DOI: 10.36517/resdite.v6.n1.2021.a6 **ARTIGO**

MIRIAM: proposta de solução baseada em blockchain para gerenciamento de registros profissionais de médicos

MIRIAM: A BLOCKCHAIN-BASED SOLUTION PROPOSAL FOR MANAGEMENT OF PROFESSIONAL REGISTRATIONS OF MEDICAL DOCTORS

Raphael Lima Saraiva[1], Allysson Allex Araújo[2], Pamella Sousa[3], Jerffeson Souza[4]

[1]Doutorando em Ciência da Computação - Universidade Estadual do Ceará.
ORCID: https://orcid.org/0000-0003-2054-1982
E-mail: raphael.saraiva@aluno.uece.br
[2] Doutor em Administração - Universidade Federal do Ceará.
ORCID: https://orcid.org/0000-0003-2108-2335
E-mail: allysson.araujo@crateus.ufc.br
[3] Mestranda em Ciência da Computação - Universidade Estadual do Ceará.
ORCID: https://orcid.org/0000-0002-8691-7180
E-mail: pamella.soares@aluno.uece.br
[4] Doutor em Ciência da Computação - Universidade Estadual do Ceará.
ORCID: https://orcid.org/0000-0001-8361-4806
E-mail: jerffeson.souza@uece.br

Correspondência: Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Departamento de Computação. Av. Paranjana 1700 - Campus do Itaperí Itaperí - Fortaleza, CE, Brasil. CEP: 60740000.

Conflito de interesses: os autores declaram que não há conflito de interesses.

Como citar este artigo

Saraiva RL; Araújo AA; Sousa P; Souza JT de. MIRIAM: proposta de solução baseada em blockchain para gerenciamento de registros profissionais de médicos. Revista de Saúde Digital e Tecnologias Educacionais. [online], volume 6, n. 1. Editor responsável: Luiz Roberto de Oliveira. Fortaleza, agosto de 2021, p.01-21. Disponível em: http://periodicos.ufc.br/resdite/index. Acesso em "dia/mês/ano".

Data de recebimento do artigo: 21/07/2020
Data de aprovação do artigo: 21/01/2021
Data de publicação: 12/08/2021

Resumo

Introdução: Constatam-se atualmente vários incidentes e fraudes quanto ao exercício legal de médicos, como emissão de diplomas forjados ou disponibilidade de informações não validadas pelos órgãos fiscalizadores. Justifica-se, portanto, a relevância em investigar soluções que gerenciem, de forma segura e transparente, o histórico profissional de cada médico. **Objetivo:** Assim, o principal objetivo deste trabalho consiste em apresentar MIRIAM, uma solução baseada em blockchain que permite gerenciar de maneira descentralizada e confiável o armazenamento de informações relevantes necessárias para o registro de profissionais médicos. **Método**: Além de uma avaliação quantitativa sobre o desempenho, os eventos cobertos pela proposta foram validados qualitativamente com um diretor de um Conselho Regional de Medicina. **Conclusão:** Dentre as contribuições do projeto, destaca-se a avaliação de uma solução baseada em blockchain para gerenciar registros de

profissionais médicos brasileiros, aderente às normas vigentes no país e viável em termos de desempenho.

Palavras-chave: Blockchain, Hyperledger, Registros de Profissionais Médicos.

Abstract

Introduction: *We notice several incidents and fraud related to medical doctors' exercise, such as issuing forged diplomas or information not validated by the fiscal agencies. One can perceive it to be relevant to investigate innovative solutions that safely and transparentlymanage the professional history of each doctor.* ***Objective:*** *Our main objective is to present MIRIAM, a blockchain-based solution that allows, in a decentralized and reliable fashion, to store relevant information required for the registration of medical professionals.* ***Method:*** *In addition to quantitative performance evaluation, we conducted a qualitative evaluation with a Regional Medical Council's high-level director.* ***Conclusion:*** *Therefore, we contribute by designing and empirically evaluating a blockchain-based solution to manage the registration of medical doctors that fit Brazilian standards as well as suitable performance measures.*

Keywords: *Blockchain, Hyperledger, Registrations of Medical Professionals.*

1. Introdução

A atuação dos órgãos de fiscalização profissional tem sido de real relevância para a sociedade, tendo em vista a necessidade de elaboração e manutenção de normas específicas e particulares de cada profissão em prol da garantia do exercício legal. Nesse contexto, podem ser destacados os profissionais relacionados à medicina, dado o impacto e importância social da categoria. Os atuantes neste campo precisam dedicar-se de forma a não negligenciar os cuidados necessários para com terceiros, cumprindo, assim, as obrigações de forma honesta e legal[1].

Devido à interação entre diferentes agentes para garantia do exercício legal da medicina, faz-se salutar que as informações profissionais dos médicos possam ser gerenciadas de forma segura e confiável. Tal motivação advém da necessidade de se evitar fraudes e inconsistências que possam propiciar crimes relacionados ao exercício ilegal da medicina, conforme prescrito na Lei 2.848/40 do Código Penal Brasileiro, Artigo 282[2].

Assim, o desenvolvimento de tecnologias inovadoras que disponham de segurança para manipulação de dados significativos como os previamente contextualizados, têm se mostrado cada vez mais preponderante, em especial na área de saúde digital[3]. Nesse contexto, pode-se destacar o uso de *Distributed Ledger Technologies* (DLTs), com os quais tornou-se possível o registro de dados de maneira descentralizada e replicadas em cada nó da rede. Conforme Pires *et al.*[4], DLTs são responsáveis pelo armazenamento organizado de informações diversas, independente da aplicação feita aos dados. A *blockchain* é um caso especial de DLTs, em que se implementa um mecanismo baseado em encadeamento de blocos[5].

Blockchain é um livro-razão de propósito geral que oferece uma base de dados altamente transparente, segura e resiliente contra falhas[6]. Tal resiliência ocorre devido a dois fatores: i) a *blockchain* ser replicada em cada nó que compõe a rede; ii) a existência de mecanismos robustos de consenso entre os nós garantindo a integridade do DLT. Assim, as plataformas que utilizam *blockchain* permitem que partes completamente anônimas e que não confiam entre si possam formar uma rede que armazena informações confiáveis. Logo, essa tecnologia tornou-se uma alternativa aos tradicionais sistemas centralizados, dispensando a necessidade de um agente intermediário confiável para gerenciar as informações armazenadas[7].

Ao analisar a literatura, constata-se a ausência de pesquisas relacionadas ao controle de registros profissionais de médicos no Brasil. Considerando tal lacuna e a contextualização previamente mencionada, o presente trabalho tem como objetivo principal propor, utilizando a tecnologia *blockchain*, uma solução, denominada MIRIAM (sisteMa para regIstro de pRofissIonAis Médicos), que permita armazenar as informações relevantes referentes ao controle de registros profissionais de médicos.

