



**UNIVERSIDADE ESTADUAL DO CEARÁ  
CENTRO DE CIÊNCIAS E TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO  
MESTRADO ACADÊMICO EM CIÊNCIA DA COMPUTAÇÃO**

**PAMELLA SOARES DE SOUSA**

**UM ESTUDO SOCIOTÉCNICO MULTI-MÉTODO PARA DESENVOLVIMENTO E  
AVALIAÇÃO DE UM PRONTUÁRIO ELETRÔNICO DO PACIENTE BASEADO EM  
BLOCKCHAIN**

**FORTALEZA – CEARÁ  
2021**

## RESUMO

O Prontuário Eletrônico do Paciente (PEP) transformou a forma como as informações clínicas são gerenciadas, facilitando a continuidade do cuidado do paciente e interoperabilidade entre diferentes provedores de saúde. Apesar disso, fazem-se necessárias soluções que propiciem o acesso aberto a dados sensíveis de forma a preservar a privacidade dos pacientes e inviabilizar o uso por terceiros desautorizados. Blockchain mostra-se promissora quando atrelada aos PEPs devido sua capacidade em permitir que partes completamente anônimas e que não confiam entre si formem uma rede que armazena informações confiáveis. Entretanto, identifica-se na literatura uma lacuna quanto ao entendimento sobre o efeito da adoção de *blockchain* no contexto de PEP à luz de construtos colaborativos. Apesar das vantagens, deve-se buscar entender como tais tecnologias podem afetar nas atividades dos indivíduos e/ou de grupos na perspectiva colaborativa. Dessa forma, o presente trabalho apresenta um estudo pautado em uma perspectiva sociotécnica para desenvolvimento e avaliação de uma solução para PEP baseada em *blockchain* pela qual o paciente pode compartilhar seus dados médicos com diferentes entidades de forma segura. Procura-se ademais adequar a proposta sob o contexto brasileiro de forma a discutir a conformidade de tal solução frente aos requisitos definidos pela Sociedade Brasileira de Informática em Saúde (SBIS) e da Lei Geral de Proteção de Dados (LGPD). Por meio das avaliações realizadas, foi possível obter uma análise do arcabouço regimental para adequação do uso de blockchain em PEPs e, a partir das delimitações identificadas, a formalização da proposta de uma arquitetura e a implementação de uma Prova de Conceito representativa. Adicionalmente, o uso de uma metodologia sociotécnica permitiu promover, através de Grupos Focais, uma discussão e identificação de temas relevantes sobre aspectos colaborativos na integração de PEPs e *blockchain*.

**Palavras-chave:** PEP. Blockchain. Abordagem Sociotécnica.

## ABSTRACT

The Electronic Patient Record (EPR) has transformed how clinical information is managed, facilitating the continuity of patient care and interoperability among different healthcare providers. Despite this, solutions are needed that provide open access to sensitive data to preserve the privacy of patients and make it unfeasible to use by unauthorized third parties. Blockchain shows promise when coupled with EPRs because it allows completely anonymous and distrusting parties to form a network that stores trusted information. However, a gap is identified in the literature regarding the understanding of the effect of blockchain adoption in EPR in the light of collaborative constructs. Despite the advantages, one must seek to understand how such technologies can affect the activities of individuals and/or groups in a collaborative perspective. Thus, the present work presents a study based on a socio-technical perspective for developing and evaluating a blockchain-based EPR solution through which patients can share their medical data with different entities in a secure manner. It also seeks to adapt the proposal under the Brazilian context to discuss the compliance of such a solution against the requirements defined by the Brazilian Society of Health Informatics (in Portuguese, SBIS, Sociedade Brasileira de Informática em Saúde) and the Brazilian General Data Protection Act (in Portuguese, LGPD, Lei Geral de Proteção de Dados). Through the evaluations carried out, it was possible to obtain an analysis of the regimental framework for the adequacy of the use of blockchain in EPRs and, from the identified boundaries, the formalization of the proposal for architecture and the implementation of a representative Proof of Concept. Additionally, using a socio-technical methodology allowed promoting, through Focus Groups, a discussion and identification of relevant themes about collaborative aspects in the integration of EPRs and blockchains.

**Keywords:** EPR. Blockchain. Sociotechnical Approach.

## LISTA DE ILUSTRAÇÕES

<b>Figura 1 – Representação simplificada de uma <i>blockchain</i>.</b>	21
<b>Figura 2 – Funcionamento básico de uma <i>blockchain</i>.</b>	23
<b>Figura 3 – Categorias de Recursos do FHIR.</b>	34
<b>Figura 4 – Arquitetura lógica do FHIR.</b>	34
<b>Figura 5 – Modelo 3C de Colaboração.</b>	36
<b>Figura 6 – Procedimentos Metodológicos baseados em Design Science Research.</b>	46
<b>Figura 7 – Fluxo da Avaliação Social.</b>	50
<b>Figura 8 – Caracterização dos Participantes.</b>	51
<b>Figura 9 – Passos do Processamento de Dados do Grupo Focal.</b>	52
<b>Figura 10 – Visão Geral da Arquitetura de Software.</b>	57
<b>Figura 11 – IDE Remix e o Contrato Inteligente em Solidity</b>	60
<b>Figura 12 – Conexão com a <i>blockchain</i> utilizando <i>Web3.js</i></b>	61
<b>Figura 13 – Chamada da função incluirPosse por meio da <i>Web3.js</i></b>	62
<b>Figura 14 – Modelagem Relacional baseada no FHIR.</b>	64
<b>Figura 15 – Keyspace medical_record.</b>	65
<b>Figura 16 – Conectando ao Apache Cassandra pelo Node.js Driver.</b>	65
<b>Figura 17 – Inserção com Node.js Driver ao BDD Cassandra.</b>	66
<b>Figura 18 – Leitura com Node.js Driver ao BDD Cassandra.</b>	66
<b>Figura 19 – Remoção com Node.js Driver ao BDD Cassandra.</b>	66
<b>Figura 20 – Tela de Cadastro do PS.</b>	69
<b>Figura 21 – Tela de Cadastro do LM e da IS.</b>	69
<b>Figura 22 – Tela de Cadastro do Registro de Anamnese.</b>	70
<b>Figura 23 – Tela de Cadastro do Registro de Observação.</b>	70
<b>Figura 24 – Tela de Cadastro do Registro de Exame.</b>	71
<b>Figura 25 – Tela de Cadastro do Registro de Medicação.</b>	71
<b>Figura 26 – Tela de Listagem de Pacientes.</b>	72
<b>Figura 27 – Tela de Listagem de Registros.</b>	72
<b>Figura 28 – Tela de Cadastro do Paciente.</b>	73
<b>Figura 29 – Tela de Registros do Paciente.</b>	73
<b>Figura 30 – Tela de ES autorizadas.</b>	74

<b>Figura 31 – Demonstração da Abordagem.</b>	74
<b>Figura 32 – Configurações do Experimento.</b>	91
<b>Figura 33 – Tempo de Publicação.</b>	92
<b>Figura 34 – Tempo de Busca.</b>	94

## **LISTA DE QUADROS**

<b>Quadro 1 – Principais componentes dos diferentes tipos de <i>blockchain</i>.</b> . . . . .	27
<b>Quadro 2 – Tabela comparativa dos trabalhos relacionados.</b> . . . . .	42
<b>Quadro 3 – Perspetiva Tecnológica.</b> . . . . .	57
<b>Quadro 4 – Subconjunto dos potenciais requisitos impactados pelas es- tratégias utilizadas.</b> . . . . .	77
<b>Quadro 5 – Subconjunto dos potenciais princípios impactados pelas es- tratégias utilizadas.</b> . . . . .	85
<b>Quadro 6 – Procedimentos de Coletas das Métricas</b> . . . . .	91
<b>Quadro 7 – Ocorrência de Subtemas nos Grupos Focais.</b> . . . . .	96

## LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
API	<i>Application Programming Interface</i>
BDD	Banco de Dados Distribuído
CSCW	<i>Computer Supported Cooperative Work</i>
CSV	<i>Comma-Separated Values</i>
DHT	<i>Distributed Hash Table</i>
DSR	<i>Design Science Research</i>
EHR	<i>Electronic Health Record</i>
ES	Entidade de Saúde
EVM	<i>Ethereum Virtual Machine</i>
FHIR	<i>Fast Healthcare Interoperability Resources</i>
GDPR	<i>General Data Protection Regulation</i>
GF	Grupo Focal
HIPAA	Lei de Portabilidade e Responsabilidade de Seguros de Saúde
HL7	<i>Health Level Seven International</i>
ICP	Infraestrutura de Chaves Públicas
IPFS	<i>InterPlanetary File System</i>
IS	Instituição de Saúde
LGPD	Lei Geral de Proteção de Dados
LM	Laboratório Médico
NGS1	Nível de Garantia de Segurança 1
NGS2	Nível de Garantia de Segurança 2
NSA	<i>National Security Agency</i>
ONC	<i>Office of the National Coordinator for Health Information Technology</i>
P2P	<i>Peer-to-peer</i>
PBFT	<i>Practical Byzantine Fault Tolerance</i>
PEP	Prontuário Eletrônico do Paciente
PoC	<i>Proof-of-Concept</i>
PoS	<i>Proof of Stake</i>
PoW	<i>Proof of Work</i>
PS	Profissional de Saúde

