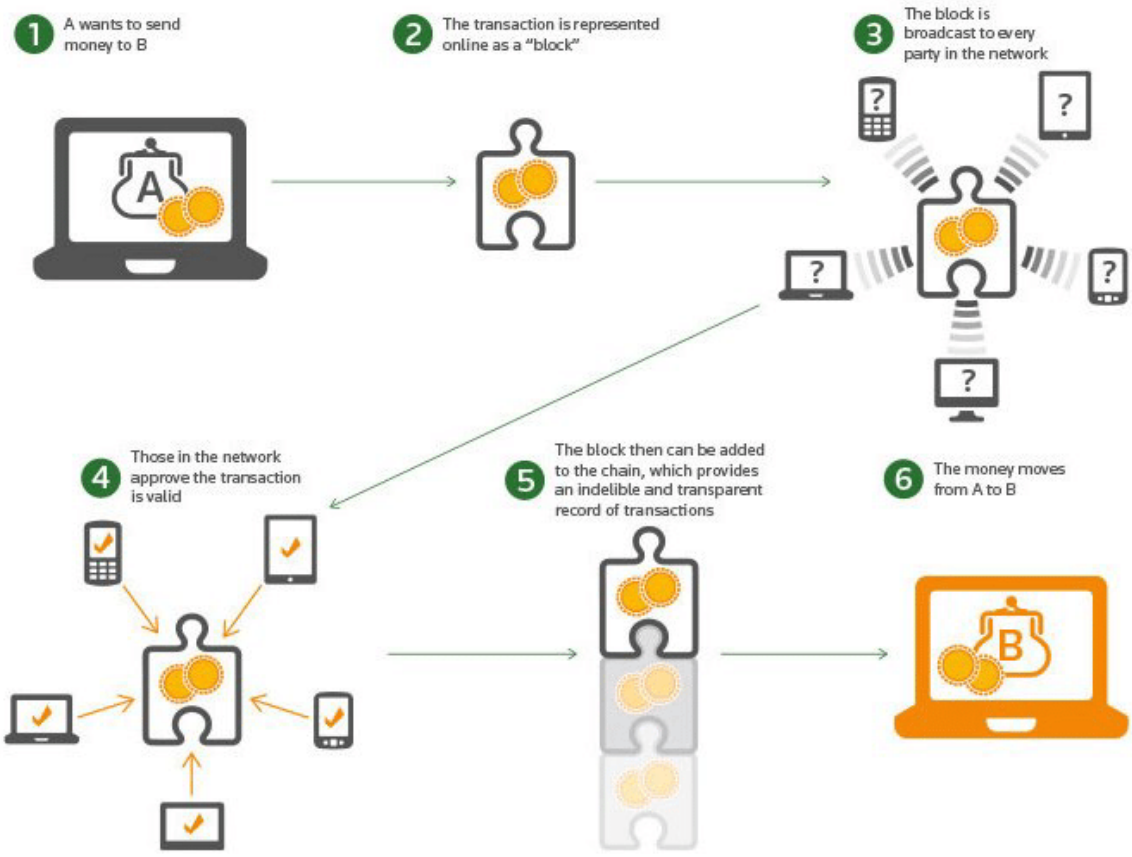
A tecnologia da rede *Blockchain* introduziu o conceito de uma base de dados distribuída que guarda informações de maneira descentralizada, ou seja: as informações são compartilhadas entre todos os participantes da rede (ALHARBY; MOORSEL, 2017). Uma das principais características do *Blockchain* é o mecanismo de troca *peer-to-peer* (P2P), o qual permite aos membros realizar transações de maneira segura sem a necessidade da existência de um terceiro agente entre as partes (como uma instituição bancária ou governo), desta forma possibilitando a eliminação de burocracias e dificultando corrupção (EBIZIMOH *et al.*, 2019). Na área da saúde é possível analisar um crescimento de interesse na utilização desta tecnologia para melhorar a segurança, privacidade e interoperabilidade dos dados de saúde (Mettler, 2016).

A estrutura do protocolo é formada por uma lista ordenada de blocos identificados por uma *hash* em que cada uma referência o anterior a ele na rede, guardando informações sobre um conjunto de transações realizadas por um membro. Para a adição de novos blocos na rede, existem dois conceitos que se destacam nas implementações da *Blockchain*, no método *Proof of Work* (PoW), usuários conhecidos como mineradores realizam grandes cálculos matemáticos gastando poder de processamento e uso de memória para realizar a mineração dos dados, o minerador que conseguir resolver o enigma ganhará uma recompensa pelo seu trabalho (Schinckus, 2021). A principal técnica concorrente ao PoW é o *Proof of Stack* (PoS), onde alguns personagens da rede são validadores de informação, para participar desse ecossistema uma parte das moedas do usuário são congeladas como garantia do seu trabalho, caso a pessoa trabalhe de má fé, ela perderá o montante previamente

disponibilizado (ETHEREUM, 2022b). Quando se deseja adicionar uma cadeia de blocos a rede, os validadores devem fazer uma aposta para decidir quais blocos são validos. Quando um bloco é adicionado, a rede disponibilizará uma recompensa com base no tamanho da aposta realizada por cada usuário (Li *et al.,* 2017).

Uma vez que o bloco é criado e adicionado à rede, não pode ser alterado, o que mantém a integridade das operações. A FIGURA 1 apresenta o passo a passo de uma transação financeira entre duas entidades usando esse protocolo e a forma como rede confirma a veracidade da operação.

FIGURA 1 – FLUXO DE EXECUÇÃO BLOCKCHAIN



FONTE: Nelaturu *et al.* (2022).

É importante observar que ainda existem desafios a serem superados antes que a tecnologia *Blockchain* possa ser implementada em larga escala na área da saúde. Além das problemáticas regulatórias, a falta de escalabilidade da *Blockchain* no armazenamento de grandes massas de dados também é apontada como um

problema por conta da baixa performance e alto custo das redes que implementam esse protocolo (CHUKWU; GARG, 2020).

2.2 SMART CONTRACTS

Um contrato inteligente é um *script* que executa na rede *Blockchain* visando automatizar, reforçar e garantir termos pré-programados pelo próprio *Smart Contract*. Uma vez que as condições predefinidas são cumpridas, o seu objetivo é efetuar automaticamente as premissas do contrato entre as partes (MOHANTA *et al.*, 2018) Portanto, essa tecnologia proporciona: 1) uma diminuição no custo do processo em comparação aos sistemas tradicionais de contratos, os quais exigem que um intermediário valide os termos dos membros; 2) redução de riscos de fraudes e comportamentos maliciosos, pois ao publicar uma instância do programa na rede ele é imutável e todo o processo de transações são rastreáveis e auditáveis; 3) a diminuição da burocracia, uma vez que, com a retirada do agente intermediário do processo, todas as validações serão feitas por um algoritmo de maneira automática, retornando o resultado da operação em uma menor taxa de tempo; e 4) mitigação dos erros, tendo em vista que a análise dos termos do contrato será feita por uma máquina, assim eliminando os problemas de avaliação e interpretação que poderiam ser causados por um humano ao validar o caso (ZHENG *et al.,* 2020).

Cada contrato terá um endereço único na rede *Blockchain*. No caso da *Ethereum*, o tamanho desse endereço pode ser 20 ou 160 bytes (ETHEREUM, 2022a). Para executá-lo, os usuários podem simplesmente enviar uma transação para o seu endereço. Assim, ela será validada por todos os membros mineradores da rede, que chegarão a um consenso sobre o resultado, para que então o estado do contrato seja alterado.

Com a popularização do *Ethereum*, os *Smart Contracts* ganharam relevância na área da tecnologia devido à sua versatilidade de aplicações. Um contrato inteligente pode ser usado em diferentes áreas que necessitam da eliminação de intermediários e para automação de sistemas. Dentro deste escopo existem trabalhos relevantes em áreas como gerência de cadeia de suprimentos, *Internet of Things* (IOT), sistema financeiro, entre outros (MOHANTA *et al.*, 2018). Ao longo deste trabalho reflete-se a aplicação dessa tecnologia na área da saúde com foco na automação de sistemas de prontuário médico.

2.3 ETHEREUM

A primeira implementação do protocolo *Blockchain* surgiu com a criptomoeda *Bitcoin*, o que possibilitou um sistema de negociação entre duas partes não confiáveis sem um intermediário. Contudo, o *Bitcoin* não é flexível em sua programação e assim dificulta construções de aplicações complexas baseadas nesse protocolo (ATZEI *et al.,* 2018). Dessa forma, outras implementações foram surgindo com o objetivo de suprir essa necessidade. Neste contexto nasceu a rede *Ethereum*, a qual constitui uma implantação da *Blockchain* baseada em contratos inteligentes, fator que permite a criação de grandes aplicações e organizações descentralizadas (ETHEREUM, 2023).

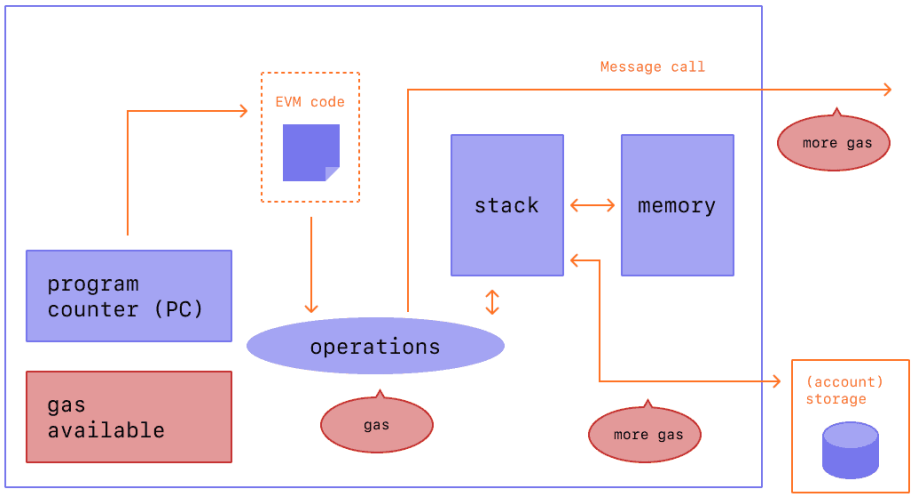
A *Ethereum* utiliza o algoritmo de PoS para persistência de novos blocos. Dessa forma, há uma melhoria relevante na eficiência energética da rede inteira, uma vez que ela para de depender de grandes computadores para criação de novos blocos e validações de transações (FANTI *et al.* 2021). Outra consequência é a maior descentralização, pois a barreira de entrada passa a ser menor com o aumento da complexidade da rede (EHTEREUM, 2022c), permitindo assim a maior escalabilidade da *Ethereum* e a criação de grandes aplicações baseadas nessa rede.