Ademais, destacam-se as seguintes contribuições: (1) modelagem do problema para o contexto brasileiro segundo as normas vigentes; (2) fomento à cultura da transparência, da auditabilidade e da integridade de dados; (3) projeto e implementação da Prova de Conceito utilizando o *HyperledgerFabric*; (4) diagnóstico quantitativo sobre o desempenho do sistema; e, por fim, (5) validação qualitativa do processo com especialista membro da administração do Conselho Regional de Medicina do Estado do Ceará (CREMEC).

O restante do trabalho organiza-se da seguinte forma: na Seção I. apresenta-se a introdução e a fundamentação teórica, bem como é definida a arquitetura da solução de forma aderente às normas brasileiras; na Seção II. é apresentada a metodologia abordada neste artigo; na Seção III. apresenta-se a solução proposta; uma demonstração da solução, discutindo-se a avaliação empírica. Por fim, na Seção IV, destacam-se as considerações finais.

1.1 Fundamentação teórica

1.1.1 Controle de Registros Profissionais de Médicos

As responsabilidades do profissional da medicina no Brasil são indicadas pelo Código de Ética Médica (CEM), segundo a Resolução nº 1.246, de 08 de janeiro de 1988, do

Conselho Federal de Medicina (CFM). Apesar da existência destas normas, são frequentes os relatos de ilegalidade no exercício profissional. Para lidar com tais infortúnios, os Conselhos Regionais de Medicina (CRM) atuam como órgãos fiscalizadores e disciplinadores com o intuito de realizar o controle de entidades físicas e jurídicas. O funcionamento dos conselhos é deliberado de acordo com o anexo do Estatuto para os Conselhos de Medicina o qual preceitua em seu Artigo 5º. que o CFM possui jurisdição sobre todo o território nacional. Por sua vez, cada CRM tem sede em sua respectiva capital de Estado e no Distrito Federal, conforme suas áreas de jurisdição.

Dentre as atribuições incumbidas a cada CRM, destaca-se o dever de auxiliar no registro das informações necessárias para o exercício profissional legal de pessoa física e das atividades de pessoas jurídicas de direito público ou privado como proteção à saúde da coletividade. Os médicos, por sua vez, têm o dever de realizar o "prévio registro de seus títulos, diplomas, certificados ou cartas no Ministério da Educação e Cultura e de sua inscrição no Conselho Regional de Medicina [...]"[8]. Por meio da supervisão adequada de informações sobre os profissionais da medicina, pode-se reduzir ilegalidades e informações inconsistentes. Além disso, conforme dispõe o Artigo 3º da Lei nº 12.527/2011, é necessário garantir o acesso à informação segundo os princípios da administração pública[9].

A Resolução CFM nº 2.180/20187 estabelece quais os dados a serem divulgados eletronicamente referentes aos médicos inscritos no Sistema de Conselhos de Medicina para fins de informações ao público: (i) nome completo; (ii) número do CRM; (iii) Unidade da Federação; (iv) sexo; (v) data de inscrição; (vi) fotografia; (vii) endereço comercial e telefone profissional; (viii) tipo de inscrição; (ix) situação da inscrição; (x) especialidades e respectivas áreas de atuação e, por fim (xii) informações sobre inscrições em outras unidades da Federação.

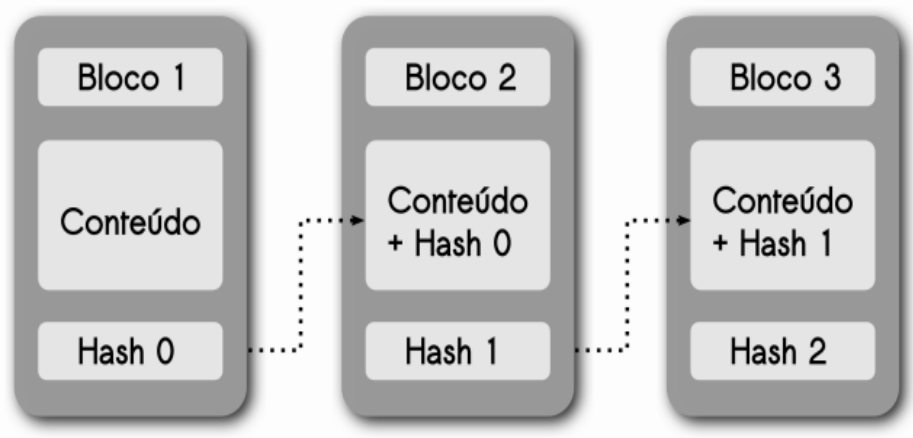
Apesar de informações como estas já serem disponibilizadas digitalmente, ainda se enfrentam variados tipos de ilegalidades. Os médicos que se envolvem em delitos, por exemplo, frequentemente não apresentam o registro de seus títulos, de forma a respeitar as normas estabelecidas.

1.1.2 Blockchain

Em uma *blockchain*, existe uma estratégia responsável por mapear todo o conteúdo armazenado em cada bloco identificado por meio de uma sequência única de bits de comprimento fixo denominado *hash*[10]. Assim, o *hash* que identifica o bloco anterior será

utilizado na definição do *hash* do bloco seguinte, como pode ser visto na Figura 1. Por meio desse encadeamento de blocos denotados pelos valores de *hash*, torna-se possível rastrear blocos anteriores.

Figura 1: Visão Geral



Fonte: Os Autores.

A segurança dos dados é mantida pela replicação do banco de dados e assegurada pelas regras de consenso. Para que toda a rede concorde na ordem dos fatos e preserve sua integridade é necessário um sistema de sincronização de dados conhecido como Algoritmo de Consenso[11]. As possibilidades de modernização de processos tradicionais via *blockchain* têm gerado plataformas de diferentes domínios, demandando, assim, distintos tipos de *blockchains*.

Nesse caso, as *blockchain* permissionadas destacam-se por fornecerem uma maneira de proteger as interações entre um grupo de entidades que têm um objetivo comum, mas que não confiam totalmente umas nas outras[12]. Diferente de uma *blockchain* pública, na qual qualquer um pode participar da rede para visualizar e realizar transações, em uma *blockchain* permissionada é preciso ter a permissão do responsável pela rede.

1.2 Trabalhos relacionados

Após levantamento bibliográfico, identificou-se a ausência de soluções que tratam do controle de registros profissionais de médicos no Brasil. No entanto, ressalta-se a existência de propostas que tratam de um contexto geral sobre o armazenamento de dados oficiais na *blockchain*, como, por exemplo, registro de dados clínicos de pacientes ou certificações acadêmicas. Nesse contexto, Costa *et al.*[10] propõem um serviço pelo qual instituições de

ensino registram documentos oficiais em *blockchain*, como diplomas e certificados, permitindo que outros interessados verifiquem a legitimidade do documento.