S-RES	Sistema de Registro Eletrônico de Saúde
SBIS	Sociedade Brasileira de Informática em Saúde
TCLE	Termo de Consentimento Livre e Esclarecido
UE	União Européia
UX	<i>User eXperience</i>
VM	<i>Virtual Machine</i>

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	15
<b>1.1</b>	<b>Objetivos</b>	18
1.1.1	Objetivo Geral	18
1.1.2	Objetivos Específicos	18
<b>1.2</b>	<b>Estrutura do Trabalho</b>	18
<b>2</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b>	20
<b>2.1</b>	<b>Blockchain</b>	20
2.1.1	Algoritmos de Consenso	24
2.1.2	Tipos de Blockchains	26
<b>2.2</b>	<b>Contratos Inteligentes e Decentralized Applications (dApps)</b>	27
<b>2.3</b>	<b>Escalabilidade em Blockchains</b>	29
<b>2.4</b>	<b>Prontuário Eletrônico do Paciente (PEP)</b>	31
<b>2.5</b>	<b>Computer Supported Cooperative Work (CSCW)</b>	35
<b>2.6</b>	<b>Conclusões do Capítulo</b>	37
<b>3</b>	<b>TRABALHOS RELACIONADOS</b>	39
<b>3.1</b>	<b>Conclusões do Capítulo</b>	43
<b>4</b>	<b>PROCEDIMENTOS METODOLÓGICOS</b>	45
<b>4.1</b>	<b>Caracterização da Pesquisa</b>	45
<b>4.2</b>	<b>Design das Avaliações</b>	47
4.2.1	Avaliação Técnica	47
4.2.2	Avaliação Social	49
<b>4.2.2.1</b>	<b>Análise dos Dados do Grupo Focal</b>	52
<b>4.3</b>	<b>Conclusões do Capítulo</b>	53
<b>5</b>	<b>SOLUÇÃO PROPOSTA</b>	54
<b>5.1</b>	<b>Papéis envolvidos na solução</b>	54
<b>5.2</b>	<b>Ativos e seu armazenamento na rede</b>	55
<b>5.3</b>	<b>Arquitetura de Software e Implementação</b>	56
5.3.1	Camada Armazenamento <i>On-chain</i>	58
5.3.2	Camada de Armazenamento <i>Off-chain</i>	62
5.3.3	Camada de Aplicação	66
<b>5.3.3.1</b>	<b>Interface de Usuário</b>	68

5.3.3.1.1	<i>Visão das Entidades de Saúde</i> . . . . .	68
5.3.3.1.2	<i>Visão do Paciente</i> . . . . .	72
5.3.4	Demonstração do Workflow Ilustrativo . . . . .	74
<b>5.4</b>	<b>Conclusões do Capítulo</b> . . . . .	75
<b>6</b>	<b>AVALIAÇÃO TÉCNICA</b> . . . . .	76
<b>6.1</b>	<b>Avaliação de Aderência aos Requisitos advindos de Normas Técnicas Nacionais</b> . . . . .	76
6.1.1	Requisitos de Conformidade segundo a Certificação da SBIS . . . . .	76
<b>6.1.1.1</b>	<b><i>Identificação e autenticação de pessoas / Autorização e controle de acesso / Privacidade / Atores</i></b> . . . . .	78
<b>6.1.1.2</b>	<b><i>Disponibilidade do RES</i></b> . . . . .	79
<b>6.1.1.3</b>	<b><i>Problemas/condições de saúde e outras questões / Médico-legal</i></b> . . . . .	80
<b>6.1.1.4</b>	<b><i>Dados clínicos / Gerais</i></b> . . . . .	81
<b>6.1.1.5</b>	<b><i>Segurança de Dados</i></b> . . . . .	82
<b>6.1.1.6</b>	<b><i>Autenticação de usuário utilizando certificado digital / Digitalização de documentos</i></b> . . . . .	82
<b>6.1.1.7</b>	<b><i>Escalabilidade e performance (FUNC.12)</i></b> . . . . .	83
6.1.2	Requisitos de Conformidade segundo a Lei Geral de Proteção de Dados	83
<b>6.1.2.1</b>	<b><i>Minimização de dados pessoais / Anonimização / Limitação de armazenamento</i></b> . . . . .	85
<b>6.1.2.2</b>	<b><i>Integridade e Confidencialidade / Consentimento</i></b> . . . . .	86
<b>6.1.2.3</b>	<b><i>Direito ao esquecimento</i></b> . . . . .	87
<b>6.1.2.4</b>	<b><i>Direito de acesso / Direito à informação / Portabilidade dos dados / Identificação dos responsáveis pelo tratamento</i></b> . . . . .	88
<b>6.2</b>	<b>Avaliação de Desempenho</b> . . . . .	89
6.2.1	Configurações do Experimento Computacional . . . . .	90
6.2.2	Resultados e Análises . . . . .	92
<b>6.2.2.1</b>	<b><i>Tempo de Publicação</i></b> . . . . .	92
<b>6.2.2.2</b>	<b><i>Tempo de Busca</i></b> . . . . .	93
<b>6.3</b>	<b>Conclusões do Capítulo</b> . . . . .	95
<b>7</b>	<b>AVALIAÇÃO SOCIAL</b> . . . . .	96
<b>7.1</b>	<b>O uso atual de PEPs pelos profissionais de saúde</b> . . . . .	96
<b>7.2</b>	<b>Modelo 4C de Colaboração</b> . . . . .	99

7.3	<b>PEP baseado em Blockchain</b> . . . . .	102
7.4	<b>Melhoria na Qualidade</b> . . . . .	105
7.5	<b>Lições Aprendidas e Oportunidades</b> . . . . .	106
7.6	<b>Conclusão do Capítulo</b> . . . . .	109
8	<b>AMEAÇAS À VALIDADE</b> . . . . .	112
9	<b>CONSIDERAÇÕES FINAIS</b> . . . . .	114
9.1	<b>Contribuições</b> . . . . .	114
9.2	<b>Limitações</b> . . . . .	115
9.3	<b>Trabalhos Futuros</b> . . . . .	116
	<b>REFERÊNCIAS</b> . . . . .	118
	<b>APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO</b> . . . . .	130
	<b>APÊNDICE B – FORMULÁRIO DE CARACTERIZAÇÃO DOS PAR-TICIPANTES</b> . . . . .	131
	<b>APÊNDICE C – CENÁRIO 1 DO EXPERIMENTO SOCIAL</b> . . . . .	132
	<b>APÊNDICE D – CENÁRIO 2 DO EXPERIMENTO SOCIAL</b> . . . . .	133
	<b>APÊNDICE E – CENÁRIO 3 DO EXPERIMENTO SOCIAL</b> . . . . .	134
	<b>APÊNDICE F – CENÁRIO 4 DO EXPERIMENTO SOCIAL</b> . . . . .	135
	<b>APÊNDICE G – QUESTÕES DO GRUPO FOCAL</b> . . . . .	136

## 1 INTRODUÇÃO

A Sociedade Brasileira de Informática em Saúde (SBIS) salienta que o prontuário em papel apresenta uma série de dificuldades como, por exemplo, disponibilidade a uma pessoa por vez, baixa mobilidade, ilegibilidade, ambiguidade/perda de informações e que sua guarda requer amplos espaços em serviços de arquivamentos (SBIS, 2012). A partir dessas limitações, deu-se início ao desenvolvimento do Prontuário Eletrônico do Paciente (PEP), uma estrutura para manutenção da informação eletrônica sobre o estado de saúde do indivíduo e os cuidados recebidos durante sua vida (MAS-SAD et al., 2003). Portanto, o PEP registra todas as informações indispesáveis para a comunicação da equipe multiprofissional e o paciente (LAHM; CARVALHO, 2015).

Além da finalidade de armazenamento, a garantia da continuidade do cuidado e do gerenciamento das unidades de saúde, os dados armazenados no PEP podem ser utilizados como fonte para estudos de extração de conhecimento, demandando, assim, interoperabilidade. Tal característica é fundamental para a comunicação adequada entre diferentes sistemas de saúde e profissionais da saúde. Outro requisito que se revela crítico é a garantia da privacidade quanto aos dados dos pacientes (RICARTE, 2019) alicerçado pela Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018). Conforme destacado por Conceição et al. (2018), a questão principal é como prover acesso aberto a dados sensíveis de modo que preserve a privacidade e anonimidade dos pacientes, assim como evitar o uso desautorizado de terceiros. Sendo o PEP de tamanha relevância, diversas inovações têm sido propostas visando a qualificação dos processos de atendimento ao paciente (MARTINS et al., 2019).

Diante das referidas particularidades, a tecnologia *blockchain* demonstra-se promissora para o contexto de PEP devido à viabilização de partes completamente anônimas e que não confiam entre si formar uma rede que armazena informações confiáveis (WÜST; GERVAIS, 2018). Em termos genéricos, o *blockchain* pode ser entendido como um banco de dados distribuído, protegido por criptografia e governado por um mecanismo de consenso (BECK et al., 2017), ou seja, é essencialmente um registro de eventos digitais altamente transparente, seguro e resiliente. Tal tecnologia introduz elementos eficazes para a implementação de um sistema no qual pode-se haver consenso entre diferentes participantes desconhecidos, além da garantia de auditabilidade, autenticidade, disponibilidade, não repudiabilidade e integridade das

transações validadas e armazenadas no livro-razão distribuído. Estas propriedades contribuem para um sistema de informação em saúde seguro e confiável.