As automações dentro da Ethereum são feitas utilizando uma linguagem de alto nível denominada *Solidity*. Os scripts adicionados dentro da rede são interpretados e executados através da *Ethereum Virtual Machine* (EVM) (ETHEREUM, 2022d). O site oficial da rede *Ethereum* (não p., 2023) define a EVM como:

> O contexto físico da Máquina Virtual do *Ethereum* (EVM, na sigla em inglês) não pode ser descrito da mesma maneira que é descrita uma nuvem nocéu ou uma onda no meio do oceano, se não que deve ser entendido como uma entidade singular mantida por milhares de computadores conectados operandoum cliente de *Ethereum*.
>
> O próprio protocolo *Ethereum* existe apenas com o propósito de manter a operação contínua, ininterrupta e imutável dessa máquina de estado especial. É o ambiente em que todas as contas *Ethereum* e contratos inteligentes vivem.Para qualquer bloco na cadeia, o *Ethereum* tem um estado "canônico", e a EVM é a responsável por definir as regras para registrar um novo estado válido de um bloco para o seguinte.

Outro conceito importante utilizado pela EVM é o gás. Este define a complexidade computacional necessária para execução dos contratos inteligentes dentro da rede, quando maior esforço, maior é a taxa a ser paga pela execução do programa, se custo para efetuação do código for maior que a quantidade de gás disponível, será lançado uma exceção, a FIGURA 2 apresenta o pipeline da EVM no momento de execução de um contrato inteligente.

FIGURA 2 – MODELO DE EXECUÇÃO DA ETHEREUM VIRTUAL MACHINE



FONTE: Máquina virtual do Ethereum (2023).

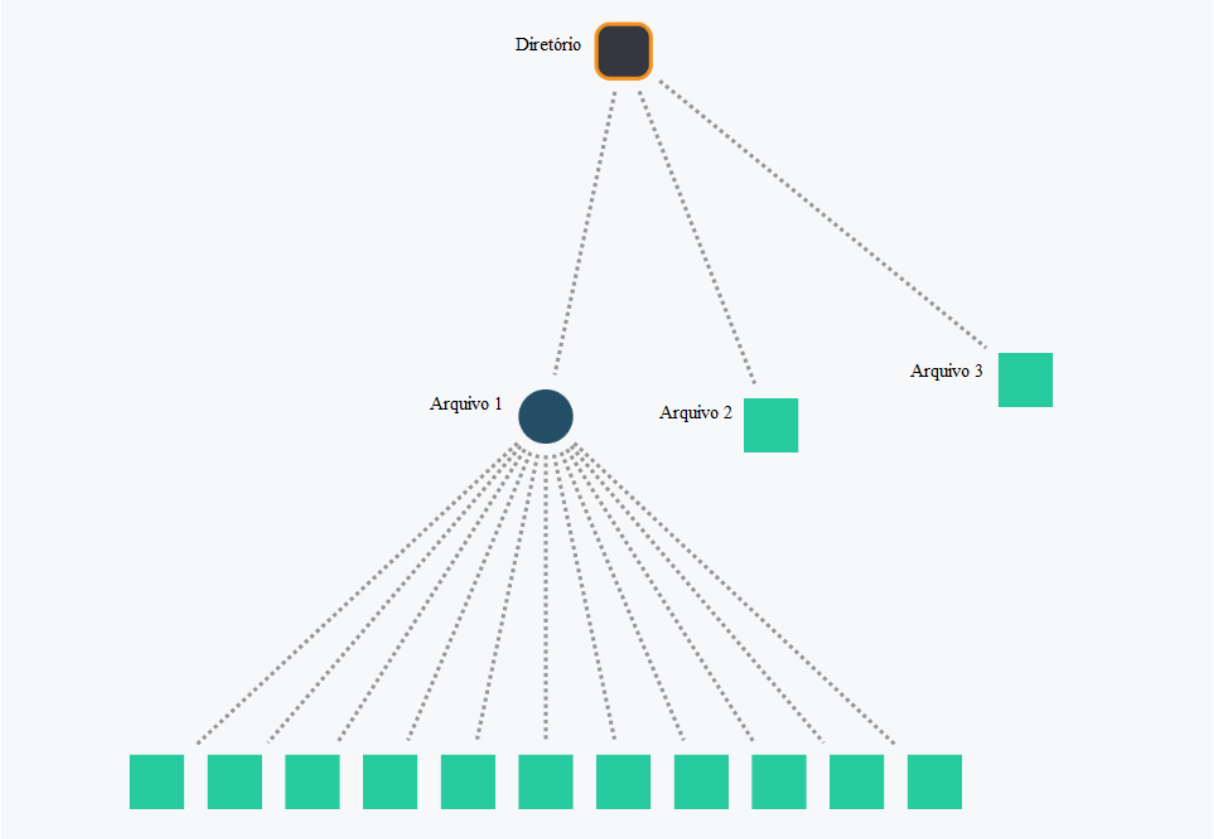
A taxa para execução do *script* é calculada em giga-wei (*Gwei*), uma representação da moeda principal da rede, o *Ether* (ETH), onde 1 wei equivale a um valor igual a 0,00000001 ETH (10^{-9} ETH). O gás também funciona como um mecanismo de defesa da *Ethereum*, ajudando na identificação de desperdícios e limitando a quantidade máxima de recursos que podem ser usados em transações (ETHEREUM, 2022e). Isso implica que, apesar da *Ethereum* ser mais escalável em relação as suas aplicações do que outras implementações da *Blockchain*, ela continua tendo as algumas limitações com custos e desempenho. Não é recomendado armazenar grandes quantidades de dados dentro de um contrato na rede *Ethereum*, ou até mesmo realizar custosos cálculos matemáticos, pois isso geraria grandes taxas e lentidão nas transações da rede.

2.4 INTERPLANETARY FILE SYSTEM

O *InterPlanetary File System* é um sistema distribuído P2P inspirado em outras aplicações com a mesma característica; tais quais *Git* e *Torrent*, ele armazena informações em uma estrutura de *Distributed Hash Table* (DHT) (BENET, 2014). Isto é, os objetos salvos na rede podem ser acessados de maneira análoga a uma tabela *hash* simples com chave-valor, porém de maneira distribuída em um *Merkle Directed Acyclic Graphs* (DAG) um grafo direcionado acíclico em que cada nodo contém um identificador único. Essa estrutura de dados tem um funcionamento próximo ao de uma árvore B+, pois os arquivos ficam salvos somente nas folhas e os galhos funcionam como indexes que auxiliam na busca entre os nós (IPFS, 2023a).

Ao salvar um arquivo no IPFS, será retornado um *content identifier* (CID), uma hash criada atráves do algoritmo *SHA-256* que poderá ser usada posteriormente para recuperação do registro (IPFS, 2023b). O identificador é gerado com base no conteúdo do arquivo, isso faz com que qualquer alteração gere uma nova CID. Durante o registro, o IPFS analisa o tamanho do arquivo. Documentos grandes são separados em pequenos blocos usando o *Unix File System* (UnixFS), um protocolo de *buffer* que faz a desestruturação desses dados e cria um *link* entre eles para uma reconstrução futura (IPFS, 2022). Esse algoritmo auxilia na criação da *Markle DAG.* A FIGURA 3 mostra um exemplo desse grafo. Repare que o Arquivo 1 teve de ser separado em múltiplos pedaços. A CID retornada ao final da inserção é igual ao identificador do nó raiz, que contém todas as partes do arquivo. Caso ele não precise ser divido, como os casos dos Arquivos 2 e 3, o identificador retornado são as das próprias folhas (IPFS, 2023a).