Em Mackey *et al.*[11], os autores conduziram uma revisão de literatura a fim de identificar soluções atuais e em desenvolvimento que combatem a falsificação de medicamentos. Já em Ekblaw *et al.*[12] é introduzido o registro de dados de saúde dos pacientes, e aquisição facilitada à essas informações por parte de instituições de saúde através de uma rede *blockchain* privada. Por sua vez, em Liu *et al.*[13] é proposto uma estrutura de compartilhamento seguro e troca de imagens médicas de raios-X baseada na tecnologia *blockchain*.

Meyliana *et al.*[14] apresentam o McRys, um modelo baseado em *blockchain* que registra atividades de uma universidade da Indonésia e integra diferentes partes interessadas. Similarmente, Gresch *et al.*[15] propõem um sistema UZHBC cujo objetivo é o gerenciamento de diplomas para a Universidade de Zurich.

2. Procedimentos Metodológicos

Em termos metodológicos, este trabalho se enquadra em um escopo quali-quantitativo do tipo exploratório. Os procedimentos adotados para consecução do estudo foram organizados em três etapas. A **primeira etapa** ocorreu inicialmente através de uma análise documental[19], pela qual foi possível obter uma compreensão geral do domínio da proposta a partir do estudo das leis e normas que regem os processos referentes à regulamentação do profissional de medicina junto ao CRM. Adicionalmente, realizou-se uma revisão da literatura visando obter elementos teóricos e práticos pertinentes para a abordagem. Para tal processo, pesquisou-se, em fevereiro de 2020, no Google Scholar, as palavras chaves: *Blockchain*, *e-health,* diploma, fraudes, *health records*, *medicine* e *certification*. Salienta-se que o objetivo desse levantamento não foi servir como revisão sistemática da literatura, mas apoiar investigação de bibliografia específica relacionada aos trabalhos relacionados[13-17] e fundamentação científica[18] requerida para o desenvolvimento do projeto, fornecendo, assim, a sustentação teórica para as demais fases.

Na **segunda etapa**, deu-se a implementação da aplicação. A arquitetura definida para a solução foi dividida em duas partes: uma interface web que possibilita o acesso por computador e a *blockchain* responsável por armazenar as informações das inscrições dos registros dos médicos. Para desenvolvimento da interface web, utilizou-se a linguagem PHP juntamente com o *framework* Laravel. Já para o desenvolvimento da *blockchain*, utilizou-se

a *Hyperledger Fabric* em conjunto com o framework *Composer* para comunicação e integração com a interface web.

Por fim, na **terceira etapa** realizou-se uma avaliação empírica, dividida em duas sub-etapas: (i) avaliação quantitativa e (ii) avaliação qualitativa. Em relação à avaliação quantitativa, sabe-se que a *blockchain* pode ser considerada como um gargalo no desempenho da solução proposta, uma vez que para a aplicação funcionar corretamente é necessário um tempo de resposta razoável independentemente dos fatores que possam afetar seu desempenho. Para tal, foi projetado um experimento computacional a fim de analisar o desempenho da solução, investigando a métrica de tempo de resposta. Para o experimento estabeleceram-se então duas variáveis independentes ("Número de Clientes" e "Tipo de Requisição") e uma variável dependente ("Latência de Resposta"). Por sua vez, foram avaliadas quantidades variadas de número de clientes, entre 1 e 400, para cada tipo de requisição.

Sobre a variável "número de clientes", presume-se que à medida que esta aumenta, o desempenho do sistema diminuirá. Já a variável independente "tipo de requisição", por sua vez, pode afetar diretamente o desempenho do sistema dependendo do tipo de requisição. Existem dois tipos de requisição HTTP relacionadas à aplicação atual: *GET* e *POST*, responsáveis pela leitura e escrita dos dados médicos na *blockchain*, respectivamente. O método *GET* tende a ser mais rápido, já que está apenas lendo informações da *blockchain*, não alterando o estado do livro-razão. Já o método *POST* grava informações no *blockchain* e muda o estado do livro-razão, o que o torna mais lento. Adotou-se o *JMeter* 5.0[20] para simular cargas e enviá-las para a *blockchain*. Para todas as medições, foi utilizado um contador de interação definido como 1s. Informações sobre o ambiente computacional encontram-se disponíveis na página de suporte[21].

Quanto à avaliação qualitativa realizou-se uma entrevista em profundidade de, aproximadamente, uma hora de duração junto a um membro da diretoria colegiada do Conselho Regional de Medicina do Estado do Ceará (CREMEC). O entrevistado (nome omitido por razões de confidencialidade) possui uma formação acadêmica de Doutorado em Ciências Médicas, com 30 anos de experiência na área médica. Tal perfil, com ampla experiência acadêmica e prática, denota a relevância pela opção de uma amostragem proposital, cujo principal benefício consiste em obter casos enriquecedores para o estudo[22].

Em suma, o propósito da entrevista foi 1) validar qualitativamente a compreensão dos processos coletados na análise documental e 2) compreender a aderência da solução

em um contexto real a partir dos pontos positivos e negativos envolvidos. Seguindo as boas práticas sugeridas por Boyce e Neale[23], o roteiro da entrevista semi-estruturada consistiu em quatro fases buscando encorajar respostas extensas e descritivas. Primeiramente, foi realizada uma breve explicação sobre a pesquisa ao entrevistado e coletada a assinatura de termos sobre acordos de confidencialidade e não divulgação. Em uma segunda sub-etapa, ocorreu uma explicação detalhada sobre o funcionamento da abordagem proposta e a realização de perguntas a fim de obter a caracterização do entrevistado. Na terceira sub-etapa, foi discutido um conjunto de dez perguntas abertas permeando três tópicos: os serviços prestados pelo CRM, o armazenamento e compartilhamento de dados e, finalmente, os pontos positivos e negativos da solução. Na quarta e última sub-etapa, foram esclarecidas as possíveis dúvidas e coletados os feedbacks gerais sobre o processo de entrevista. Detalhes sobre o roteiro da entrevista estão disponíveis na página de suporte[21].