Com o apoio de *blockchain*, as pessoas, as instituições e os diferentes setores, colaboram entre si para a solução de diferentes problemas, sendo possível a criação dos atuais espaços sociais para o trabalho por meio de sistemas colaborativos. Especificamente, a área de Trabalho Cooperativo Suportado por Computador (inglês *Computer Supported Cooperative Work* ou CSCW) conceitua a construção de sistemas que atendem tanto o ponto de vista da tecnologia, quanto aos efeitos psicológicos, sociais e organizacionais do trabalho em grupo (COSTA; PIMENTEL, 2011). Nesse sentido, sabe-se que a adoção de novas tecnologias, como *blockchain*, pode transformar, de forma significativa, as várias dimensões de um contexto real da sociedade (PRINZ, 2018). Conforme Cukierman et al. (2007), tais mudanças afetam as relações e comunicações interpessoais, desde negócios até questões políticas. Apesar da relevância e impactos de tais influências, a adoção de *blockchain* no contexto de PEP tem sido avaliada apenas sob o ponto de vista técnico, denotando, assim, uma escassez de estudos que buscam compreender os relevantes efeitos da tecnologia sobre as pessoas, de forma individual e coletiva.

Para mitigar tal lacuna, a abordagem sociotécnica se demonstra relevante, pois, além de se preocupar com o viés tecnológico, considera o contexto de trabalho no processo de desenvolvimento e como usuários são impactados ao interagirem com a tecnologia (MORAES et al., 2019). Dessa forma, ao fundamentar-se numa perspectiva sociotécnica, torna-se possível, por exemplo, concretizar análises sobre o atendimento dos pilares de comunicação, coordenação, cooperação e colaboração entre os usuários (COSTA et al., 2014), elementos estes especialmente relevantes no contexto do compartilhamento das informações médicas através do PEP.

Ao investigar a literatura, constatou-se que, de fato, já existem propostas baseadas em *blockchain* que lidam com gerenciamento de registros médicos (CONCEIÇÃO et al., 2018; QUEIROZ et al., 2018). Todavia, foram identificadas lacunas no que se refere à propostas que se adequam ao contexto brasileiro quanto ao desenvolvimento de um PEP. Além disso, percebeu-se que os referidos trabalhos não investigam como os PEPs atrelados ao uso da tecnologia *blockchain* podem impactar em questões colaborativas, tanto no âmbito organizacional como entre as pessoas. Dessa forma, observou-se a oportunidade de se arquitetar soluções baseadas em *blockchain* em

conformidade aos requisitos especificados pela SBIS e às leis referentes à gerência e proteção dos dados do paciente, como a LGPD. Outrossim, faz-se necessário o entendimento em como, de fato, tais tecnologias afetam na interação e desempenho entre os profissionais de saúde. Sobretudo, para que tais achados guiem o desenvolvimento e avaliação desses sistemas, já que são usados por pessoas. Adicionalmente, ao se arquitetar propostas de PEP, faz-se necessária a adoção de estratégias tecnológicas para compor a estrutura e atender aos requisitos necessários para a sua construção.

Ademais, é crescente o volume de informações clínicas transacionadas e armazenadas nos bancos de dados das instituições de saúde. Os sistemas de informação em saúde precisam ser capazes de processar grandes quantidades de dados sem deixar o usuário à espera (BACELAR; CORREIA, 2015), considerando sempre a performance e a escalabilidade adequadas. Porém, verifica-se que um dos desafios do *blockchain* ainda é a escalabilidade (KOTESKA et al., 2017). Em um cenário de saúde em larga escala, quando *blockchain* é usado como um banco de dados para armazenar dados clínicos paciente, milhões de registros podem ser replicados em todos os participantes do *blockchain* (AGBO et al., 2019).

Portanto, este trabalho tem como foco propor uma arquitetura que atenda aos requisitos necessários para o desenvolvimento de um PEP no cenário brasileiro de forma a respeitar os requisitos definidos pela SBIS e da LGPD, incluindo normas e resoluções vigentes (MIRANDA et al., 2019), bem como destacar as potencialidades, e desafios atrelados ao uso de *blockchain* no domínio sob análise e sua utilização do ponto de vista colaborativo. Adicionalmente, pretende-se utilizar de estratégias tecnológicas necessárias na composição da arquitetura a fim de atender tais demandas, como a adoção de uma estratégia *off-chain* e o funcionamento das camadas de software.

Assim, para formalização de tal arquitetura, este trabalho se baseou em uma metodologia multi-método, guiado por um escopo sociotécnico e alicerçado por *Design Science Research* (DSR) (VAISHNAVI; KUECHLER, 2004), para nortear o desenvolvimento e a avaliação de uma solução baseada em *blockchain* que possibilita o paciente compartilhar seus dados com profissionais da saúde de forma a propiciar diferentes interações entre as partes. As etapas do DSR no desenvolvimento deste trabalho iniciaram-se no levantamento bibliográfico para conscientização do problema, perpassando pela modelagem e desenvolvimento da solução até as avaliações técnicas

e sociais.

## 1.1 Objetivos

### 1.1.1 Objetivo Geral

Este trabalho tem como objetivo investigar, através de uma metodologia sociotécnica multi-método, uma proposta de solução de software para integração de *blockchain* no contexto de Prontuário Eletrônico do Paciente para permitir o controle de acesso e compartilhamento de registros médicos entre diferentes entidades de saúde.

### 1.1.2 Objetivos Específicos

Em relação aos objetivos específicos, pretende-se:

- a) Projetar uma arquitetura para um Prontuário Eletrônico do Paciente baseada em *blockchain* sob o contexto brasileiro;
- b) Implementar uma Prova de Conceito (PoC, do inglês *Proof-of-Concept*) baseada na arquitetura modelada;
- c) Implementar técnicas de armazenamento *off-chain* a fim de amenizar os desafios de escalabilidade;
- d) Avaliar a conformidade de tal solução frente aos requisitos, normas e resoluções vigentes definidos pela certificação da SBIS e LGPD;
- e) Avaliar o desempenho da arquitetura proposta conforme as métricas utilizadas em sistemas *blockchain*;
- f) Avaliar os aspectos colaborativos da solução através de Grupos Focais (GF) e interação com o artefato proposto.

## 1.2 Estrutura do Trabalho

O trabalho está organizado em nove capítulos, incluindo a presente Introdução. Desse modo, os demais capítulos são resumidos abaixo:

- a) **Capítulo 2 - Fundamentação Teórica:** Primeiramente, os conceitos gerais sobre a tecnologia *blockchain* são apresentados, incluindo sua história e suas características. Além disso, a descrição de suas particularidades, como estrutura e algoritmos que servem de base para seu

funcionamento. Tem-se também a descrição de componentes essenciais para sua aplicação, como os contratos inteligentes e os diferentes tipos de *blockchains*. Além disso, foi apresentado um dos desafios que *blockchains* enfrenta, o qual também será avaliado no presente trabalho. Conceitos básicos sobre o PEP e do FHIR foram mostrados, este último um padrão de interoperabilidade. Por fim, uma breve explanação sobre sistemas colaborativos foi apresentada.

- b) **Capítulo 3 - Trabalhos Relacionados:** são apresentados os principais trabalhos relacionados sobre as abordagens propostas de PEPs.
- c) **Capítulo 4 - Procedimentos Metodológicos:** as características da pesquisa e o fluxo das etapas guiadas pelo método DSR são apresentados, incluindo detalhes dos processos nas avaliações social e técnica.
- d) **Capítulo 5 - Solução Proposta:** são apresentadas as definições de papéis participantes da rede, assim como sobre o ativo a ser armazenado. Tem-se uma visão geral da arquitetura de software proposta e sua implementação, a qual está sendo dividida em três camadas que foram projetadas para adequar-se aos requisitos levantados para a adequação ao contexto brasileiro. Ao final, foi apresentado um fluxo ilustrativo.
- e) **Capítulo 6 - Avaliação Técnica:** foram analisadas as estratégias utilizadas frente aos requisitos previamente extraídos do Manual de Certificação da SBIS (2019) e da LGPD. Adicionalmente, o desempenho da solução foi analisado com algumas métricas.
- f) **Capítulo 7 - Avaliação Social:** foram descritos e analisados os temas e subtemas identificados na discussão dos participantes envolvidos nos GFs executados.
- g) **Capítulo 8 - Ameaças à Validade:** as possíveis ameaças que poderiam comprometer a validade do presente trabalho foram elencadas.
- h) **Capítulo 9 - Considerações Finais:** foram discutidas as contribuições do presente estudo, suas limitações e futuros trabalhos.