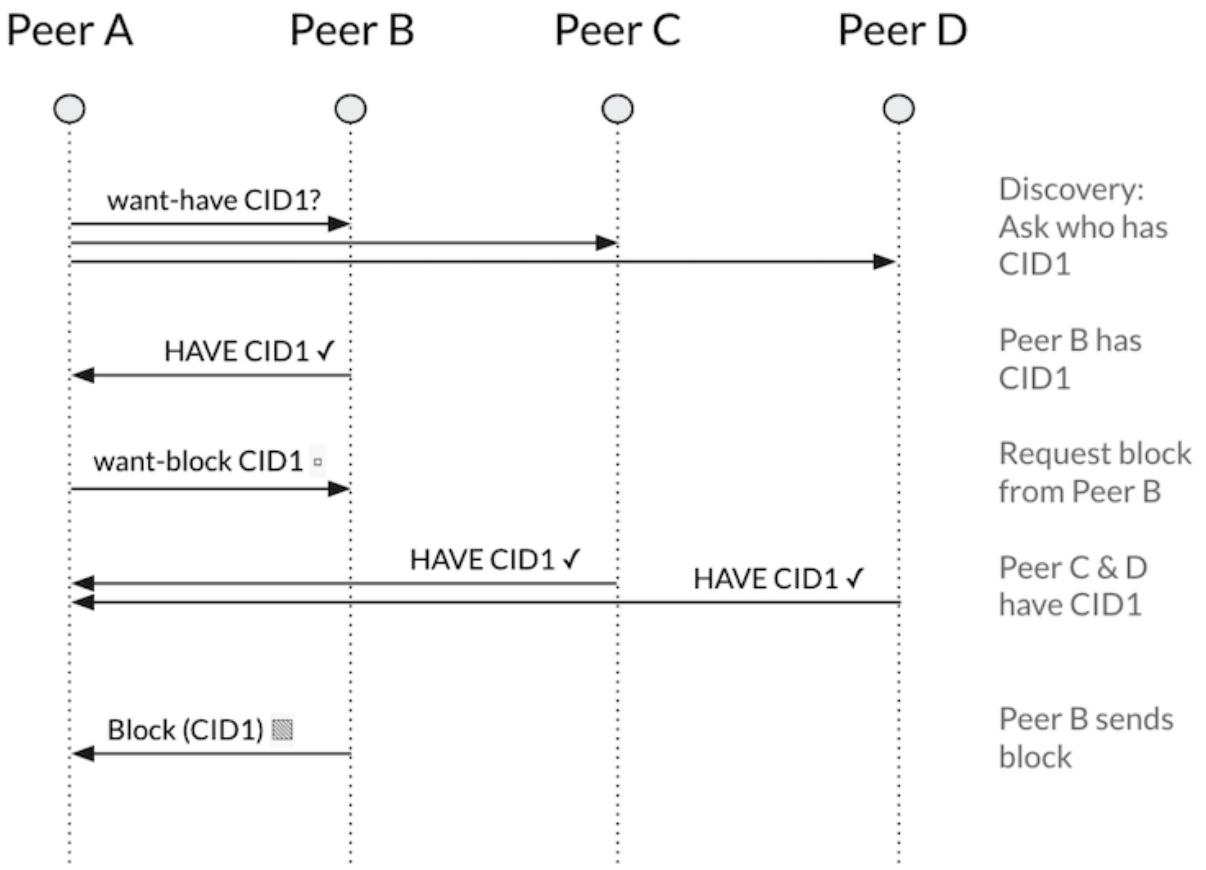
FIGURA 3 – UM EXEMPLO DE DAG



FONTE: Desenvolvido no DAG *builder* (2023).

Para a recuperação e reconstrução do dado, o IPFS utiliza o *Bitswap*, um protocolo baseado em mensagens entre os blocos da rede. a comunicação feita por ele contém dois tipos de dados 1) *want-lists*, que constitui uma lista dos CIDs que se deseja ser recuperado. Essa informação é passada pelo nó raiz (aquele que chama a rede IPFS para adquirir o arquivo) para os outros *peers* da rede; 2) os blocos de arquivos. Caso algum nó tenha a CID requisitada, é enviada o sinal "*have CID*" a quem fez o disparado e a raiz da chamada enviará um sinal de "*want-block*" diretamente ao *peer* que o comunicou anteriormente. Na sequência lhe é enviado o bloco (FIGURA 4). Nodos que não contém a CID lançam um sinal "*dont-have*" para o chamador. Caso nenhum nó retorne à informação, é feita uma chamada para a DHT, validando se existe algum nó na rede que contenha o identificador (IPFS, 2023c).

FIGURA 4 – COMUNICAÇÃO ATRAVÉS DO PROTOCOLO BITSWAP



FONTE: Bitswap (2023).

O *Bitswap* é um dos grandes trunfos do IPFS. De la Rocha *et al.* (2021) mostram o ganho de desempenho oferecido pelo protocolo em comparação a outros algoritmos de busca em uma *Markle* DAG. Já Confais *et al.* (2016), por sua vez, realizam uma comparação de performance nos momentos de escrita e leitura em relação ao banco de dados *no-SQL* Casandra, mostrando um resultado satisfatório dentro dos cenários apresentados. Por fim, Daniel e Tschorsch (2022) alertam que, por conta da tecnologia ainda ser recente, faltam pesquisas e *benchmarks* usando dados maiores na casa dos *petabytes*, por exemplo.

Visando melhorias, foi desenvolvida pelo mesmo criador do *InterPlanetary File System* o *filecoin*, uma implementação *open-source* de uma rede descentralizada de armazenamento de arquivos baseada no IPFS (PSARAS; DIAS, 2020). Diferentemente do primeiro, o *filecoin* inclui mecanismos de incentivo para o armazenamento de dados em larga escala, onde os pagamentos e penalidades são gerenciados de maneira automatizada pelo protocolo. Outra vantagem dessa tecnologia em relação ao IPFS é o número de aplicações que fornecem interfaces

mais amigáveis ao programador que deseja fazer a integração com sua aplicação (FILECOIN, 2023), como por exemplo o *Web3Storage*, uma biblioteca usada no *JavaScript* que abstrai diversas peculiaridades de uma comunicação direta com o *filecoin*.

3 METODOLOGIA

3.1 TIPO DE PESQUISA

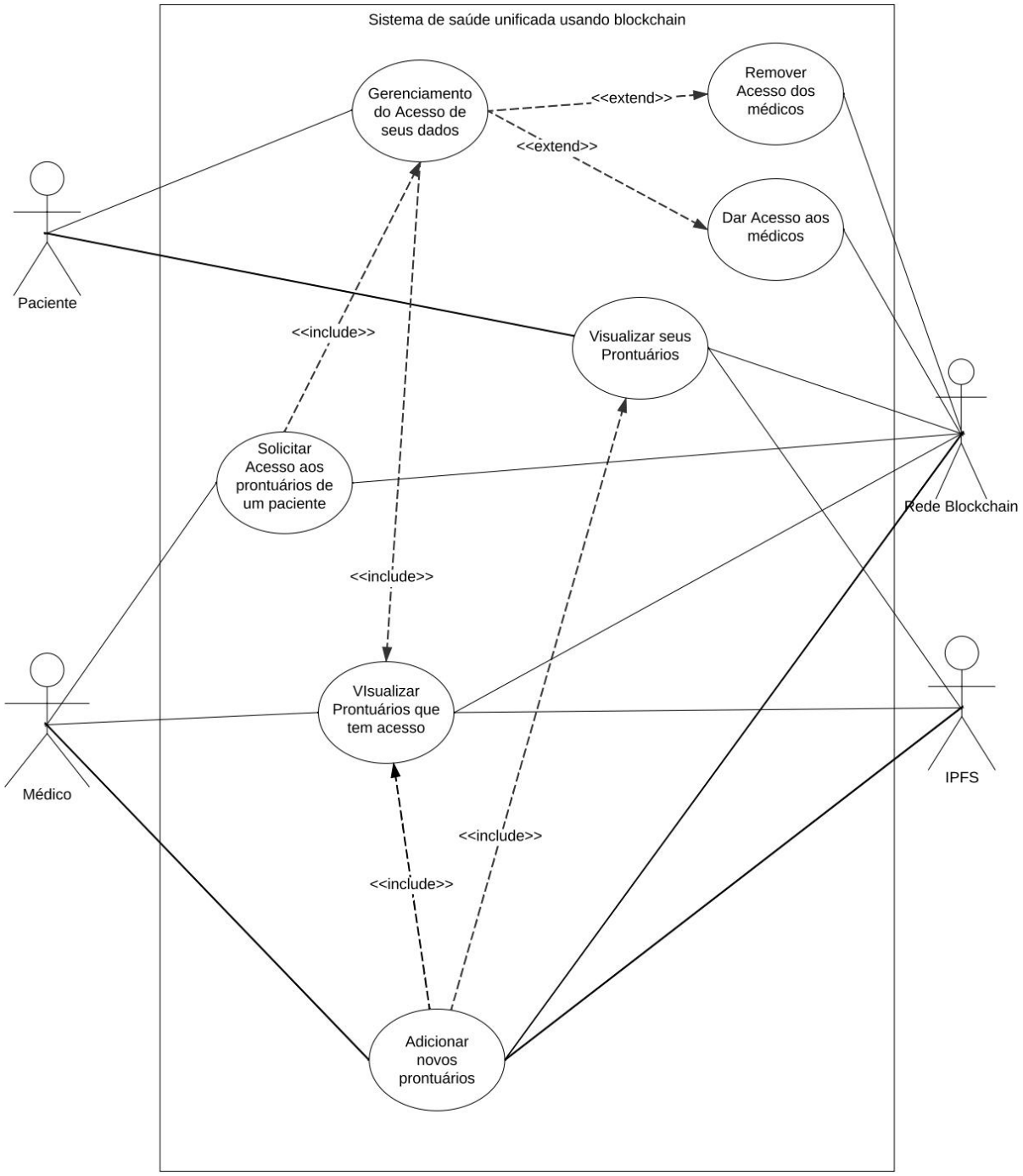
Segundo Vergara (1990), pesquisas aplicadas visam de forma fundamental resolver problemas reais da sociedade através de um estudo sistemático e prático. Tendo em vista essa explicação, pode-se definir esse trabalho como um estudo aplicado, visto que propõe uma solução unificada para os sistemas de saúde, com o objetivo de resolver as dificuldades na integração entre os hospitais, médicos e pacientes.

3.2 ESPECIFICAÇÃO DO SISTEMA

3.2.1 Casos de uso

Antes da concretização da arquitetura do sistema, foi criado um diagrama de casos de uso (FIGURA 5) que é utilizado na compreensão de aplicações no que diz respeito ao modo como as funcionalidades se relacionam entre si e com os atores externos do sistema. Para isto, utiliza-se a *Unified Modeling Language* (UML), uma linguagem de modelagem visual comum, largamente difundida no desenvolvimento de software (LUCIDCHART).

FIGURA 5 – CASOS DE USO



FONTE: Os autores (2023).