3. Resultados e discussão

3.1 Solução Proposta

A presente solução, denominada MIRIAM (sisteMa para regIstro de pRofissIonAis Médicos), é baseada nos atuais processos necessários para a inscrição do médico e de suas informações relevantes no CRM, podendo este realizar eventos diversos, tais como a sua primeira inscrição, reinscrição, transferências, cancelamentos e registro de especialidade. Assim, faz-se necessário levar em consideração as entidades que compõem o cenário de registro de informações. Em consonância aos processos descritos na seção anterior, propõem-se as seguintes categorias aos nós participantes da rede:

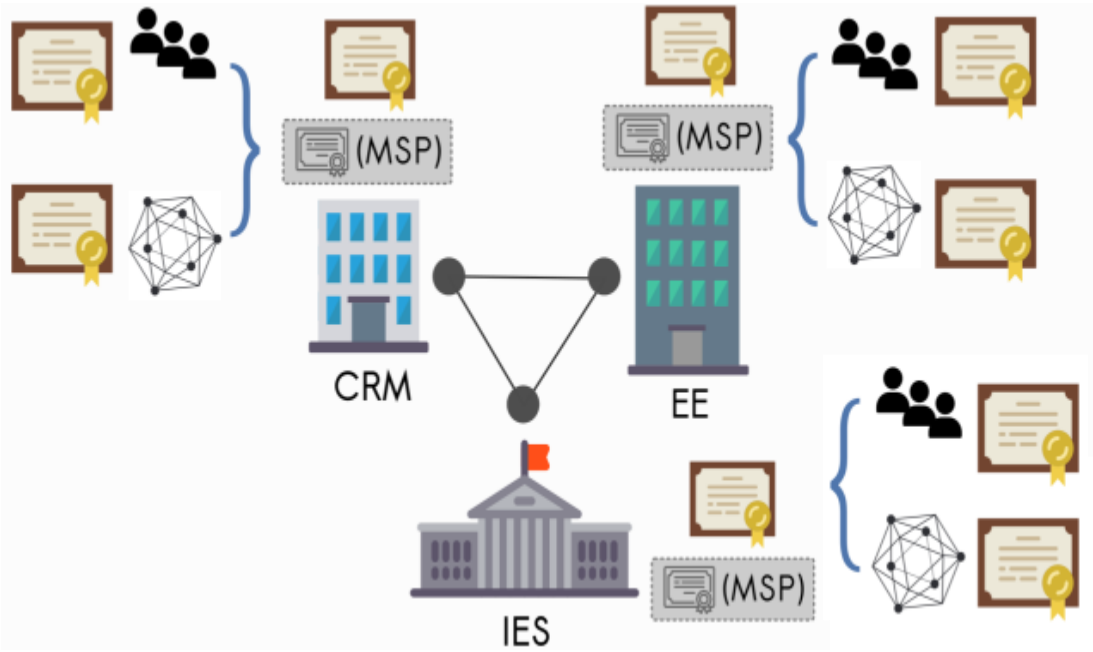
- **Conselho Regional de Medicina (CRM):** é a entidade responsável por fiscalizar, apurar e julgar irregularidades contra médicos no Estado. Além disso, é responsável pelo registro de diplomas, títulos de especialidade e informações relevantes referentes ao profissional;
- **Instituição de Ensino Superior (IES):** é uma instituição que promove educação em nível superior;
- **Entidade de Especialidade (EE):** é uma instituição que possibilita a qualificação do médico em nível de pós-graduação, e emite os certificados de residência médica e títulos de especialidades. Apenas as sociedades de especialidades filiadas à Associação Médica

Brasileira e/ou instituições de residência médica credenciados pela Comissão Nacional de Residência Médica podem realizar tais emissões[19].

Cada uma dessas categorias é composta por um conjunto de nós. Por exemplo, os 27 nós integrantes da categoria CRM representam o CRM de cada estado brasileiro e o Distrito Federal, assim como existem nós que representam cada IESs e EEs. Portanto, forma-se uma rede composta de nós que correspondem a cada uma dessas entidades.

A presente proposta utiliza uma *blockchain* permissionada da tecnologia *Hyperledger* em que cada nó define papéis que são atribuídos aos participantes, e o acesso é concedido ou restrito por meio desses papéis. Um Membership Service Provider (MSP) gera as credenciais para os tipos de participantes. As credenciais da rede são atribuídas por meio de um certificado (Figura 2). Cada organização recebe um certificado e, de acordo com seu nível de autoridade, pode usar um MSP para emitir certificados para os participantes da infraestrutura.

Figura 2: Visão Geral



Fonte: Os Autores.

Assim, uma organização como o CRM recebe o certificado da rede e, por meio dele, novos certificados são gerados para todos os membros de acordo com o nível de acesso. Apenas um membro específico terá permissão aos recursos importantes, como o cadastro dos registros médicos. Além disso, é possível que o CRM autorize sub-redes dentro da rede

principal por meio do certificado emitido. Isso permite que a organização controle quais outras organizações (IES ou EE) podem acessar certas informações.

3.1.1 Hyperledger Fabric

O *Fabric* é um sistema open source que consiste em uma *blockchain* permissionada desenvolvida no espaço colaborativo do *Hyperledger* que dá suporte à implementação de diferentes componentes, como mecanismos de consenso e associação para os membros.

Quatro contêineres são instanciados como parte do ambiente *Hyperledger*. O primeiro e segundo são os **MSP** e **Orderer**, responsáveis pelo serviço de associação de novos membros e o serviço de criação de novos blocos, respectivamente. O terceiro é o **Peer** em que fica o DLT, dependente, por sua vez, do quarto contêiner, **CouchDB**, para guardar os dados de estado.

O *Fabric* gerencia transações por meio de: (i) *Chaincodes*, os quais lidam com a lógica de negócios da rede; (ii) *Ordering Service* que se encarrega de criar, ordenar e anexar os blocos ao DLT; e (iii) *Peers*, que são responsáveis por receber atualizações de estado na forma de blocos do *Ordering Service*.

3.1.2 Hyperledger Composer

O Composer é um conjunto de ferramentas desenvolvido para facilitar a criação de aplicativos utilizando o *Hyperledger* e suportar a infraestrutura do *Fabric*[24]. Tal framework otimiza o tempo gasto na construção da *blockchain* e facilita a integração aos sistemas de negócios. Além de permitir a integração da *blockchain* com aplicativos *web*, o *Composer* pode ser usado para desenvolver a modelagem de casos de uso e a definição da rede do negócio.

Como parte do modelo da rede, definem-se as transações que podem interagir com os serviços. Redes de negócios incluem os participantes que interagem com eles, cada um dos quais pode ser associado a uma identidade única, em várias redes de negócios. O *Composer* suporta protocolos de consenso para garantir que as transações sejam validadas de acordo com a política definida pelos participantes da rede.