## 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, serão apresentados alguns conceitos fundamentais deste trabalho. Inicialmente, na Seção 2.1 será introduzida a definição de *blockchain*, a sua história iniciando-se pela criação do Bitcoin e as motivações para seu surgimento, como o Problema dos Generais Bizantinos e do Gasto Duplo. Além disso, foram apresentados os componentes da estrutura de uma *blockchain* genérica e sobre seu funcionamento. A partir disso, algumas das características da *blockchain* foram elencadas. Os algoritmos de consenso, cerne do funcionamento da *blockchain*, foram descritos na Seção 2.1.1. A Seção 2.1.2 apresenta os diferentes tipos de *blockchains*. Em seguida (Seção 2.2), foram apresentados conceitos sobre os elementos que possibilitaram a ampliação do uso de *blockchain* para diferentes domínios além do financeiro, os contratos inteligentes e as aplicações descentralizadas. O desafio de escalabilidade em *blockchains* foi explanado na Seção 2.3. Na Seção 2.4, são apresentados os conceitos gerais sobre o PEP e os conceitos básicos do padrão de interoperabilidade, o FHIR. Por fim, uma breve explanação sobre sistemas colaborativos é apresentada na Seção 2.5.

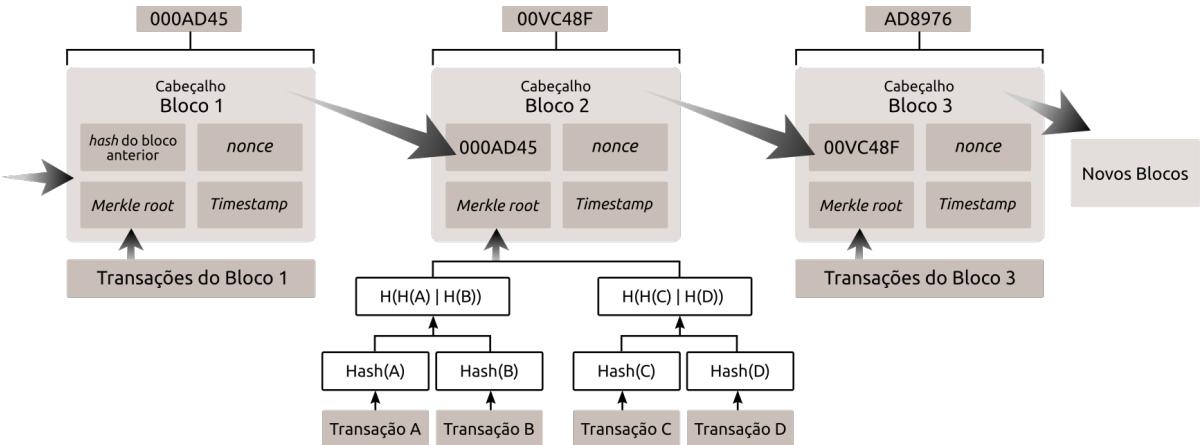
### 2.1 Blockchain

Blockchain é uma rede *peer-to-peer* (P2P) constituída por um livro-razão distribuído (ou *ledger* distribuído) que armazena transações somente por meio de consenso da rede e que, juntamente com uso de criptografia, contratos inteligentes e outros componentes, torna-se uma rede segura e confiável (ACHARYA et al., 2019). Segundo Xu et al. (2019), um livro-razão distribuído é uma estrutura que armazena transações “*append-only*”, ou seja, realiza apenas operações de inserção, não sendo possíveis alterações ou deleções de dados já armazenados entre diferentes máquinas. Por sua vez, a *blockchain*, um tipo de livro-razão distribuído, organiza essas transações ordenadas em blocos que são encadeados por meio de *hashes* criptográficos para assegurar proteção do link de um bloco para seu antecessor.

A estrutura do *blockchain* funciona como uma cadeia de blocos composto por transações, armazenados sequencialmente, de modo que cada novo bloco validado é interligado com o último bloco adicionado à rede através de *hash* criptográfico. Como apresentado na Figura 1, cada bloco é vinculado ao bloco anterior por meio desse *hash* criptográfico que, por sua vez, é determinado pelo conteúdo do bloco individual e o

*hash* criptográfico do bloco anterior (MÖLKEN, 2018). Isso proporciona a integridade e imutabilidade das informações, visto que qualquer modificação invalidaria a cadeia de blocos (WÜST; GERVAIS, 2018).

**Figura 1 – Representação simplificada de uma *blockchain*.**



Fonte: Adaptado de Rocha et al. (2021).

No caso da tecnologia Bitcoin, o primeiro bloco que compõe uma Blockchain é denominado de bloco *genesis*. Como pode ser visto na Figura 1, o bloco é formado por um conjunto de transações que são organizadas em uma estrutura de dados definida como ***Merkle Tree***. Em tal estrutura, as transações são agrupadas em pares e o *hash* de cada uma das transações são armazenadas em um nó pai. Da mesma forma, os nós pais são agrupados em pares e seus respectivos *hashes* armazenados em um nível acima da árvore. Isso ocorre sucessivamente até o nó raiz da *Merkle Tree* (NARAYANAN et al., 2016). Assim, o apontador *hash* da *Merkle Tree*, composta pelas transações, é armazenado no cabeçalho do bloco.

Além disso, o bloco contém um valor denominado *nonce* que é um número a ser descoberto através da resolução de um enigma computacional para fins de validação do bloco, o *hash* do bloco anterior, e o *timestamp*, que é o tempo aproximado de criação deste bloco (segundos do *Unix Epoch*) (ANTONOPoulos, 2014). Ressalta-se que tal representação da *blockchain* está sendo generalizada, visto que diferentes tipos de blockchains podem conter metadados específicos a depender dos algoritmos utilizados. Para blockchains que utilizam o algoritmo Prova de Trabalho (PoW, do inglês *Proof-of-Work*), por exemplo, tem-se também o campo *dificuldade alvo*.

A tecnologia Blockchain foi introduzida em 2008 com a criação do Bitcoin por Satoshi Nakamoto que publicou um artigo seminal intitulado “*Bitcoin: A peer-to-*

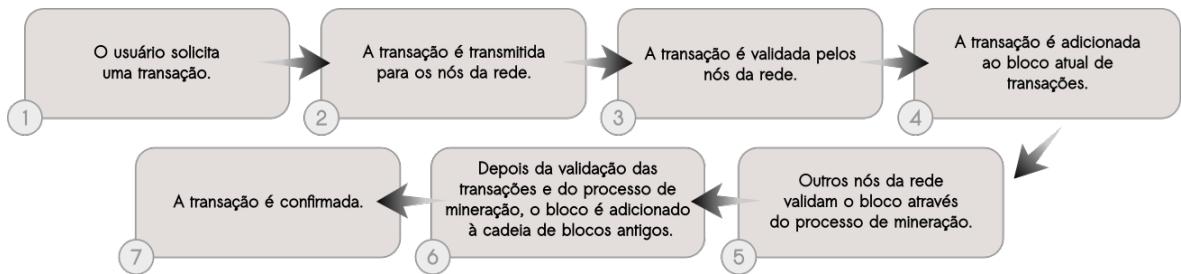
*peer electronic cash system*" (NAKAMOTO, 2008), o qual, no ano seguinte (2009), logo começou a ser operacionalizado. O Bitcoin tem como ideia principal uma moeda eletrônica que pode ser transacionada em uma rede P2P sem a necessidade de uma autoridade intermediária para realizar a transferência de pagamentos entre os pares (BASHIR, 2017). Tal característica foi possível graças à combinação das técnicas e algoritmos que fundamentam a tecnologia *blockchain*, pois o envio de transações sem a necessidade de uma autoridade central somente pode ser realizada através de consenso da maioria dos nós da rede. Em suma, por meio de um protocolo de consenso bizantino baseado em desafios criptográficos, os nós da rede irão decidir a ordem em que as transações serão realizadas e armazenadas de forma permanente na *blockchain* (GREVE et al., 2018).

Além da eliminação de uma autoridade centralizadora, o uso da tecnologia Blockchain como base para o desenvolvimento da criptomoeda Bitcoin, teve o objetivo de solucionar o problema denominado de "Gasto Duplo" o qual ocorre quando uma mesma quantia monetária é utilizada em transações financeiras diferentes (LUCENA; HENRIQUES, 2016). Segundo Nakamoto (2008), para confirmar a validade das transações de forma a mitigar o problema do Gasto Duplo sem a necessidade de um intermediário confiável, "as transações precisam ser publicamente anunciadas" através de "um sistema em que os participantes concordem em um único histórico da ordem em que elas foram recebidas". A rede Bitcoin protege-se contra esse problema através da verificação de cada transação com a utilização de Algoritmos de Consenso, os quais serão explanados em seções seguintes do presente trabalho.

A Figura 2 apresenta um fluxo simplificado do funcionamento de uma *blockchain*. No passo 1, quando um usuário armazenar dados ou trocá-los com outro usuário na *blockchain*, é necessário que ele submeta uma transação para a rede. Tal transação pode conter a ação que deve ser executada e o ativo a ser transferido (MÖLKEN, 2018). Além disso, envolve a assinatura digital do emissor e o endereço do receptor. A transação é transmitida (*broadcast*) para todos os nós ativos da rede P2P (Passo 2) que, no Passo 3, é validada localmente pelos nós. Esta validação é baseada em um conjunto de regras da rede que podem envolver, por exemplo, a verificação das assinaturas, confirmação de valores de *hashes* de transações anteriores referenciadas, etc. Em cada nó, as transações que forem validadas conforme as regras ficarão pendentes em uma fila de transações. No Passo 4, estas transações serão combinadas

criptograficamente em um bloco atual de transações. Similarmente ao ocorrido com as transações, no Passo 5, os blocos também são transmitidos para os nós da rede os quais deverão validar o bloco através do processo de mineração (ou Algoritmos de Consenso, como explanado na Seção 2.1.1). No Passo 6, após o consenso ser atingido, o bloco é adicionado à *blockchain* e a transação é confirmada (Passo 7).