O paciente possui relacionamento com duas funcionalidades do sistema: o gerenciamento de acesso aos dados – funcionalidades de autorização e desautorização dos médicos que podem observar suas informações – e visualização de seus prontuários em tempo real. Já o médico associa-se com três casos de uso: 1) solicitação de acesso aos prontuários, cuja funcionalidade requer permissão do paciente, pois sempre que uma nova solicitação for feita ele deve decidir se a esta

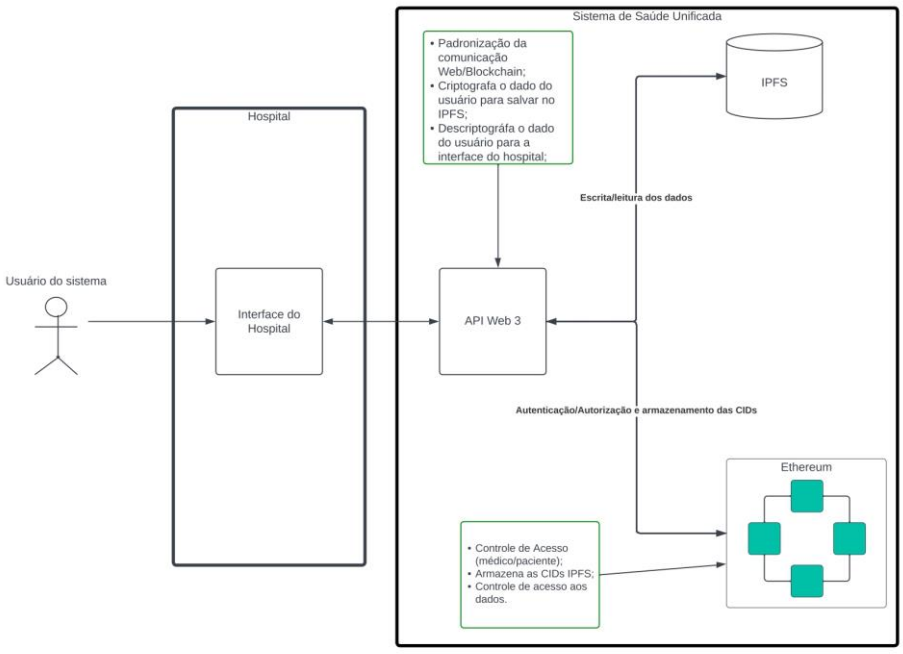
será concedida ou não; 2) visualização dos prontuários com acesso, assim como a anterior, esta se relaciona diretamente com o permissionamento dos dados do paciente, pois o doutor só contemplará os dados caso tenha autorização; e por fim, 3) adição de novos prontuários, sendo vital que, após a realização dessa ação, a visão de ambos atores (médicos e pacientes) seja prontamente atualizada com as novas informações.

A Rede *Blockchain* possui participação em todas as funcionalidades do sistema. O controle de permissionamento é implementado nos contratos inteligentes, que também armazena os identificadores dos prontuários médicos utilizados para recuperação dos dados no IPFS – os quais, por sua vez, mantêm relacionamento apenas com as funcionalidades que tem a ver com a leitura e escrita dos dados.

3.2.2 Arquitetura

Para a concepção do aplicativo, criou-se uma modelagem macro do sistema a fim de fornecer melhor visualização dos módulos e de suas responsabilidades dentro de todo *APP*. A FIGURA 6 exibe a arquitetura proposta.

FIGURA 6 – ARQUITETURA BASE DO SISTEMA



FONTE: Os autores (2023).

O módulo do hospital é a interface do usuário, podendo variar entre as instituições que utilizam o aplicativo, e deve garantir uma boa experiência e usabilidade, isto é, o sistema deve ser simples, eficiente e agradável no seu uso, tanto funcionalmente quanto esteticamente para os médicos e pacientes que consumirão o aplicativo. Além disso, é responsabilidade do hospital escolher a melhor forma de acessar e providenciar os recursos disponibilizados pelo módulo servidor aos usuários.

O servidor pode ser separado em 3 blocos que trabalham em conjunto para retornar as informações solicitadas pelo hospital: a rede *Ethereum*, que contém os *Smart Contracts*; o IPFS, para o armazenamento dos prontuários médicos; e a API, que integra esses dois segmentos do servidor processando os dados e entregando ao módulo hospitalar.

Os métodos desenvolvidos por meio do contrato inteligente possuem permissões distintas de acordo com o ator que utiliza o sistema. Pacientes não podem criar prontuários, por exemplo, e médicos não podem acessar os registros se não tiver autorização do enfermo (TABELA 1). Como abordado na seção sobre *Ethereum*, salvar dados grandes na rede *Blockchain* é custoso tanto financeiramente quanto computacionalmente, gerando lentidão e altos custos. Logo, o *Smart Contract* deve guardar apenas uma referência do arquivo, um identificador que permita que o prontuário médico seja recuperado posteriormente, para esse sistema é a CID retornada pelo IPFS.

TABELA 1 – LISTA DE ACESSO AOS MÉTODOS DO CONTRATO INTELIGENTE

Método	Paciente	Médico
Autorizar médico	✓	x
Desautorizar médico	✓	x
Listar médicos que pediram acesso	✓	x
Listar médicos com acesso	✓	x
Listar prontuários	✓	✓
Solicitar acesso a dados	x	✓
Listar pacientes que têm acesso	x	✓
Adicionar prontuários	x	✓

FONTE: Os autores (2023).

Além das funções de comunicação da API, ela adiciona mais uma camada de segurança para a aplicação: após receber o dado que deve ser salvo, é aplicado o

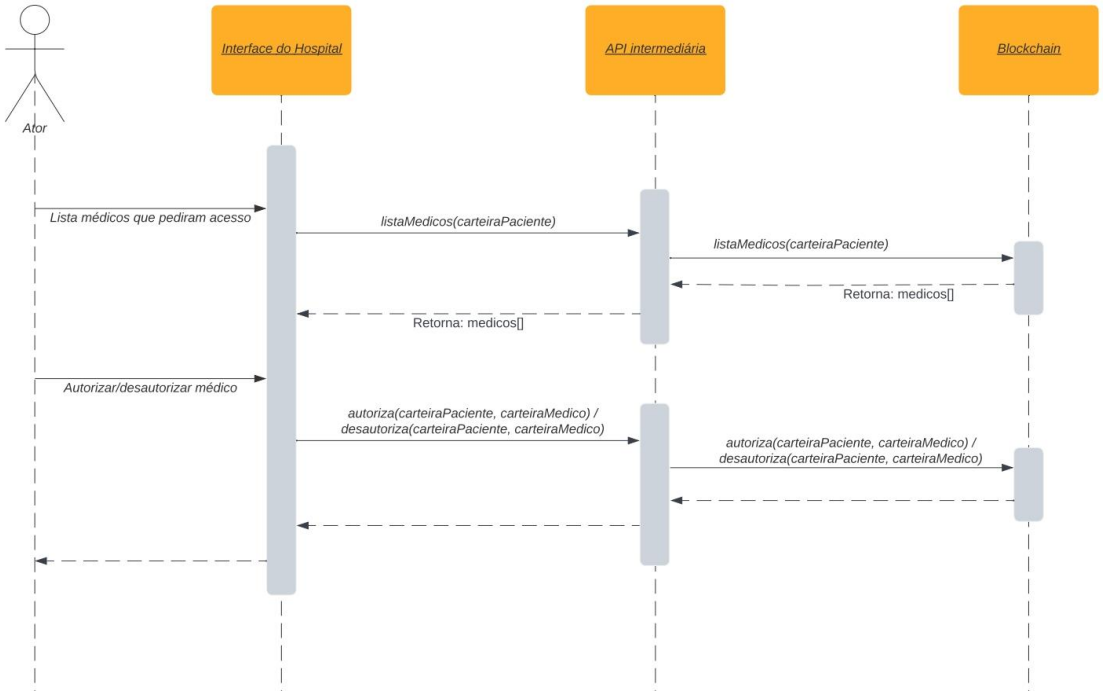
algoritmo de criptografia simétrica *Advanced Encryption Standard* (AES), uma cifra de bloco e chave única, com a segurança reconhecida internacionalmente (DAEMEN; RIJMEN, 1999), ou seja, por mais que um atacante consiga a CID do prontuário, não conseguiria acessar os dados, uma vez que a informação estará criptografada e necessitará da chave, que apenas a API possui.

3.2.3 Diagramas de Sequência

Diagramas de Sequência ou de evento é uma das linguagens de modelagem da UML que possui o objetivo de mostrar a iteração entre atores e módulos do sistema, descrevendo a ordem das execuções em que ocorrem as operações (LUCIDCHART). De maneira antagônica ao diagrama de casos de uso, os diagramas de evento especificam a comunicação dentro de uma linha temporal, indo mais a fundo na especificação do aplicativo e mostrando, por exemplo, as funções chamadas por cada serviço e os seus retornos em algumas situações.

O fluxo da FIGURA 7 mostra o processo de autorização das informações de um usuário após o médico disparar o método de solicitação aos dados. A imagem evidencia que, antes da decisão final do paciente, este recebe uma lista dos médicos que requisitaram a autorização, assim garantindo que ele sempre terá essa listagem atualizada. Além disso, caso o paciente conceda acesso ao médico, posteriormente ainda poderá ser feito a desautorização do profissional da saúde, haja vista que o enfermo possui controle de todos os usuários com acesso às suas informações, tendo a liberdade de restringir quem tem o comando de gerenciar seus dados.

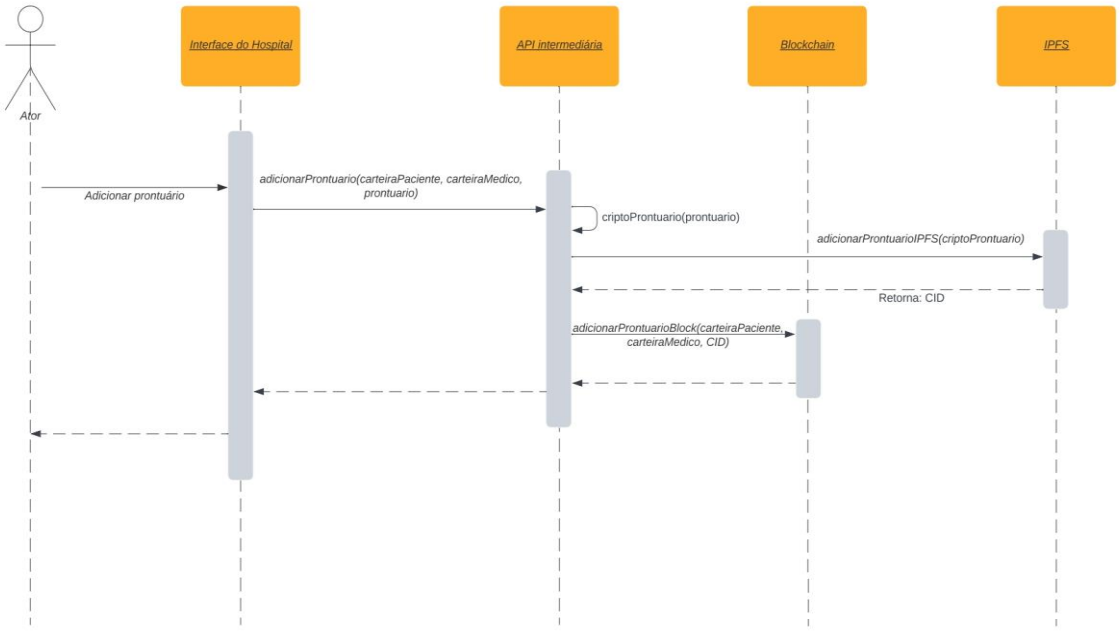
FIGURA 7 – FLUXO DE AUTORIZAÇÃO



FONTE: Os autores (2023).