A estrutura de um projeto criado no *Composer* é composta por: (i) arquivo com extensão .cto pelo qual os participantes, os ativos e as transações são modelados; (ii) arquivo responsável por definir a lógica de cada transação; (iii) arquivo com a extensão .acl

em que estão as regras de controle de acesso aos recursos; e, por fim (iv) arquivo com a extensão .qry, que define as consultas.

A Figura 3 ilustra o arquivo .cto utilizado na solução proposta. Nele são definidos: os tipos participantes (IES, EE e CRM) com seus atributos, os ativos que serão manipulados por esses participantes (Diploma, Especialidade e Registro Médico) e que tipos de transações podem ser feitas com esses ativos.

Figura 3: Exemplo de arquivo CTO usado na abordagem proposta

```
participant abstract Membro identified by Id {
  o String Id
  o String Nome
  ...

participant IES extends Membro {
  ...
}
participant IE extends Membro {
  ...
}
participant CRM extends Membro {
  o String estado
  ...
}
```

```
asset diploma identified by Id {
  o String Id
  ...
}
asset especialidade identified by Id {
  o String Id
  ...
}
asset registroMedico identified by Id {
  o String Id
  --> asset diploma
  --> asset especialidade
  ...
}
```

```
transaction RegistrarDiploma {
  --> diploma ativo
  ...
}
transaction RegistrarEspecialidade {
  --> especialidade ativo
  ...
}
transaction RegistrarDadosMedicos {
  --> registroMedico ativo
  ...
}
```

Fonte: Autores

Salienta-se que o ativo **registroMedico** pode armazenar os dados do médico e os ponteiros para os ativos Diploma e Especialidade de um profissional. Quanto às transações, cada uma foi definida de modo que um tipo específico de participante possa manipular cada ativo, sendo essa manipulação restringida pelo controle de acesso.

Na Figura 4, demonstram-se as regras de controle de acesso. A primeira regra. **LerDados**, permite que todos os participantes que têm acesso à rede possam apenas ler as informações dos Registros Médicos, sendo bloqueada a possibilidade de escrita ou alteração desses dados. As demais restrições são utilizadas para permitir que apenas os participantes definidos possam realizar operações em recursos específicos – por exemplo, a regra **ManipularDiploma**, que permite que apenas participantes definidos do tipo IES possam utilizar transações do tipo **RegistrarDiploma** e manipular o ativo Diploma.

A Figura 5 mostra um exemplo de arquivo .qry, responsável pelas consultas aos registros dos profissionais médicos. A priori, foram definidos dois tipos de consulta: **todosRegistros**, que retorna um *.json* com todos os registros médicos armazenados na *blockchain* e **registroEspecifico** retorna um *.json* com o registro baseado no Id passado no momento da consulta. Ressalta-se que consultas por outras informações do médico podem ser adicionadas. Por fim, todos os arquivos apresentados são integrados em um arquivo com a extensão .bna que será a entrada do *Fabric*.

Figura 4: Exemplo de ACL usado no Controle de Acesso.

```
rule LerDados {
 description: "Todos os participantes podem ler os dados."
 participant: "crm.*"
 operation: READ
 resource: "crm.*"
 action: ALLOW
}
rule manipularDados {
 description: "Apenas IES manipula dados do Diploma."
 participant: "crm.IES"
 operation: ALL
 resource: "crm.diploma"
 transaction: "crm.RegistrarDiploma"
 action: ALLOW
}
rule ManipularEspecialidade {
 description: "Apenas IE manipula dados de Especialidade."
 participant: "crm.IE"
 operation: ALL
 resource: "crm.especialidade"
 transaction: "crm.RegistrarEspecialidade"
 action: ALLOW
}
rule manipularRegistroMedico {
 description: "Apenas CRM manipula os dados dos Médicos."
 participant: "crm.CRM"
 operation: UPDATE
 resource: "crm.registroMedico"
 transaction: "crm.RegistrarDadosMedicos"
 action: ALLOW
}
```

Fonte: Os Autores.

Figura 5: Exemplos de consultas utilizadas.

```
query todosRegistros {
 description: "Seleciona todos os registros médicos."
 statement:
   SELECT crm.registroMedico
}
query registroEspecifico {
 description: "Seleciona o registro de um médico específico"
 statement:
   SELECT crm.registroMedico
     WHERE (cadId == $id)
}
```

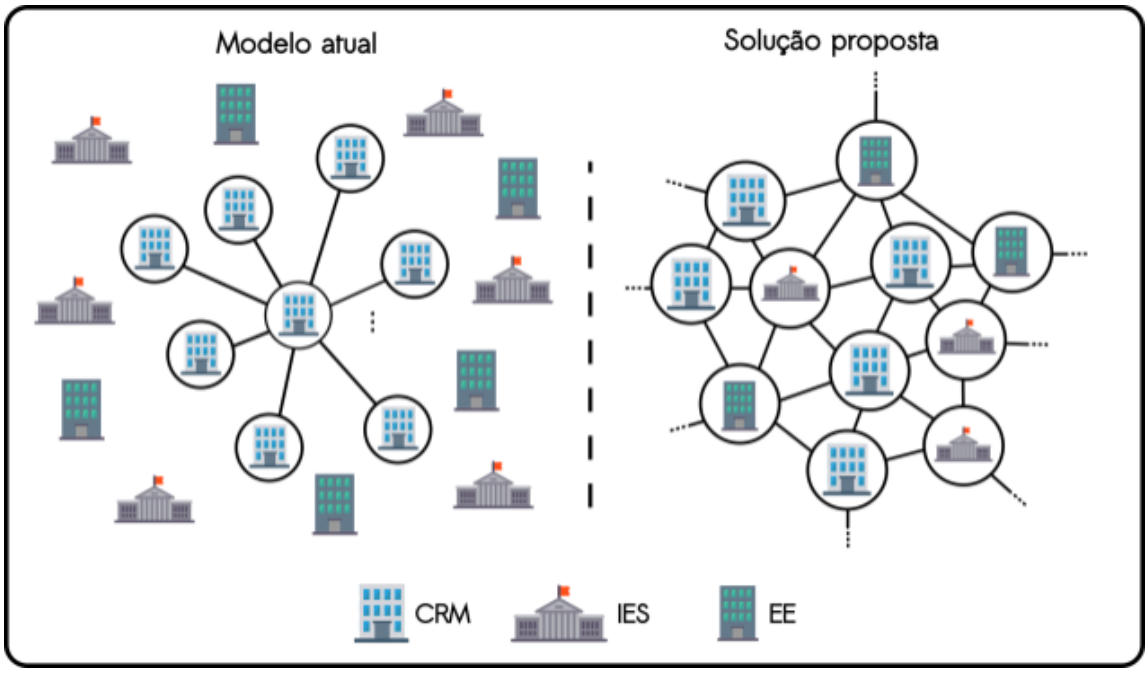
Fonte: Os Autores.