**Figura 2 – Funcionamento básico de uma *blockchain*.**



Fonte: Elaborada pelo autor.

Tal tecnologia introduz elementos eficazes para a implementação de um sistema no qual deve-se haver consenso entre diferentes partes. Dentre eles a possibilidade de consenso em uma rede aberta com participantes desconhecidos, além da garantia de auditabilidade, autenticidade, disponibilidade, não repudiabilidade e integridade das transações validadas e armazenadas no livro-razão distribuído (GREVE et al., 2018). Algumas dessas propriedades são detalhadas a seguir.

- Descentralização e Desintermediação: As aplicações desenvolvidas utilizando *blockchain* são executadas em uma rede P2P, isto é, distribuidamente e de forma que não seja necessária uma entidade para intermediar as ações entre partes desconhecidas. Tal característica pode minimizar gastos adicionais e desburocratizar processos que outrora dependiam do intermédio de órgãos específicos.
- Disponibilidade: Os nós da rede *blockchain* possuem a mesma cópia do livro-razão onde estão armazenadas as transações de maneira segura e consistente. Além disso, caso algum nó sofra alguma falha e/ou perca esses dados, é possível recuperá-los visto que estão replicados na rede.
- Transparência: As transações armazenadas em redes *blockchains* públicas podem ser acessadas por qualquer participante da rede, sendo possível a verificação das informações armazenadas no livro-razão além de favorecer a auditabilidade desses ativos entre as diferentes entidades da rede.
- Imutabilidade e Não repudiabilidade: Como já mencionado, os blocos são encadeados

ados criptograficamente de forma que qualquer alteração invalidaria toda a cadeia de blocos. Isto significa que os dados não podem ser alterados ou removidos após sua inserção na *blockchain*. Por sua vez, o não repúdio pode ser atendido, visto que um participante não pode negar a autenticidade de sua assinatura em uma transação. Além disso, essa natureza imutável proporciona o rastreamento dos ativos registrados em *blockchains*.

### 2.1.1 Algoritmos de Consenso

O primeiro algoritmo de consenso a ser criado foi o PoW, desenvolvido por Satoshi Nakamoto e implementado no Bitcoin como forma de evitar as chamadas Falhas Bizantinas, advindas do conhecido “Problema dos Generais Bizantinos” (LAMPORT et al., 2019). Em suma, nesse problema tem-se o cenário em que tropas do exército bizantino, cada um com seu próprio general, dividem-se e cercam uma cidade adversária para atacá-la. Os generais devem decidir sobre um plano comum, mas eles só podem se comunicar por meio de mensageiros. Alguns desses generais podem ser traidores, ao ponto de impedir que os generais leais cheguem em um comum acordo. Assim, os generais devem ter um algoritmo em que: (a) os generais leais possam ter o mesmo plano de ação: atacar ou não a cidade inimiga; e (b) um pequeno número de traidores não seja capaz de fazer com que os generais leais optem pelo plano errado.

Em uma *blockchain*, as transações são consideradas como um conjunto de operações de leitura e escrita executadas e replicadas em cada nó de um banco de dados distribuído (GUPTA; SADOGHI, 2019). Antes que as transações submetidas sejam incluídas permanentemente à *blockchain*, nós da rede denominados de “mineradores” precisam avaliar e concordar com todas as inserções. Assim, deve-se haver o consenso da rede para que as transações sejam aceitas (MÖLKEN, 2018). Tal acordo é executado por meio de Algoritmos de Consenso implementados na rede *blockchain*.

Como já mencionado, um dos mais comumente utilizados é o algoritmo PoW. Este algoritmo é baseado na ideia de que um nó aleatório é selecionado sempre para criar um novo bloco de transações. Um nó minerador é aquele capaz de provar que realizou um cálculo não-trivial apresentado a solução do desafio computacional. Dessa forma, um nó minerador deve resolver um desafio criptográfico baseado em força bruta o qual, em suma, consiste em aplicar uma função *hash H* sobre o *header* do bloco

sucessivas vezes até encontrar o valor correto do *nonce*, de maneira que o resultado do *hash* seja menor do que a *dificuldade alvo* imposta pela rede (GREVE et al., 2018). O nó minerador que encontrar o valor do *nonce* irá transmitir o bloco para outros nós que deverão verificar mutuamente o valor *hash* (ZHENG et al., 2017). Caso o bloco seja validado, os outros mineradores irão anexar o bloco à *blockchain*, e o minerador que descobriu o *nonce* correto recebe recompensas.

No caso da rede Bitcoin, que utiliza PoW como algoritmo de consenso, essa dificuldade alvo é ajustada de forma que novos blocos possam ser gerados pela rede a cada 10 minutos. Como a probabilidade de geração bem-sucedida é baixa, é difícil prever qual nó em funcionamento na rede irá gerar o próximo bloco (LIN; LIAO, 2017). Uma das desvantagens do algoritmo PoW é que este demanda um alto poder computacional e, consequentemente, elevado consumo de energia visto que executa força bruta para descobrir um *nonce* aleatório. Isso pode distorcer a natureza descentralizada da rede, pois somente os nós com alto poder computacional terão maior probabilidade de minerar o bloco e receber recompensas.

Uma das alternativas ao alto custo computacional da PoW é a Prova de Participação (PoS, do inglês *Proof of Stake*) introduzida por King e Nadal (2012). Neste algoritmo de consenso, um nó pode criar blocos e receber recompensas quando este prova que tem a posse de uma quantidade considerável de moedas. A escolha do nó é feita de forma probabilística e o tamanho da *stake* determina as chances do “nó” ser selecionado como próximo validador. Diferentes mecanismos estão sendo propostos e podem ser adaptados conforme as demandas da aplicação a ser construída, dentre eles estão *Proof of Activity* (BENTOV et al., 2014), *Proof of Burn* (KARANTIAS et al., 2020), *Proof of Space* (PARK et al., 2015), *Proof of Elapsed Time* (PoET) (CORPORATION, 2017), dentre outras. Bach et al. (2018) e Mingxiao et al. (2017) apresentam análises comparativas dos mais variados tipos de algoritmos de consenso.

Nguyen e Kim (2018) apresentam algumas variantes de algoritmos de consenso dentro da Blockchain e os categorizam em dois tipos principais: Algoritmos de Consenso Baseados em Prova e Algoritmos de Consenso Baseados em Votação. Os algoritmos mencionados anteriormente são do tipo baseados em prova, isso significa que o nó que executa a prova suficiente terá o direito de acrescentar um novo bloco à cadeia e receber a recompensa. Por sua vez, nos algoritmos baseados em votação, os nós dentro da rede devem ser conhecidos e ajustáveis, para que a comunicação

possa ocorrer mais facilmente. Deste último tipo, um dos mais utilizados é o *Practical Byzantine Fault Tolerance* (PBFT) (CASTRO et al., 1999).

No PBFT, existem dois tipos de nós: um nó líder e alguns nós de validação, os quais executam algumas rodadas para anexar um bloco à *blockchain*. Inicialmente, os clientes enviam suas solicitações de transações para seus nós de validação correspondentes que, por sua vez, validarão as transações e as transmitirão a outros nós validadores e ao nó líder. O nó líder irá ordenar um conjunto das transações pelo seu tempo de criação, organizando-as em um bloco. Posteriormente, o líder transmite seu bloco proposto para outros nós que irão receber e armazenar o bloco localmente. A fim de que tenham a certeza de que o bloco recebido do líder é o mesmo, eles fazem uma verificação dupla. Caso algum nó receba os blocos, que são iguais aos armazenados localmente antes, de mais de 2/3 de todos os nós, ele validarão o bloco. Em seguida, o mesmo procedimento é registrado após a confirmação, que é o requisito para qualquer nó executar as transações no bloco proposto e anexá-lo às suas cadeias atuais.

### 2.1.2 Tipos de Blockchains

A tecnologia *blockchain* tem sido integrada em diferentes domínios de aplicação, com suas particularidades e características nos diferentes níveis de implementação, sendo estes na camada de *blockchain*, na camada de rede e na própria camada de aplicação, por exemplo. Sendo necessária essa adequação da tecnologia em novos domínios, a *blockchain* pode ser categorizada em dois tipos diferentes de redes: Pública e Privada. Ambas têm características comuns sobre os conceitos fundamentais de uma *blockchain*, mas possuem suas vantagens e desvantagens para diferentes modelos de negócios (MÖLKEN, 2018).

Por sua vez, redes *blockchains* públicas e privadas podem conceder diferentes tipos de permissões, por isso são classificadas de permissionadas (*permissioned*) ou não permissionadas (*permission-less*). Conforme Acharya et al. (2019), uma *blockchain* não permissionada geralmente é conhecida como *blockchain* pública pois qualquer nó pode juntar-se à rede, com a possibilidade de realizar escrita e leitura das transações. Além disso, os nós são anônimos já que não têm a necessidade de verificar a identidade dos participantes da rede. Em relação às redes permissionadas, apenas usuários ou organizações autorizados previamente podem executar transações

de escrita e/ou leitura. Xu et al. (2019) apresentam o relacionamento dos tipos de *blockchain* com seus respectivos tipos de permissão, como apresentado no Quadro 1.