A partir do momento em que o médico tem autorização para manipular os dados do paciente, ele pode executar o fluxo da FIGURA 8. Por se tratar de uma adição de um novo prontuário médico esse diagrama depende da iteração com o IPFS, mas antes dessa comunicação o registro é cifrado utilizando AES, como já citado anteriormente. O IPFS retornará uma CID que será persistido na rede *Ethereum* para recuperação posterior. Já que a transmissão entre a interface e a API é através do *Hyper Text Transfer Protocol Secure* HTTPS, é esperado um retorno usando os códigos padrões do protocolo. Em caso positivo, será mostrado o 201, significando que o prontuário foi criado com sucesso; e em casos de falha serão retornados códigos em um intervalo de 400-599.

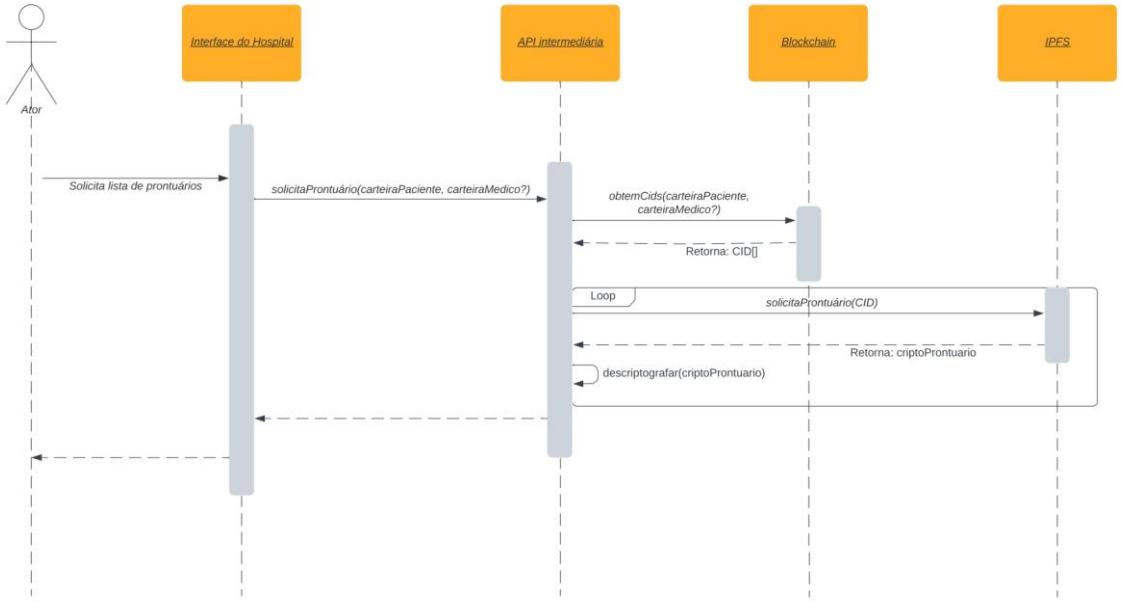
FIGURA 8 – FLUXO DE ADIÇÃO DE PRONTUÁRIOS



FONTE: Os autores (2023).

O fluxo de listagem de prontuários pode ser feito por médicos e pacientes (FIGURA 9). A validação é feita na *Blockchain* de forma que, caso o método *obtemCids* seja chamado pelo paciente, ele precisa apenas passar a sua carteira e a *Blockchain* fará a autenticação, assim como retornará os dados relacionados ao usuário. Se a função for requerida por um profissional da saúde, além de passar a informação do enfermo, deve ser passada a sua carteira, pois a *Blockchain* deve validar se o médico realmente tem acesso aos dados. Após o retorno da lista de CIDs é feito um laço, onde a API vai passar a CID para o IFPS e ela receberá o prontuário criptografado que, depois da sua decodificação e o fim do *loop*, será retornada a interface do sistema para a visualização do usuário.

FIGURA 9 – FLUXO DE LISTAGEM DE PRONTUÁRIOS



FONTE: Os autores (2023).

3.3 AMBIENTE DE EXECUÇÃO

A rede *Ethereum* da aplicação foi criada através do Ganache, um programa que gera uma *Blockchain* local que por padrão fica instanciada no endereço *localhost* da máquina. A rede foi configurada com 10 usuários onde cada um deles possui 100 ETH. Além disso, a constante *gasPrice* foi mantida com o valor próximo do real praticado na *Ethereum* em janeiro de 2023, 25 Gweis (YCHARTS, 2023), e o *gasLimit* não foi alterado por não afetar as transações feitas na rede (TRUFFLE SUITE, 202-a), já que os dados que foram salvos nos blocos não chegam nesse limite pré-definido pelo Ganache. Realiza-se o *deploy* do contrato inteligente utilizando o *Truffle*, um ambiente para programação de *Smart Contracts* suportados pela EVM. Em nossa pesquisa, usamos a linguagem padrão da *Ethereum*, o *Solidity* (TRUFFLE SUITE, 202-b). O modulo IPFS foi implementado utilizando *Web3.Storage*, que consiste em um conjunto de API que permite a comunicação via protocolo *Representational State Transfer* (REST), o mais comum tratando-se de integração entre sistemas web modernos (WEB3STORAGE, 2023). Já os dados da aplicação são gerenciados pela rede IPFS, cuja implementação os armazena na criptomoeda *filecoin*, adicionando mais uma camada de proteção criptográfica ao sistema.

Assim como a rede *Ethereum*, a API intermediária é instanciada localmente, comunicando-se com o IPFS via *Web3.Storage* e com o *Ethereum* através do *Web3.*

O modulo Interface do Hospital foi implementado como uma *Single Page Application* (SPA) utilizando a biblioteca React. A comunicação é feita via HTTPS e os dados são processados na API e mostrados na tela através do *frontend*.

3.3.1 Hardware

O computador utilizado para os testes possuí as configurações listadas abaixo:

- **Processador:** 11th Gen Intel® Core™ i7-11800H @ 2.30GHz, x64, 8 núcleos e 16 *threads*, cache L2: 10240 KB e cache L3: 24576 KB;
- **Placa de Vídeo:** NVIDIA GeForce RTX 3060 Laptop GPU, 6 GB VRAM;
- **Memória RAM:** 16 GB, com frequência de 3200 MHz;
- **Disco:** SSD IM2P33F3A NVMe ADATA 512GB, com Leitura 2000 MB/s e Gravação 1100 MB/s

4 ANÁLISE DO SISTEMA

4.1 IMPLEMENTAÇÃO

4.1.1 Contrato Inteligente

O contrato inteligente foi construído pensando na estrutura de dados que compõe um paciente e o modo como essas propriedades se relacionavam com os métodos definidos nos requisitos do sistema. Como a funcionalidade de login e registro da nossa implementação é simplificada, não foi de nossa preocupação armazenar uma senha e e-mail. Outra consequência foi a criação de um método especifico do sistema para o registro de nome do paciente, melhorando a visualização na tela final do usuário (ALGORITMO 1).

Algoritmo 1 Estrutura de Dados do Contrato Inteligente

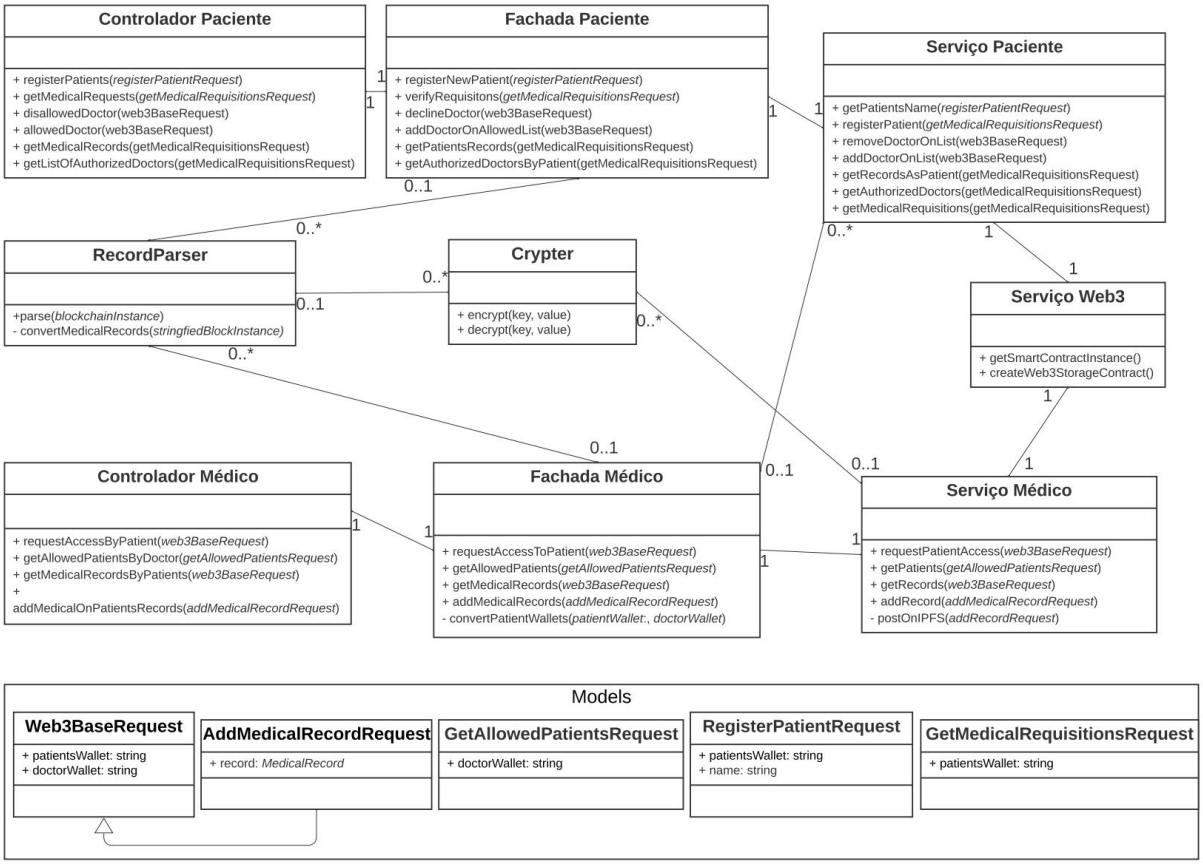
```
struct Pacient_t{
   string name;
   string[]medicalRecordsCID;
   address[] pendingApprovals;
   mapping(address => bool)
   authorizedWalletsToPacientData;
}


mapping(address => Pacient_t) private pacientsList;
mapping(address => address[]) private doctorPacientAuthMatri
```