3.2 Vantagens da Solução Proposta

Conforme pode ser observado na Figura 6 (lado esquerdo), o atual modelo de compartilhamento dos dados ocorre de forma que os CRMs transmitam todas as informações de maneira exclusiva para um servidor central. No caso do modelo em questão,

o servidor central está presente no Distrito Federal. Sendo assim, as informações de todos os CRMs estarão reunidas em apenas um único ponto. Caso algum CRM requeira dados de um CRM de outro estado, é necessário fazer as solicitações ao servidor central a fim de obter a informação desejada. Esse modelo pode favorecer a ação de ataques maliciosos, o que pode afetar os dados de toda a rede. Em contrapartida, a solução proposta neste trabalho evita esse tipo de situação, pois os dados são armazenados descentralizadamente, como pode ser visto na Figura 6 (lado direito), o que elimina a necessidade de um servidor central para proteger e autenticar os dados. Cada nó possui uma cópia de todas as informações. Agora as consultas podem ser realizadas ao nó mais próximo, minimizando assim o tempo de resposta para uma consulta junto ao CRM e aos demais participantes da rede (EEs, IESs). Além disso, sistemas distribuídos permitem que os dados sejam recuperados caso um nó sofra alguma falha e perca esses dados.

Figura 6: Contraste entre Modelo Atual e Solução Proposta.



Fonte: Os Autores.

Outra vantagem da solução proposta é a imutabilidade dos dados, pois os blocos de dados, uma vez criados, não podem ser modificados posteriormente. Ou seja, quando os dados são registrados em uma *blockchain*, não é possível removê-los ou alterá-los. Dada essa imutabilidade, o uso de *blockchain* demonstra-se pertinente para viabilizar a rastreabilidade das informações, visto que se pode promover transparência aos dados,

desde a sua concepção até um estado atual. Sendo assim, cada nó pode obter todo o histórico de um médico e, a partir disso, analisá-lo a fim de obter alguma informação relevante.

Além dos benefícios citados previamente, pode-se considerar a automação de grande parte dos processos, principalmente aqueles que necessitam de uma interação entre os diferentes participantes da rede. Tais vantagens influenciam potencialmente na desburocratização de processos internos entre os participantes, assim como na redução de fatores importantes como custos e tempo de atendimento.

Ademais, poderosos mecanismos de consenso da tecnologia *blockchain* garantem que a informação seja inserida apenas quando a maioria dos nós concordam. Tal mecanismo evita que informações não consensuadas sejam adicionadas por pessoas não autorizadas, evitando, assim, possíveis fraudes na manipulação dos dados inseridos.

3.3 Demonstração da Solução

A Figura 7 apresenta os fluxos de processos relacionados ao registro de informações do médico no CRM. Como já mencionado, para o médico exercer legalmente a medicina é necessário que este realize seu registro junto ao CRM de seu diploma devidamente expedido por uma IES e que oferta um curso reconhecido pelo MEC. O processo para realizar outros procedimentos, tais como inscrição secundária, reinscrição, transferência, dentre outros, é semelhante aos passos a seguir quanto ao quesito documentação, no qual o CRM verifica as informações referentes ao diploma e as outras informações necessárias apresentadas e confere a inscrição ao médico.

Figura 7: Fluxo do Registro de Informações Médicas ao CRM.

Fonte: Os Autores.

A partir da Figura 7, verifica-se o desenvolvimento das seguintes ações:

1. A fim de realizar a primeira inscrição, o recém-graduado em medicina depende da emissão de seu diploma pela sua IES. Assim, o início do fluxo de funcionamento da abordagem proposta necessita que a IES registre o diploma na *blockchain*.

2. O médico solicita o registro de sua inscrição ao CRM de acordo com as normas previamente estabelecidas.

3. O CRM verifica a validade do diploma registrado pela IES ou certificados pelas EEs ao consultar a *blockchain*.

4. Após o CRM verificar o registro do diploma na *blockchain*, dados os devidos procedimentos, este registra ou atualiza os dados do médico na *blockchain*. A presente demonstração destaca e detalha outro evento em específico: o registro de especialidades do médico. Esse destaque é dado pelo fato de que tal atividade envolve órgãos terceiros que emitem os certificados e títulos de especialidades, documentos que também precisam ter o devido cuidado quanto à validação de sua vercidade e à integridade das informações. Portanto, sugere-se que, assim como o diploma emitido pela IES, os certificados de

especialidades também sejam registrados na *blockchain*. Os passos a seguir demonstram um cenário de funcionamento da solução para tal fim.

5. As EEs consultam as informações do profissional na *blockchain* com o propósito de verificar o diploma e as informações registradas no CRM.

6. Após verificar se as informações necessárias estão válidas, a instituição de especialidade realiza o registro do certificado de residência médica, caso seja uma instituição credenciada na CNRM ou certificado de prova de título, caso seja uma sociedade filiada à AMB.

7. O médico realiza a solicitação do registro de especialidade de acordo com as normas estabelecidas.

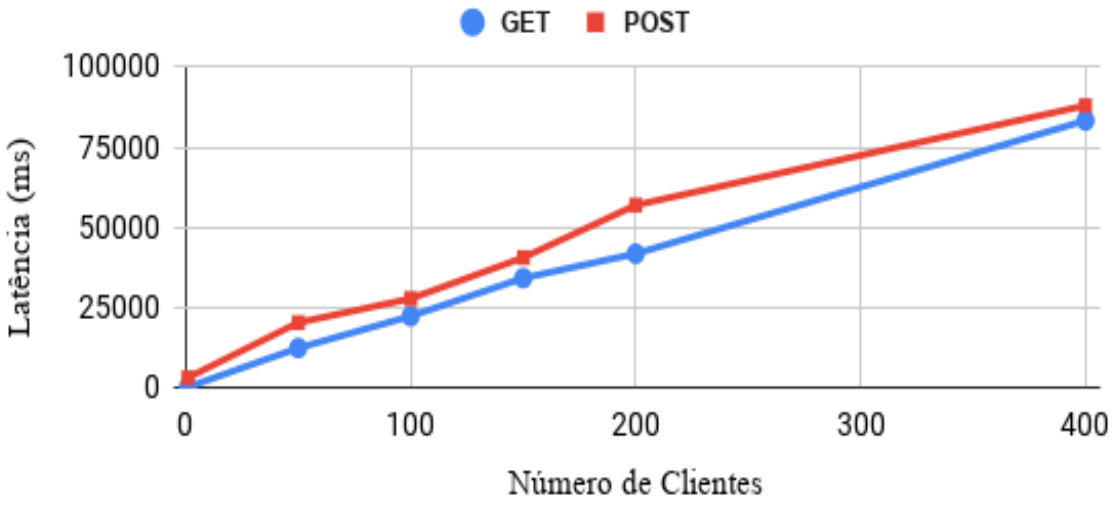
Semelhante ao fluxo de realizar a primeira inscrição, os passos 3 e 4 se repetem após o passo 7, visto que o CRM deve consultar a validade das informações e registrar a especialidade do profissional na *blockchain*. Além dos fluxos apresentados na Figura 6, pode-se considerar o acesso a essas informações pelos próprios profissionais de medicina, visto que estes podem consultar se os documentos oficiais que garantem sua habilitação e cumprimento das exigências necessárias foram adicionados à *blockchain*. Por exemplo, o médico, consultando a plataforma *blockchain* implementada, pode acompanhar se seu diploma foi registrado pela IES, facilitando assim a comunicação entre as partes. Demais detalhes sobre o funcionamento do sistema podem ser encontrados na página de suporte[21] do presente trabalho.