**Quadro 1 – Principais componentes dos diferentes tipos de *blockchain*.**

	<b>Não permissionado</b>	<b>Permissionado</b>
<b>Público</b>	Consenso: - Prova de X Gerenciamento de permissão: - Camada Blockchain - Camada de aplicação Incentivo: - Camada Blockchain	Consenso: - Prova de X- PBFT, consenso federado, Round Robin, etc Gerenciamento de permissão: - Camada Blockchain - Camada de aplicativo (opcional) Incentivo: - Camada Blockchain - Governança em torno de permissões
<b>Privado</b>	Consenso: - Prova de X - PBFT, consenso federado, Round Robin, etc Gerenciamento de permissões: - Camada Blockchain - Camada de rede - Camada de aplicativo (opcional) Incentivo: - Governança em torno de permissões	Consenso: - Prova de X - PBFT, consenso federado, Round Robin, etc Gerenciamento de permissões: - Camada Blockchain - Camada de rede - Camada de aplicativo (opcional) Incentivo: - Governança em torno de permissões

Fonte: Adaptado de Xu et al. (2019), tradução nossa.

Ambas as redes públicas não permissionada e permissionada oferecem transparência, desintermediação e anonimato (ACHARYA et al., 2019). A diferença é que na pública não permissionada todos podem ingressar na *blockchain* através de sua máquina, formando assim, uma rede de partes não confiáveis. Todos os nós podem ler e escrever, e fazer validações das transações. Nas redes públicas permissionadas, todos os usuários podem ler as transações, porém apenas alguns têm a permissão de escrever, ou vice-versa. Nesse caso, existem restrições para leitura e/ou gravação.

Nas redes *blockchains* privadas e não permissionadas somente membros selecionados podem executar ações como gravação, leitura e validação de transações. Geralmente, as permissões são centralizadas a determinados membros, o que pode até eliminar a natureza descentralizada da rede, mas favorecem possíveis necessidades de privacidade. Já em *blockchains* privadas permissionadas as partes são identificáveis e as permissões gerenciadas, e a privacidade dos dados transacionados pode ser exclusiva para um grupo de participantes pré-definido, assim como o controle do consenso da rede.

## 2.2 Contratos Inteligentes e Decentralized Applications (dApps)

Através da expansão do uso de *blockchain* além da aplicação financeira permitida pelo Bitcoin, novas gerações dessa tecnologia possibilitaram o desenvolvimento

de diferentes lógicas de negócio, abrangendo setores como governo, saúde, ciência, educação, dentre outros. Tal característica é possível por meio do uso de Contratos Inteligentes, introduzidos em blockchains na criação da rede Ethereum (BUTERIN et al., 2013). Contratos Inteligentes (ou *Smart Contracts*, no inglês) consistem em *scripts* que executam a lógica de negócios quando determinadas condições são atingidas, e isso ocorre no topo da *blockchain* (BASHIR, 2017). Segundo Xu et al. (2019):

Contratos inteligentes são programas implantados como dados [...] e executados em transações no *blockchain*. Os contratos inteligentes podem conter e transferir ativos digitais gerenciados pelo *blockchain* e podem invocar outros contratos inteligentes armazenados no *blockchain*. O código de contrato inteligente é determinístico e imutável uma vez implantado.

Os contratos inteligentes podem automatizar e gerenciar a execução de contratos legais entre diferentes partes a partir de protocolos de interações previamente definidos. Tal ação contribui para colaboração do negócio entre empresas, além de impulsionar e inovar no desenvolvimento de sistemas que usam *blockchain* em diversos casos de uso e áreas. Os *scripts* executados no Bitcoin tem uma capacidade computacional bastante limitada, diferente da rede Ethereum que permite que programas de computador sejam escritos em uma linguagem de programação *Turing-complete*.

Um contrato inteligente pode ser invocado por meio de transações que, por sua vez, é auto-executado em cada nó da rede conforme o que estiver proposto na lógica de negócio. Em outras palavras, cada nó da *blockchain* que executa o contrato inteligente, está executando uma Máquina Virtual (VM, do inglês *Virtual Machine*) e a *blockchain* funciona como uma VM distribuída (CHRISTIDIS; DEVETSIKOTIS, 2016). Na Ethereum, o código dos contratos inteligentes é escrito em uma linguagem de *bytecode* baseada em pilha e executado na *Ethereum Virtual Machine* (EVM).

O uso de contratos inteligentes na implementação de aplicações e sistemas introduziu o desenvolvimento de Aplicações Descentralizadas (*Decentralized Applications*, no inglês). Os aplicativos descentralizados têm como uma de suas principais características o fato de que não há um único servidor ou entidade controlando-os como em um modelo cliente-servidor. Além disso, esses têm como base o uso de *blockchain* como armazenamento e processamento, através da implementação de con-

tratos inteligentes (METCALFE, 2020). Antonopoulos e Wood (2018) consideram que a natureza descentralizada de *dApps* abrangem muitos dos aspectos, como *backend* e *frontend*, armazenamento dos dados, protocolos de comunicação, dentre outros.

De acordo com Raval (2016) e Metcalfe (2020), os *dApps* podem ser implementados em diferentes dispositivos utilizando as mesmas ferramentas e linguagens de programação como qualquer outra aplicação a diferença é que precisam atender aos seguintes critérios :

- Código Aberto: A aplicação deve ser totalmente de código aberto e operar autonomamente, de maneira que não haja uma autoridade central monopolizando os *tokens* da rede e que sejam possíveis verificação por parte de terceiros.
- Descentralizada: Dados e registros devem ser armazenados em uma *blockchain* ou rede P2P de forma a evitar pontos centrais de falha.
- Incentivo por meio de *tokens*: *dApps* usam *tokens* criptográficos para acessar as aplicações, realizar transações e prover recompensas.
- Algoritmo/Protocolo: Inclusão de mecanismos de consenso, como PoW, PoS ou mesmo o próprio adaptado para o *dApp*.

### 2.3 Escalabilidade em Blockchains

Apesar das características que fazem a tecnologia *blockchain* ser tão promissora, esta ainda lida com o desafio da escalabilidade, que pode se tornar uma barreira em aplicações reais que utilizam *blockchain*. Koteska et al. (2017) apresenta que os limites de escalabilidade da *blockchain* referem-se ao tamanho dos dados no *blockchain*, à taxa de processamento e à latência da transmissão dos dados. Seguindo o mesmo raciocínio, Xie et al. (2019) consideram três aspectos relacionados à escalabilidade na *blockchain*: *throughput*, armazenamento e *networking*.

Em relação ao *throughput* (ou taxa de transferência), este associa-se à quantidade de transações em um bloco e o intervalo em que os blocos são criados. No Bitcoin, por exemplo, tem-se um intervalo aproximadamente de 10 minutos, sendo que o número de transações depende do tamanho bloco, que geralmente está limitado à 1,4 MB<sup>4</sup>, em média. O tamanho do bloco define a quantidade de transações que podem ser processadas por segundo, podendo inibir a capacidade de crescimento da rede.

<sup>4</sup> Dados fornecidos por <https://www.blockchain.com/charts/avg-block-size>

Além disso, se as transações ultrapassarem o limite do bloco, este pode ser rejeitado pela rede (MAZLAN et al., 2020).

Sobre o desafio de escalabilidade referente ao armazenamento, sabe-se que aplicações que buscam resolver problemas do mundo real, geralmente, demandam uma grande quantidade de dados a serem transacionados e armazenados. Como já mencionado, os dados armazenados em uma *blockchain* podem ser replicados em cada nó da rede, ou seja, se cada nó tem uma réplica completa dos dados em uma *blockchain*, este contém todo o histórico de transações até o bloco *genesis*. Swan (2015) ressalta que para que um nó realize o *download* de toda a *blockchain* leve-se bastante tempo, em torno de um dia. Outro problema que pode ser gerado é a centralização da rede, visto que são necessários muitos recursos computacionais para executar o nó completo. Com isso, à medida que se faz necessário controlar uma elevada quantidade de transações, os problemas de tamanho e largura de banda podem tornar-se críticos.

Quanto à *networking*, tal desafio refere-se à transmissão das transações que são realizadas entre os nós da rede. Quando há um grande número de transações a serem transmitidas, necessita-se de recursos de largura de banda da rede. Adicionalmente, somando-se à transmissão da transação quando esta é gerada, existe também a transmissão do bloco ao ser minerado, o que também pode consumir muitos recursos e aumentar o atraso de propagação do bloco.

A fim de mitigar tais problemas de escalabilidade, diferentes abordagens têm sido propostas das quais pode-se destacar o uso de técnicas *off-chains*. Uma estratégia *off-chain* refere-se à computações ou armazenamentos feitos fora da *blockchain* (SHUKLA; SAMET, 2020). Pelo contrário, quando estas tarefas estão sendo executadas dentro da *blockchain* são chamadas de *on-chain*. Eberhardt e Tai (2017) denominam de *Content-Addressable Storage Pattern* o padrão que utiliza sistemas de armazenamento distribuído para terceirizar o local de armazenamento dos dados brutos, por exemplo. Dentre esse tipo de solução, Xie et al. (2019) destacam tecnologias como o IPFS, *Distributed Hash Table* (DHT) e Bigchain. Uma prática comum para gerenciamento de dados em sistemas baseados em *blockchain* é armazenar apenas metadados, pequenos dados críticos e *hashes/ponteiros* que referenciam os dados brutos (XU et al., 2019).