As estruturas de *mapping* funcionam como uma *hash* chave-valor. Logo, ao passar a carteira de um paciente corretamente o retorno será toda a sua estrutura. Como todas as chamadas levam em consideração o endereço de quem invocou a função, significa dizer que um usuário comum só poderá acessar seus próprios dados. Médicos que desejam visualizar as informações de algum paciente terão os seus acessos armazenados no mapeador *doctorPacientAuthMatrix*, e toda alteração nessas informações serão refletidas nessa propriedade do sistema (GITHUB, 2023).

4.1.2 Integração das Tecnologias

A API utiliza o padrão de projeto fachada, uma classe que centraliza o acesso a uma determinada informação do sistema (REFACTORING GURU, 2023). O digrama de classe da FIGURA 10 exemplifica o funcionamento da API e a comunicação entre as classes.

FIGURA 10 – DIAGRAMA DE CLASSES DA API



FONTE: Os autores (2023).

As *Models* do sistema são classes que fazem a representação das informações passadas pelo *frontend* na aplicação, estas são usadas durante todo o fluxo de execução das requisições. Classes controladores são as portas de entrada da API na comunicação com os hospitais. Delegam as requisições as fachadas, onde está armazenada as regras de negócio do aplicativo, e retornam o *status* da chamada assim como o conteúdo se necessário. Os serviços de paciente e médico fazem a

comunicação com a *Blockchain* e com o IPFS, a sua responsabilidade é pegar os parâmetros pré processados pela fachada, fazer a solicitação ao contrato inteligente e retornar o resultado para a realização do pós processamento novamente a quem fez a chamada. Já a classe Serviço Web3 cria uma ponte com o Ganache e retorna uma instancia de comunicação com o contrato inteligente persistido na rede local. As classes de apoio *Crypter* e *RecordParser* auxiliam na codificação e decodificação dos prontuários e na conversão de CID para prontuário respectivamente.

4.2 SEGURANÇA

Por se tratar de tecnologias distribuídas, a rede *Ethereum* e o IPFS são de grande valia para a garantia da disponibilidade dos dados. Isto porque, caso algum nó caia em qualquer um desses protocolos, não afeta a acessibilidade das informações. Para que o sistema de saúde integrado garanta o acesso aos dados será necessário a criação de uma infraestrutura adequada para o uso em larga escala, além de otimizações em algumas funções críticas do sistema, como a leitura dos prontuários médicos e também a adição.

A garantia da confidencialidade e integridade dos dados é concebida pelo *Smart Contract*. Apenas médicos tem a permissão de manipular registros dos enfermos e todo o controle de acesso aos dados é feito pelo paciente, podendo autorizar e desautorizar a qualquer momento um médico. Por conta das propriedades da criação das CIDs no IPFS, não é possível manipular os prontuários uma vez salvos na rede distribuída, porque os identificadores dos arquivos são únicos, impossibilitando alterações.

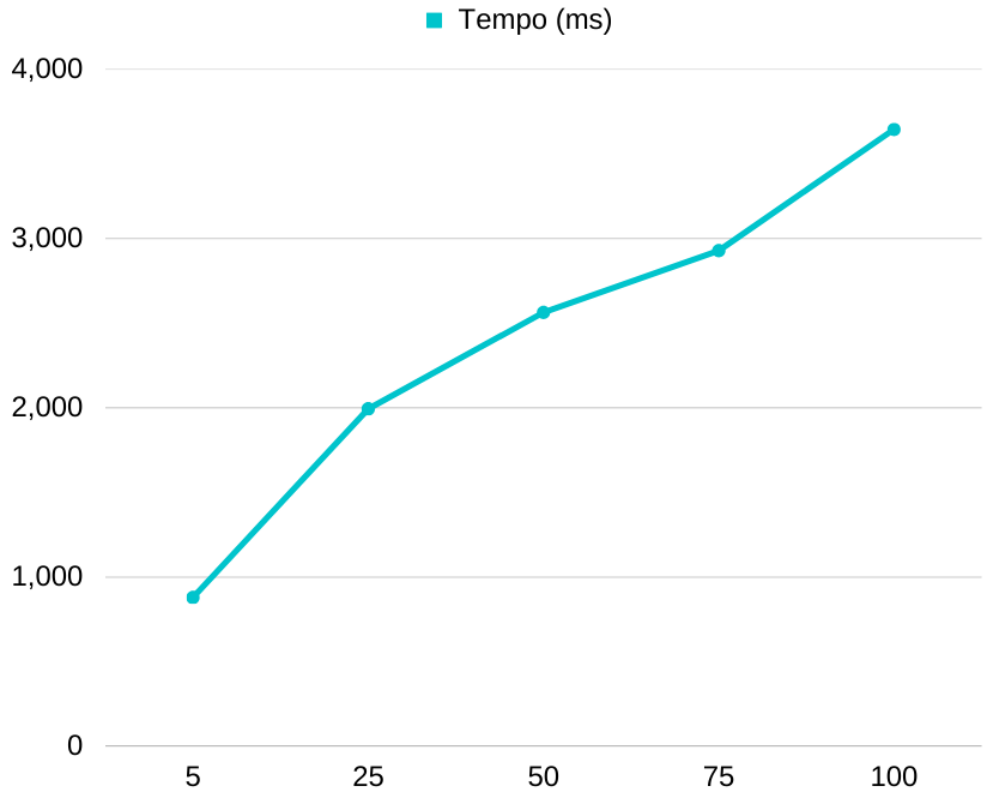
Outra medida de segurança implementada na aplicação é a criptografia AES utilizada antes de salvar a informação no IPFS. Por conta da integração com *Web3Storage* os dados já passam por uma cifra própria da moeda *Filecoin*, mas caso o atacante consiga a CID de algum prontuário, ainda assim ele não terá o acesso à informação, tendo em vista que o dado é salvo codificado.

4.3 PERFORMANCE

No que diz respeito ao tempo de resposta da aplicação, foi realizada uma análise do método mais custoso do sistema, além da leitura dos prontuários médicos,

que envolve a recuperação da lista de CIDs de um paciente, a chamada ao IPFS para cada CID, assim como a decodificação das informações salvas. O tempo mostrado no gráfico da FIGURA 11 é uma média de 50 chamadas feitas para cada variação no número de prontuários a serem recuperados, onde metade deles possuía anexo com o tamanho médio de 235.07 KB e a outra metade não continha e a média de tamanho foi de 413 B.

FIGURA 11 – TEMPO DE EXECUÇÃO PARA LISTAGEM DE PRONTUÁRIOS



FONTE: Os autores (2023).

Apesar do tempo escalar de maneira linear é possível melhorar ainda mais o desempenho. Não é comum e nem uma boa prática trabalhar com um alto número registros de uma vez só, nem acessar o IPFS sempre que for requisitado uma listagem dos prontuários. A API pode ter otimizações através da implementação de uma memória cache, diminuindo as chamadas diretas ao IPFS, que são custosas, assim como um banco de dados. Isso ocorre por terem uma fundamentação parecida, já que as duas tecnologias utilizam a estrutura de uma árvore B+. Outra técnica para a

melhoria da eficiência na entrega dos dados seria a implementação de paginação ajudando a diminuir número de registros a serem retornados em uma única chamada.

5 CONSIDERAÇÕES FINAIS

Ao longo desse trabalho foi demonstrado que, através de um olhar crítico para o avanço das tecnologias disponíveis no mercado, é possível desenvolver uma solução aplicada às principais fragilidades de um importante pilar da sociedade: a saúde. A viabilidade de implementação do sistema se justificou por meio do alinhamento com o planejamento do Ministério da Saúde, que visa, até 2028, aumentar o uso de prontuários eletrônicos e, por conseguinte, a intercomunicação de informações no sistema de saúde.

O modelo apresentado baseou-se na característica descentralizada de armazenamento de dados trazendo um incremento aos PEPs a fim de atacar as os problemas enfrentados pelas instituições de saúde. Para tanto, buscamos apoio nas tecnologias de *Blockchain* (gestão de acessos e referências de dados) e IPFS (armazenamento descentralizado) que nos proporcionaram um aumento na interoperabilidade na rede de saúde, ou seja, maior transparência na comunicação entre os agentes, devolvendo a autonomia ao paciente, porém sem deixar de lado conceitos chaves da segurança da informação como integridade, confidencialidade, disponibilidade e autenticidade.

5.1 TRABALHOS FUTUROS

Apesar de ter demonstrado um desempenho satisfatório, conforme apresentado na seção de análise de desempenho, é conhecido que, conforme escalamos o uso do sistema para grande parte da população brasileira, enfrentar-se-á pontuais barreiras que podem ser trabalhadas em projetos futuros.

Primeiramente, para que o sistema possa funcionar em escala real, deseja-se subir os contratos inteligentes em uma rede *Ethereum* pública de desenvolvimento para que usuários possam interagir com o sistema através de suas carteiras. Ademais, a fim de uma melhora de desempenho na comunicação com o IPFS, é possível incrementar a infraestrutura do sistema com o uso de uma memória cache na API que diminuirá o número de requisições necessárias ao buscar dados de prontuários. Por fim, durante a implementação da interface do hospital utilizamos um formato genérico de prontuários. Contudo, essa estrutura deve estar em sintonia com o requerido por profissionais da saúde. Portanto, para o futuro, é necessário fomentar uma discussão

entre as principais instituições de medicina a fim de chegar em um formato padrão de armazenamento de dados médicos.