3.4 Avaliação Empírica

3.4.1 Avaliação Quantitativa

Após as configurações necessárias na ferramenta *JMeter*, realizam-se as devidas execuções para a coleta das medidas a serem investigadas. Dessa forma, o desempenho geral do sistema é mostrado na Figura 8. A latência para uma requisição do tipo *GET* para 1 cliente é de 415ms, enquanto a requisição *POST* é de 3352ms. Observa-se que as requisições do tipo *POST* são mais lentas quando comparadas com as requisições do tipo *GET*, e isso pode ser constatado em todos os casos independentemente da variação no "número de clientes". Tal resultado confirmou a hipótese de que as requisições *POST* são mais lentas, pois a atualização do status do livro-razão ocasiona um tempo extra.

Figura 8: Desempenho Geral do Sistema.

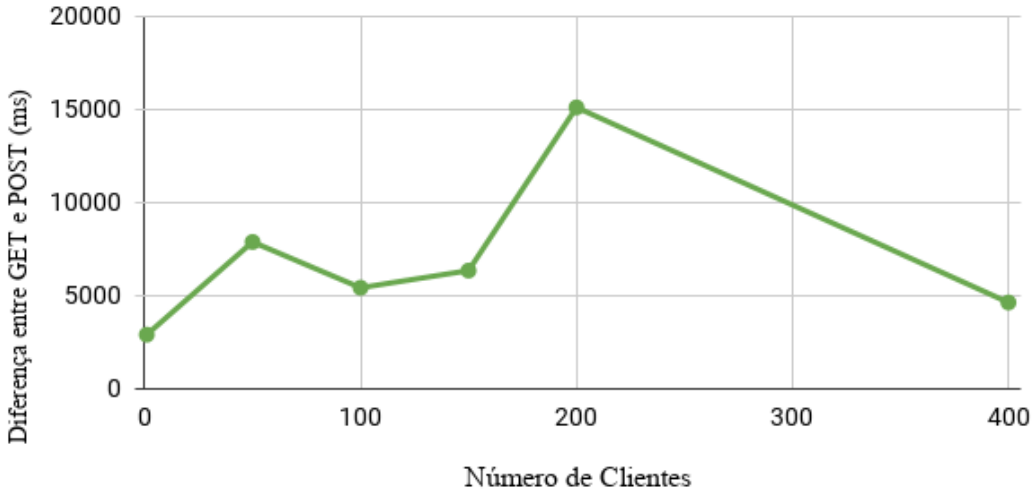


Fonte: Os Autores.

Pode-se perceber também que à medida que o número de clientes cresce, a latência aumenta praticamente linearmente. Para a solicitação *GET*, há um aumento linear quase perfeito na latência a partir de 200 clientes, que aumentou de 57012ms para 83355ms. A solicitação *POST* mostrou uma tendência semelhante, em que a latência aumentou de 3352ms para 88015ms. Assim, pode-se confirmar a segunda hipótese, que à medida que o número de clientes cresce linearmente, o desempenho diminui, ou seja, há um aumento na latência da resposta. Isso, considerando que cada cliente adicional precisa levar uma certa quantidade de tempo e de recursos.

Além disso, a diferença geral entre a requisição *POST* e *GET* é mostrada na Figura 9, encontrada ao subtrair a latência geral das requisições *GET* daquela das requisições de *POST*. A diferença média geral é de aproximadamente 7068ms, com o desvio padrão de aproximadamente 3899ms, sendo, esta, a estimativa de tempo que a *blockchain* leva para gravar informações e alterar o livro-razão. Caso um novo nó seja adicionado, ele funcionará de forma semelhante, pois os diferentes nós são executados paralelamente e independentemente, motivo pelo qual o "número de nós" não foi considerado como uma variável dependente do sistema.

Figura 9: Diferença geral entre as requisições *POST* e *GET*.



Fonte: Os Autores.

As latências de respostas apresentadas são consideráveis. Com o crescente "número de clientes", a latência aumenta, porém com 200 clientes fazendo solicitações paralelamente, o desempenho ainda está abaixo de 1 minuto e com 400 clientes, abaixo de 2 minutos. Isso pode ser adequado para uma rede como o CRM, uma vez que os dados médicos não são adicionados com uma alta frequência. A latência média para o sistema gravar dados em *blockchain* e alterar o livro-razão é inferior a 8 segundos dentro do intervalo de tempo para os clientes testados.

3.4.2 Avaliação Qualitativa

Inicialmente, buscou-se confrontar as respostas obtidas na entrevista quanto ao funcionamento do CRM em relação à base teórica levantada na Seção 1. Conforme explanado pelo participante, constatou-se que os fluxos adotados pelo presente trabalho estão condizentes com os processos realizados na prática pelos CRMs. O entrevistado acrescentou informações sobre a organização do CRM na realização de suas atividades: (i) cartorial; (ii) judicante; (iii) normativa; (iv) fiscalizatória e (v) pedagógica. Em particular, este trabalho foca na função cartorial, responsável pelas atividades de registro profissional do médico.

Visando salientar a importância de uma abordagem descentralizada, investigou-se a atual arquitetura adotada pelo CRM para o armazenamento e o gerenciamento dos dados. Conforme teorizado, o entrevistado enfatizou que os dados são registrados de forma

centralizada. O CRM de cada estado envia os dados para um único banco de dados. Portanto, observa-se a relevância de uma possível solução descentralizada de modo a evitar um único ponto de falha.

Outro ponto relevante é o compartilhamento de informações entre CRM, EE e IES. Segundo o membro da diretoria colegiada, o CRM solicitou maneiras de compartilhamento das informações por parte das entidades emissoras de certificados a fim de realizar verificações no momento do registro. Essas informações seriam, por exemplo, certificações de especialidades recém emitidas pela entidade de especialidade. Como apresentado na Seção 2, a proposta demonstra-se apta em atender esse requisito, haja vista que viabiliza o compartilhamento dos dados.