Exemplificando os problemas de escalabilidade que podem ser ocasionados

em situações reais, pode-se destacar àqueles relacionados aos sistemas de *blockchain* voltado para o domínio da saúde. Mazlan et al. (2020) apresentam alguns desafios para esse domínio, por exemplo, visto que blocos que ultrapassam o limite de tamanho podem ser rejeitados, alguns dados do paciente podem não ser processados, incluindo genômicos, órgãos críticos e outros. Semelhantemente, o alto volume de informações em um cenário de saúde de larga escala poderia levar a um “estouro de informações” devido ao grande volume de armazenamento de dados não processados. Para mais, armazenar um alto volume de dados nos sistemas baseados em *blockchain* pode levar à uma degradação crítica de seu desempenho e ocasionar em latências significativas, sendo até mesmo impraticável em algumas situações (AGBO et al., 2019).

## 2.4 Prontuário Eletrônico do Paciente (PEP)

Segundo o Conselho Federal de Medicina (BRASIL, 2002b) o prontuário é um documento único composto por diversas informações, sinais e imagens que são registradas. Esses registros são criados a partir de fatos ou situações que dizem respeito à saúde do paciente e ao cuidado prestado a ele. O prontuário permite a comunicação entre membros da equipe multiprofissional de saúde, que garante continuidade da assistência ao indivíduo.

Este documento requer um conjunto mínimo de informações que devem ser obrigatoriamente preenchidas pela equipe de saúde. Dentre eles destacam-se: identificação completa do paciente (nome, sexo, data de nascimento, nome da mãe, naturalidade e endereço), anamnese, exame físico e exames complementares com resultados e/ou hipóteses diagnósticas e tratamento prescrito e evolução diária do paciente. Além disso, deve constar nome legível, assinatura e número de inscrição no seu registro de classe (BRASIL, 2002b; BRASIL, 2002a).

Entretanto, esse documento possui desvantagens. A Sociedade Brasileira de Informática em Saúde (SBIS, 2012) aponta que o prontuário em papel está disponível a apenas uma pessoa por vez, possui baixa mobilidade e que está sujeito a ilegibilidade, ambiguidade e perda de informações e que sua guarda requer amplos espaços em serviços de arquivamentos. Mesmo assim, sabe-se que durante a história esse documento vem sendo utilizado de forma impressa pelos diversos estabelecimentos de saúde em todo o mundo.

Por outro lado, com a modernização e informatização da sociedade, o setor saúde viu necessidade de atualizar-se, dando início a formulação de um Prontuário Eletrônico do Paciente (PEP). Assim sendo, o PEP deve ser entendido como estrutura para manutenção da informação eletrônica sobre o estado de saúde do indivíduo e os cuidados recebidos durante sua vida. Portanto, o PEP registra todas as informações indispensáveis para a comunicação da equipe multiprofissional e o paciente, no qual há garantia de segurança e gestão do serviço de saúde (LAHM; CARVALHO, 2015).

Além de finalidade inicial que é o armazenamento e a garantia da continuidade do cuidado e do gerenciamento das unidades de saúde, os dados que são armazenados no PEP podem ser utilizados como fonte para estudos de extração de conhecimento. Diversas pesquisas vêm sendo realizadas a fim de melhorar o processo de cuidado em saúde a partir desses dados, dentre eles pode-se citar ferramentas de apoio à decisão em saúde, monitoramento do paciente e relatórios em tempo real aos profissionais. Além disso, com o advento de *big data* e de técnicas de mineração de dados, padrões podem ser determinados e cuidados específicos a cada pessoa podem ser direcionados. Portanto, o uso do PEP não se restringe ao armazenamento de dados, expandindo-se para áreas de crescimento científico e tecnológico.

Entretanto, apesar dos diversos benefícios apresentados, a implantação de um PEP não é tarefa simples. De acordo com Jenal e Évora (2012) “a implantação de sistemas de informação em um hospital, além de complexo, envolve um custo muito alto e um compromisso significativo da força de trabalho, esperando-se que os sistemas implantados funcionem de modo adequado”. Ressalta-se que para que a implantação de um sistema de informática aconteça, deve existir uma mudança cultural na instituição por meio da aceitação e disponibilidade de se iniciar um novo processo.

No cenário atual referente à prestação de cuidados de saúde, as informações clínicas estão fragmentadas e distribuídas em diferentes mídias e locais, dos mais variados tipos e formatos de registros (BACELAR; CORREIA, 2015). Isto ocorre porque os sistemas são construídos por diferentes empresas, as quais seguem seu próprio padrão na modelagem dos dados clínicos. Tal limitação ocasiona uma série de prejuízos ao paciente, tendo em vista que a falta de comunicação adequada entre as diferentes entidades de saúde provoca a piora na eficiência das organizações e, consequentemente, na gestão das informações clínicas. Assim, faz-se necessário que a interoperabilidade entre diferentes sistemas de informação em saúde seja alcançada.

Segundo Bacelar e Correia (2015) “a interoperabilidade semântica é o estado ideal, onde os sistemas trocam informações usando os mesmos formatos e vocabulários”.

Para mitigar esta problemática, diferentes padrões têm sido propostos para promover a interoperabilidade entre os sistemas nos mais variados níveis, assim como sua adoção nas organizações de saúde de diversos países. Dentre os padrões existentes pode-se citar o OpenEHR, padrão que permite o uso de um modelo referência e estruturas de dados clínicos a fim de preservar a semântica no campo do conhecimento clínico. Em outras palavras, é uma “tecnologia *e-health* que consiste em especificações abertas, modelos clínicos e software que podem ser usados para criar padrões e construir soluções de informação e interoperabilidade para saúde” (OPENEHR, 2021).

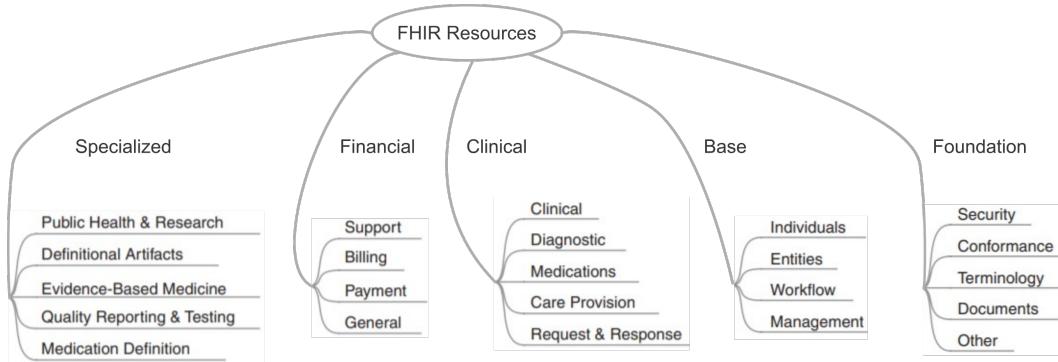
Outro padrão que vem sendo bastante utilizado é o *Fast Healthcare Interoperability Resources* (FHIR), que é um padrão que descreve formatos e elementos de dados, denominados de “recursos” e uma *Application Programming Interface* (API) para troca de registros eletrônicos de saúde (BENSON; GRIEVE, 2021). O padrão foi criado pela organização de padrões de saúde *Health Level Seven International* (HL7). O escopo do FHIR é extenso, de forma a abranger humanos e veterinários, além dos cuidados clínicos, saúde pública, ensaios clínicos, administração, aspectos financeiros, dentre outros. O padrão se destina ao uso global e em uma ampla variedade de arquiteturas e cenários. Segundo Benson e Grieve (2021), um dos pontos positivos do uso do FHIR é a facilidade e rapidez de implementação, dentre os benefícios estão:

- Várias bibliotecas de implementação, com muitos exemplos para iniciar o desenvolvimento com especificação gratuita para uso sem restrições.
- Interoperabilidade pronta para uso: os recursos básicos podem ser usados como estão, mas também podem ser adaptados conforme necessário para atender aos requisitos locais usando Perfis, Extensões e Terminologias.
- Base sólida em padrões da Web: XML, JSON, HTTP, OAuth, etc.
- Suporte para arquiteturas RESTful, troca contínua de informações usando mensagens ou documentos e arquiteturas baseadas em serviços.
- Um formato de serialização legível para facilitar o uso pelos desenvolvedores.
- Análise baseada em ontologia com mapeamento formal para correção.

O conteúdo mais significante da especificação do FHIR ocorre na definição de recursos. O FHIR define 145 tipos de recursos de forma a representar diferentes tipos de conteúdos em um nível maior da hierarquia, os quais estão divididos em:

*Foundation, Base, Clinical, Financial e Specialized.* Tal categorização e as respectivas ramificações podem ser visualizadas na Figura 3.

**Figura 3 – Categorias de Recursos do FHIR.**



Fonte: Adaptado de Benson e Grieve (2021).