REFERÊNCIAS

BRASIL. Ministério da Saúde. **Estratégia de saúde digital para o Brasil 2020-2028**. [Recurso Eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília: Ministério da Saúde, 2020. 128 p. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesos em: 02 jan. 2023.

BRASIL. Lei nº 14.709, 14 de agosto de 2018. **Portal da Legislação**, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jan. 2023.

ALHARBY, M; VAN MOORSEL, A. Blockchain-based smart contracts: A systematic mapping study. **Fourth International Conference on Computer Science and Information Technology** (CSIT-2017). Fuzhou, 2018. p.1-6. Disponível em: https://ieeexplore.ieee.org/document/8756390. Acesso em: 21 jan. 2023.

ATZEI, N.; BARTOLETTI, M.; CIMOLI, T.; LANDE, S.; ZUNINO, R. Sok: Unraveling bitcoin smart contracts. **Principles of Security and Trust**. 2018. p. 217-242. Disponível em: https://www.researchgate.net/publication/324515136_SoK_Unraveling_Bitcoin_Smart_Contracts. Acesso em: 13 jan. 2023.

BENET, J. IPFS - Content Addressed, Versioned, P2P File System. **arXiv**. 2014. p. 1-11. Disponível em: https://arxiv.org/pdf/1407.3561.pdf. Acesso em: 10 jan. 2023.

CHUKWU, E.; GARG, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. **IEEE Access**, v. 4, 2020. p. 1-20. Disponível em: https://www.researchgate.net/publication/338870963_A_Systematic_Review_of_Blockchain_in_Healthcare_Frameworks_Prototypes_and_Implementations/link/5ea90e83299bf18b958459dc/download. Acesso em: 10 jan. 2023.

CONFAIS, B.; LEBRE, A.; PARREIN, B. Performance analysis of object store systems in a fog/edge computing infrastructures. **2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)**. Luxemburgo, 2016. Disponível em: https://ieeexplore.ieee.org/document/7830696/. Acesso em: 16 jan. 2023.

DAEMEN, J.; RIJMEN, V. Aes proposal: Rijndael. **The Rijndael Block Cipher**. 1999. p. 1-45. Disponível em: https://www.researchgate.net/publication/2237728_AES_proposal_rijndael. Acesso em: 10 jan. 2023.

DANIEL, E. e TSCHORSCH, F. Ipfs and friends: A qualitative comparison of next generation peer-to-peer data networks. **IEEE Communications Surveys & Tutorials**, v. 24, n. 1. p. 31–52. Disponível em: https://arxiv.org/pdf/2102.12737.pdf. Acesso em: 13 jan. 2023.

DE LA ROCHA, A.; DIAS, D.; PSARAS, Y. **Accelerating content routing with bitswap**: A multi-path file transfer protocol in ipfs and filecoin. 2021. 11 p. Disponível em: https://research.protocol.ai/publications/accelerating-content-routing-with-bitswap-a-multi-path-file-transfer-protocol-in-ipfs-and-filecoin/delarocha2021.pdf. Acesso em: 09 jan. 2023.

FARINA, A. **Prontuário Médico.** Conselho Federal de Medicina. Disponível em: https://portal.cfm.org.br/artigos/prontuario-medico/. Acesso em: 13 jan. 2023.

EBIZIMOH, A.; NORTA, A.; AZOGU, I.; UDOKWU, C.; DRAHEIM, D. Blockchain technology for enabling transparent and traceable government collaboration in public project processes of developing economies. **18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society**. Noruega, 2019. p. 464-475. Disponível em: https://www.researchgate.net/publication/333984481_Blockchain_Technology_for_Enabling_Transparent_and_Traceable_Government_Collaboration_in_Public_Project_Processes_of_Developing_Economies. Acesso em: 13 jan. 2023.

ETHEREUM. **Anatomy of Smart Contracts.** 15 ago. 2022a. Disponível em: https://ethereum.org/en/developers/docs/smart-contracts/anatomy/. Acesso em: 18 jan. 2023.

ETHEREUM. **Consumo de energia do Ethereum.** 23 jan. 2023. Disponível em: https://ethereum.org/pt-br/energy-consumption/. Acesso em 07 fev. 2023.

ETHEREUM. **Máquina virtual do Ethereum (EVM)**. 5 dez. 2022b. Disponível em: https://ethereum.org/pt-br/developers/docs/evm/. Acesso em: 23 jan. 2023.

ETHEREUM. **Gás e Taxas**. 5 dez. 2022c. Disponível em: https://ethereum.org/pt-br/developers/docs/gas/. Acesso em: 23 jan. 2023.

FANTI, G.; KOGAN, L.; VISWANATH, P. Economics of proof-of-stake payment systems. **Imperial College London**, jun. 2020. 19 p. Disponível em: https://www.emilianopagnotta.com/descarga/discussions/Economics_of_POS.pdf. Acesso em: 10 jan. 2023.

FILECOIN. **Filecoin and IPFS**. 30 jan. 2023. Disponível em: https://docs.filecoin.io/developers/introduction/filecoin-and-ipfs/. Acesso em: 30 jan. 2023.

GONÇALVES, J. P. P.; BATISTA, L. R.; CARVALHO, L. M.; OLIVEIRA, M. P.; MOREIRA, K. S.; LEITE, M. T.d. S. Prontuário eletrônico: uma ferramenta que pode contribuir para a integração das redes de atenção à saúde. **Saúde em Debate**, Rio de Janeiro, v. 37, n. 96. p. 43-50. jan./mar. 2013. Disponível em: https://www.scielo.br/j/sdeb/a/xLMq3HyhgqNwhX6y3jjpNff/?format=pdf&lang=pt. Acesso em: 10 jan. 2023.

GITHUB. **Saúde Unificada**. 2023. Disponível em: https://github.com/pmartinsesa/saude-unificada. Acesso em: 05 fev. 2023.

IPFS. **Merkle Directed Acyclic Graphs (DAGs).** 23 jan. 2023a. Disponível em: https://docs. ipfs.tech/concepts/merkle-dag/#further-resources. Acesso em: 24 jan. 2023.

IPFS. **Content addressing and CIDs.** 16 jan. 2023b. Disponível em: https://docs.ipfs.tech/concepts/content-addressing/#cid-versions. Acesso em: 20 jan. 2023.

IPFS. **Bitswap.** 16 jan. 2023c. Disponível em: https://docs.ipfs.tech/concepts/ bitswap/. Acesso em: 18 jan. 2023.

IPFS. **Unix File System (UnixFS).** 26 jul. 2022. Disponível em: https://docs.ipfs.tech/ concepts/file-systems/#unix-file-system-unixfs. Acesso em: 18 jan. 2023.

LI, W., ANDREINA, S., BOHLI, JM., KARAME, G. (2017). **Securing Proof-of-Stake Blockchain Protocols**. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds) Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM CBT 2017 2017. Lecture Notes in Computer Science(), vol 10436. Springer, Cham. Disponível em: https://doi.org/10.1007/978-3-319-67816-0_17. Acesso em: 15 jan. 2023.

LI, Y.; WANG, Y.; WAN, J.; REN, Y.; LI, Y. Privacy protection for medical image management based on blockchain. In: Database Systems for Advanced Applications. DASFAA 2021 International Workshops, 2021. **Lecture Notes in Computer Science**, v. 12680.

LUCIDCHART. **Why use a UML diagram?** Disponível em: https://www.lucidchart.com/pages/what-is-UML-unified-modeling-language. Acesso em: 20 jan. 2023.

MASSAD, E.; MARIN, H.; AZEVEDO NETO. R. **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico**. São Paulo: H. De F. Marin, 2003.

METTLER, M. Blockchain technology in healthcare: The revolution starts here, **2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)**. Munique, 2016. p. 1-3. Disponível em: https://ieeexplore.ieee.org/document/7749510. Acesso em: 10 jan. 2023.

MOHANTA, B. PANDA, S.; JENA, D. An Overview of Smart Contract and Use Cases in Blockchain Technology. **9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**, Bengaluru, 2018. p. 1-4. Disponível em: https://ieeexplore.ieee.org/document/8494045. Acesso em: 9 jan. 2023.

NELATURU, K., DU, H. e LE, D. A review of blockchain in fintech: Taxonomy, challenges, and future directions. **Cryptography**, v. 6, n. 2. abr. 2022. Disponível em: https://www.mdpi.com/2410-387X/6/2/18. Acesso em: 23 jan. 2023.

PATRÍCIO, CAMILA & MAIA, MARIANNA & MACHIAVELLI, JOSIANE & NOVAES, MAGDALA & NAVAES, ARAÚJO. (2011). **O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos**. Scientia Medica. 21.

PSARAS, Y.; DIAS, D. The interplanetary file system and the filecoin network. **2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks- Supplemental Volume (DSN-S).** Valência, 2020. p. 80-80. Disponível em: https://ieeexplore.ieee.org/document/9159174. Acesso em: 05 jan. 2023.

REFACTORING GURU. **Facade**. 2023. Disponível em: https://refactoring.guru/pt-br/design-patterns/facade. Acesso em: 05 fev. 2023.

SCHINCKUS, C. (2021). **Proof-of-work based blockchain technology and anthropocene**: An undermined situation? Renewable and Sustainable Energy Reviews, 152:111682.

TRUFFLE SUITE. **What is Ganache?** 202-a. Disponível em: https://trufflesuite.com/docs/ganache/. Acesso em: 14 jan. 2023.

TRUFFLE SUITE. **What is Truffle?** 202-b. Disponível em: https://trufflesuite.com/docs/truffle/. Acesso em: 14 jan. 2023.

VERGARA, S. C. **Tipos de pesquisa em administração.** Rio de Janeiro: Cadernos EBAP, 1990.

WEB3STORAGE. **Frequently Asked Questions.** 2023. Disponível em: https://web3.storage/faq/. Acesso em: 15 jan. 2023.