O entrevistado frisou a segurança como o principal aspecto positivo da abordagem, pois, segundo ele, "*quanto mais mecanismos de segurança 'houverem' que resguardem nossos dados, isso é ótimo*". Porém, como desafio, levantou a questão da operacionalização da proposta: "*essa é a única barreira que eu vejo: você depender de profissionais especializados. Talvez, isso seja um gargalo.*"

4. Considerações Finais

A principal contribuição deste trabalho consiste na proposta e validação do MIRIAM, um sistema baseado em uma *blockchain* permissionada para controle dos registros profissionais de médicos. Destaca-se, ainda, a aderência da solução frente às normas brasileiras estabelecidas para o controle de registros profissionais de médicos. A descrição técnica, por meio do *Hyperledger*, também se revela importante, dado o protagonismo dessa tecnologia para o mercado e academia.

Em termos empíricos, realizou-se um experimento computacional visando analisar o desempenho do sistema o qual evidenciou a viabilidade da solução em diferentes cenários. Conduziu-se também uma entrevista em profundidade com um membro do CREMEC para 1) validar qualitativamente a compreensão dos processos analisados e 2) compreender a aderência da solução em um contexto real. Tal análise, apesar de limitada por apenas uma entrevista em profundidade, atendeu aos atributos essenciais dispostos por Paul *et. al*[25] para entrevistas, como esclarecimento da amostragem, descrição do entrevistado e inclusão de citações diretas.

Quanto aos trabalhos futuros, pretende-se ampliar o escopo de avaliação computacional e investigar melhorias na usabilidade para o sistema.

Referências

1. BRASIL. Resolução CFM Nº 2.217/2018, de 01 nov. de 2018. Aprova o Código de Ética Médica. Brasília, DF, 01 nov. 2018.
2. BRASIL. Lei Nº 2.848/40, de 07 de dezembro de 1940. Código Penal. Brasília, DF, 07 dez. 1940, 1940.
3.De Aguiar, Erikson Júlio, et al. "A survey of blockchain-based strategies for healthcare." ACM Computing Surveys (CSUR) 53.2 (2020): 1-27.
4. Mateus Pires, Daniel Souza, Rostand Costa, and Guido Lemos. Uma abordagem baseada em brokers para registro de transações em múltiplos livros-razão distribuído. In Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain), volume 1. SBC, 2018.
5. Sinclair Davidson, Primavera De Filippi, and Jason Potts. Economics of blockchain. 2016.
6. Hunhevicz, Jens J., and Daniel M. Hall. "Do you need a blockchain in construction? Use case categories and decision framework for DLT design options." Advanced Engineering Informatics 45 (2020): 101094.
7. BRASIL. Lei Nº 3.268/57, de 30 de setembro de 1957. Dispõe sobre os Conselhos de Medicina. Brasília, DF, 30 set. 1957, 1957.
8. BRASIL. Lei Nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do 3º do art. 37 e no 2 º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei Nº 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 jan. 1991; e dá outras providências. Brasília, DF, 18 nov. 2011, 2011.
9. BRASIL. Resolução CFM no 2.180/2018, de 19 de setembro de 2018. Estabelece os dados de médicos que devem ser disponibilizados em consultas eletrônicas relacionadas aos registros dos profissionais médicos inscritos no Sistema Conselhos de Medicina. Brasília, DF, 19 set. 2018, 2018.
10.Khettry, AkashRaj, Karthik R. Patil, and Abhilash C. Basavaraju. "A Detailed Review on Blockchain and Its Applications." SN Computer Science 2.1 (2021): 1-9.
11. Gabriel O Mendanha, Lıvia A Cruz, and Regis P Magalhaes. Data-chain: Uma ferramenta para assegurar a propriedade e imutabilidade de documentos digitais. In 32º Proceedings of Simpósio Brasileiro de Banco de Dados, 2018.
12. ElliAndroulaki, ArtemBarger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, GennadyLaventman, YacovManevich, et al. Hyperledgerfabric: a distributed operating system for permissionedblockchains. In Proceedings of the 13th EuroSys Conference, page 30. ACM, 2018.
13. Rostand Costa, Daniel Faustino, Guido Lemos, Ademir Queiroga, Cláudio Djohnnatha, Felipe Alves, Jordan Lira, and Mateus Pires. Uso não financeiro de blockchain: Um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos. In Anais do I WBlockchain. SBC, 2018.
14. Tim K Mackey and GaurvikaNayyar. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert opinion on drug safety, 16(5):587–602, 2017.
15. Ariel Ekblaw, Asaph Azaria, John D Halamka, and Andrew Lippman. A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference, volume 13, page 13, 2016.

16. Bingqi Liu, Mingzhe Liu, Xin Jiang, Feixiang Zhao, and Ruili Wang. A blockchain-based scheme for secure sharing of x-ray medical images. In International Conference on Security with Intelligent Computing and Big-data Services, pages 29–42. Springer, 2018.
17. YakobUtama Chandra Meyliana, Cadelina Cassandra, Henry Antonius EkaSurjandy, Erick Fernando Widjaja, HarjantoPrabowo, and Charles Joseph. Defying the certification diploma forgery with blockchain platform: a proposed model. In Proceedings of the International Conferences ICT, Society, and Human
Beings 2019; Connected Smart Cities 2019; and Web Based Communities and Social Media 2019, pages 63-71. 2018.
18. JerinasGresch, Bruno Rodrigues, Eder Scheid, Salil S Kanhere, and Burkhard Stiller. The proposal of a blockchain-based architecture for transparent certificate handling. In International Conference on Business Information Systems, pages 185–196. Springer, 2018.
19. BRASIL. Parecer CFM Nº 5/2017. Dispõe sobre os tipos de pós-graduações médicas lato sensu no Brasil. Brasília, DF, 2017.
20. Dmitri Nevedrov. Using JMeter to performance test web services. Published on dev2dev, 2006.
21. MIRIAM - supporting webpage. Disponível em: https://br-miriam.github.io
22. Bowen, G. A. et al. (2009). Document analysis as a qualitative research method. Qualitative research journal, 9(2):27
23. Boyce, Carolyn, and PalenaNeale. "Conductingin-depth interviews: A guide for designing and conductingin-depth interviews for evaluation input." (2006).
24. Hyperledger. An introduction to hyperledger, mar 2019.
25. Ralph, Paul, et al. "ACM SIGSOFT empirical standards." arXivpreprint arXiv:2010.03525 (2020).