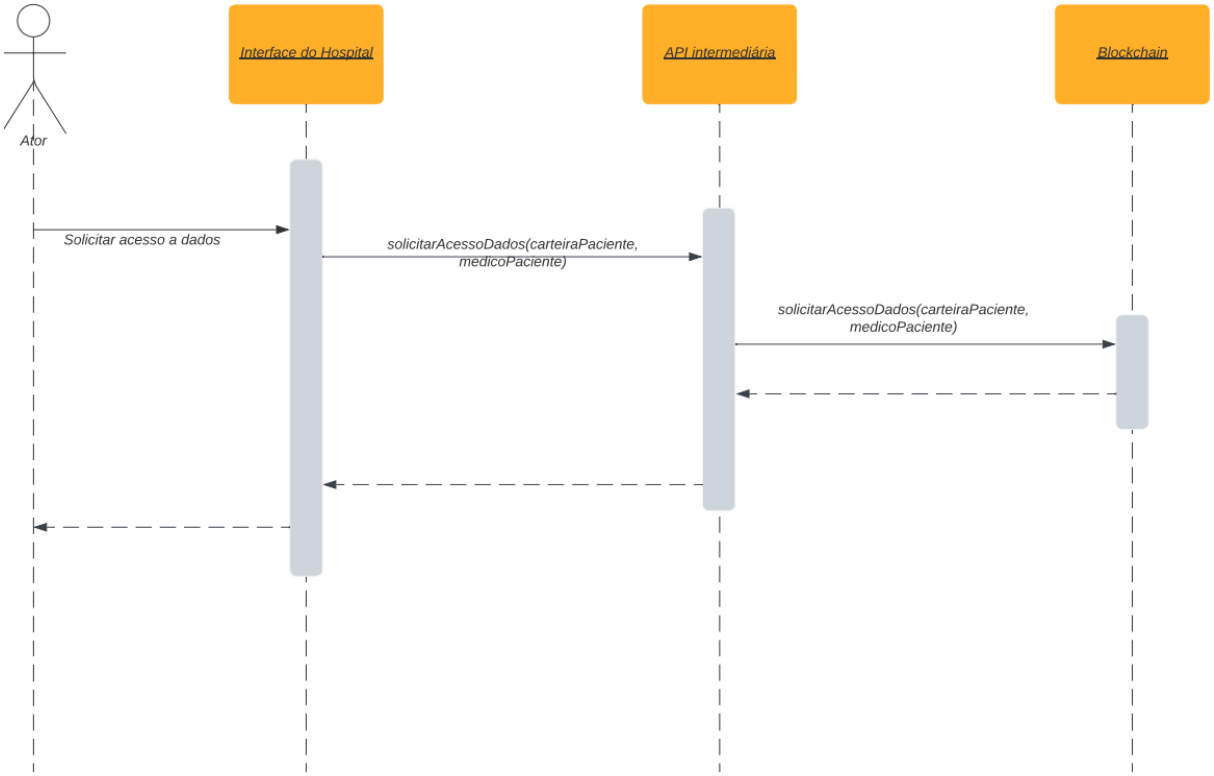
XAVIER, A. d. C. C. **Prontuário eletrônico do paciente: a contribuição da arquivística, da blockchain e dos smart contracts para a sua gestão.** Dissertação (Mestrado em Ciência da Informação) – Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, 2022.

YCHARTS. **Ethereum Average Gas Price for Jan 31 2023.** Disponível em: https://ycharts.com/indicators/ethereum_average_gas_price. Acesso em: 31 jan. 2023.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, W.; CHEN, X.; WENG, J.; IMRAN, M. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, v. 105, 2020. p. 475-491. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X19316280. Acesso em: 20 jan. 2023.

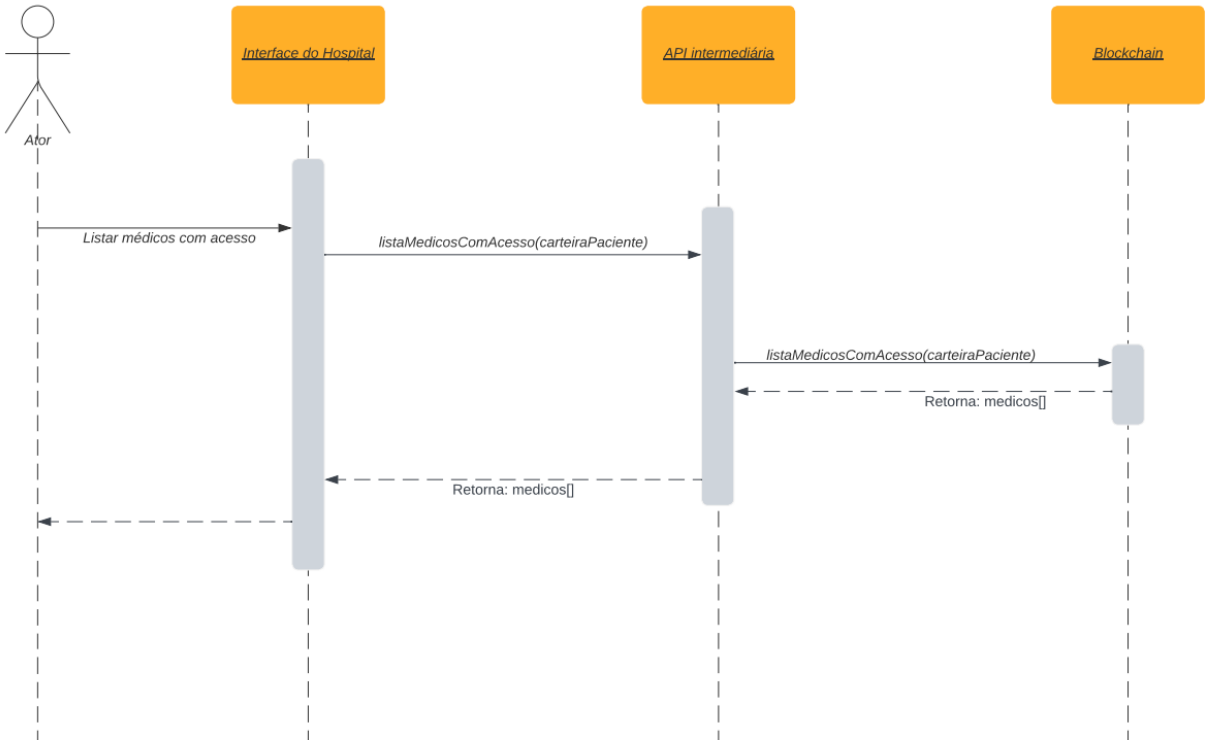
APÊNDICE 1 – DIAGRAMAS DE SEQUÊNCIA

FIGURA 1 – FLUXO DE SOLICITAÇÃO DE ACESSO AOS DADOS



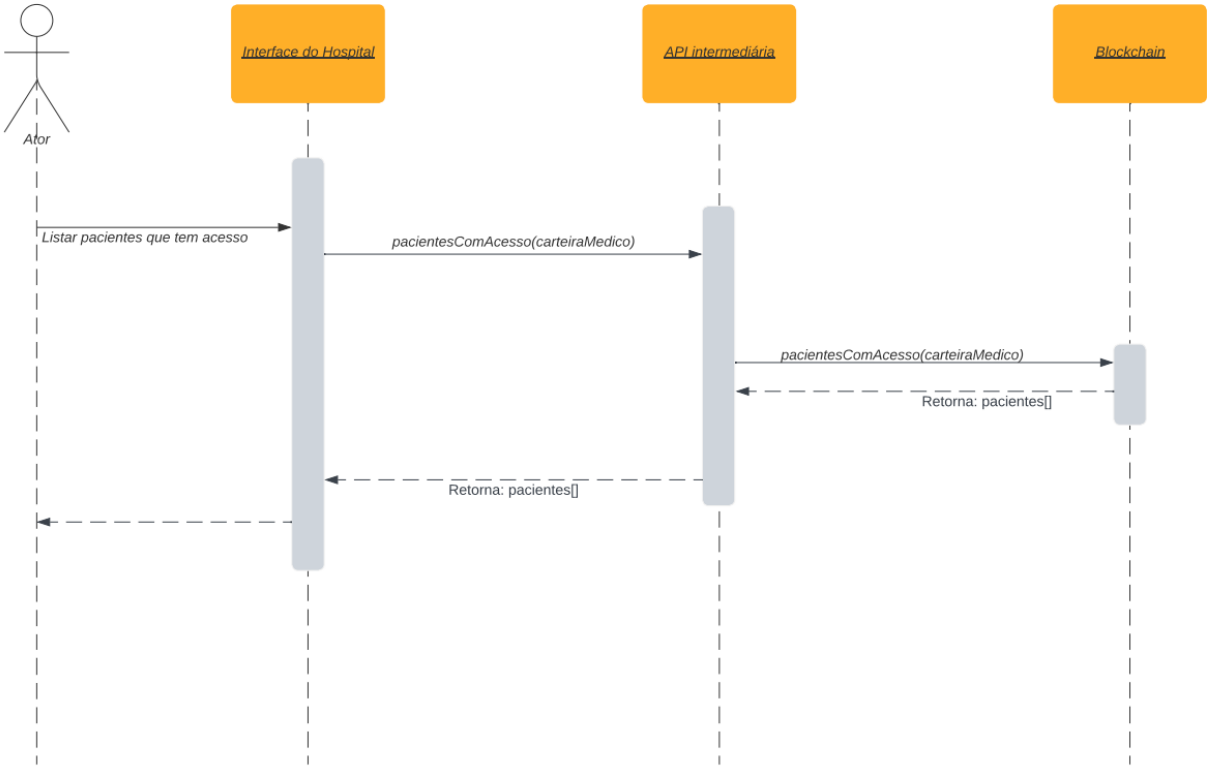
FONTE: Os autores (2023).

FIGURA 2 – FLUXO DE LISTAGEM DE MÉDICOS COM ACESSO



FONTE: Os autores (2023).

FIGURA 3 – FLUXO DE LISTAGEM DE PACIENTES COM ACESSO



FONTE: Os autores (2023).