De uma forma macro, a arquitetura lógica do FHIR pode ser visualizada conforme apresentada na Figura 4. A especificação FHIR define uma série de recursos de domínio que lidam com a troca de dados de saúde. Em torno desses recursos de domínio, a especificação FHIR fornece: (i) uma infraestrutura para troca de recursos incluindo a API RESTful; (ii) uma camada de definição/ontologia que fornece descrições narrativas do conteúdo, mapeamentos para outras especificações e um conjunto computável de definições; (iii) uma estrutura de conformidade e, por fim (iv) um conjunto de recursos para gerenciar fluxos de trabalho - solicitações para realizar ações, etc.

**Figura 4 – Arquitetura lógica do FHIR.**



Fonte: Benson e Grieve (2021), tradução nossa.

## 2.5 Computer Supported Cooperative Work (CSCW)

O termo “*Computer Supported Cooperative Work*” (CSCW) foi introduzido em um workshop por Irene Greif e Paul Cashman em 1984 no qual visavam compreender a função da tecnologia em um ambiente de trabalho e, especialmente, como as pessoas lidam de forma colaborativa na construção de tecnologias (FURKS; PIMENTEL, 2011). Tal compreensão pode ser considerada como interdisciplinar, visto que os pesquisadores visaram investigar a atividade em grupo nas mais variadas áreas, como a Psicologia, Sociologia, Antropologia, Educação, Economia e dentre outras. O termo “CSCW” tem sua representação brasileira como sendo “Sistemas Colaborativos”, no qual o primeiro é utilizado para indicar tanto os sistemas (CS) quanto os efeitos psicológicos, sociais e organizacionais do trabalho em grupo (CW).

Embora tais termos e áreas da computação tenham sido introduzidos na década de 80, o estudo e valorização do trabalho em equipe por meio de recursos técnicos é um tema antigo, surgido no final da década de 1940 com origem na **Abordagem Sociotécnica**. Oliveira et al. (2020) considera que os fatores técnicos e sociais são indissociáveis, pois um sistema de informação pode ser composto por um conjunto de (i) tecnologias, (ii) processos organizacionais e (iii) pessoas, integrados entre si. Seguindo um mesmo raciocínio, segundo Klein (2014): “A teoria sociotécnica deixa explícito o fato de que a tecnologia e as pessoas, em um ambiente de trabalho, são interdependentes [...] Tecnologia afeta o comportamento das pessoas, e o comportamento das pessoas afeta o trabalho da tecnologia”.

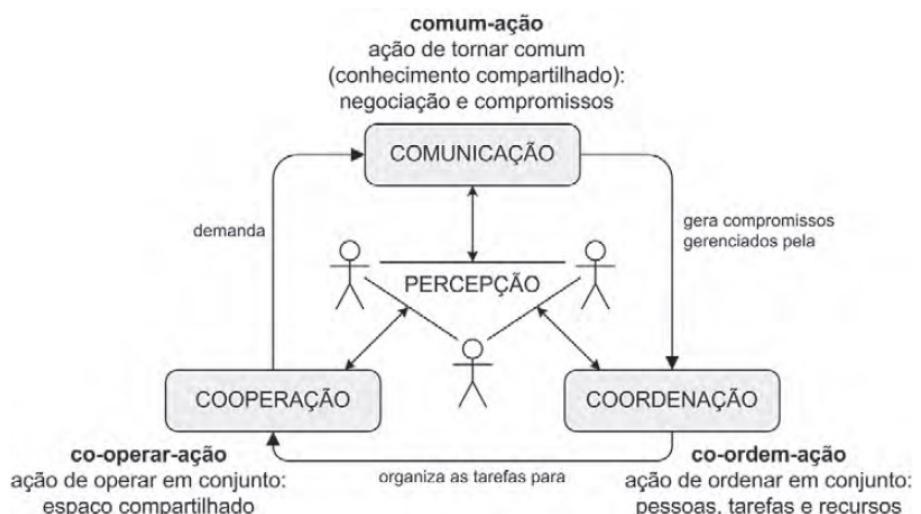
Por mais que os sistemas de *softwares* sejam intrinsecamente tecnológicos, sua análise e implementação se tornam realmente relevantes quando embasados por uma abordagem sociotécnica, tendo em vista que são feitos para resolver problemas da própria sociedade. Porém, conforme Kujawski (2003), “fomentar comunicação, motivação e liderança por meio de softwares colaborativos não é uma tarefa fácil, pois envolve fatores como o velho e complexo comportamento humano”. Além disso, há de se ressaltar também que o uso de tecnologias pela sociedade pode gerar mudanças consideráveis de forma a afetar as relações e comunicações interpessoais nos diversos nichos, desde negócios até questões políticas (CUKIERMAN et al., 2007).

Dessa forma, faz-se necessária a aplicação das devidas abordagens para análise do comportamento de pessoas e grupos ao interagirem com *softwares*, de

maneira que se possa projetar e construir adequados sistemas colaborativos que sejam efetivos para o trabalho em grupo. Por sua vez, a área CSCW possibilita uma gama de teorias e modelos de colaboração que podem ser utilizadas para fornecer uma visão sobre como e porque as pessoas trabalham em grupo, auxiliando no desenvolvimento de *softwares*. De acordo com Furks e Pimentel (2011), **teorias** são úteis para “entender, comparar, abstrair e generalizar as observações sobre o mundo que nos cerca e sobre os produtos criados na sociedade” e um **modelo científico** “é uma representação lógica ou matemática de um fenômeno, é uma descrição do fenômeno de forma abstrata, conceitual, gráfica ou visual”.

Dentre os modelos existentes, pode-se apresentar o modelo Padrões de Colaboração (VREEDE et al., 2006), que estabelece o processo de trabalho sendo composto pelas atividades de geração, redução, esclarecimento, organização, avaliação e comprometimento; o Modelo de Tuckman (TUCKMAN, 1965), o qual visa explicar os estágios de um grupo de trabalho; e o Modelo 3C de Colaboração (PIMENTEL et al., 2006), o qual considera a comunicação, coordenação e cooperação como pilares essenciais da colaboração, como apresentado na Figura 5. Este último tem sido utilizado para diferentes propósitos, tais como, a classificação de ferramentas colaborativas, análise de interfaces e avaliação de aplicações colaborativas (COSTA et al., 2014). O presente trabalho se aterá em detalhar apenas modelo 3C de colaboração, haja vista que tem-se o objetivo de utilizar uma de suas versões para investigação e avaliação deste estudo à luz de seus pilares de colaboração mencionados.

**Figura 5 – Modelo 3C de Colaboração.**



Fonte: Furks e Pimentel (2011).

Uma extensão desse modelo é apresentado por Costa et al. (2014), os quais apresentam o modelo 4C de colaboração associando-o também à melhoria de processos de desenvolvimento de software no quesito colaborativo, no qual o quarto 'C' acrescentado refere-se ao termo “colaboração”. Além da adição do termo, o Modelo 4C difere do modelo 3C de colaboração pois são considerados como conceitos distintos. As dimensões descritas a seguir se relacionam a fim de promover a colaboração em um grupo de trabalho com apoio de sistema de software.

- **Comunicação** envolve a troca de mensagens e a negociação de compromissos por meio de ferramentas que processam a interação;
- **Coordenação** trata da gestão de pessoas, tarefas e recursos para lidar com conflitos de interesse, e organiza atividades para serem realizadas em determinada ordem e períodos de tempo;
- **Cooperação** compreende tarefas desenvolvidas individualmente, e a **colaboração** ocorre em conjunto, ambos por meio de um espaço partilhado.

Os modelos possibilitados pela área CSCW podem contribuir efetivamente para construção de sistemas colaborativos e interdisciplinares, visto que pode abranger os mais variados domínios e áreas. Especificamente, Prinz (2018) introduz uma relevante discussão sobre a relação entre a CSCW e *blockchain*, denominando esta combinação de abordagens como ‘CSCBlockchain’ ou ‘CSCB’. Tal discussão levantou alguns aspectos semelhantes entre ambas as áreas ao concluir alguns temas iniciais a serem discutidos em CSCB, como: (i) possibilidade de criação de prova de consciência de colaboração baseada em um algoritmo distribuído que valida transações com base em seu contexto de cooperação; (ii) a compreensão de contratos inteligentes como padrões de cooperação regidos por regras de cooperação flexíveis e com controle de versão; (iii) utilizar os registros de transações em abordagens de gerenciamento de reputação e, por fim; (iv) custo para cooperação confiável em uma rede descentralizada.

## 2.6 Conclusões do Capítulo

Este capítulo teve por objetivo apresentar os conceitos base para o entendimento da solução proposta. Inicialmente, a tecnologia *blockchain* foi explanada por meio de sua definição, breve história, características, e descrição da sua estrutura e do seu funcionamento. A fim de apresentar os conceitos base sobre o funcionamento

de uma *blockchain*, alguns algoritmos de consenso foram apresentados. Por sua vez, diante da demanda de diferentes aplicações, foram apresentados também os tipos de *blockchain* existentes e suas características quanto às formas de permissão. Adicionalmente, o desafio de escalabilidade em *blockchains* foi explanado visto que é um das questões a serem mitigadas na presente proposta. Em seguida, a fim de apresentar o domínio a ser trabalhado, uma breve descrição sobre PEPs e de padrões de interoperabilidade foi realizada. Por fim, foram apresentados conceitos sobre sistemas colaborativos, abordagem sociotécnica e modelos utilizados para auxiliar no entendimento do comportamento de pessoas que trabalham em grupo com apoio de software.

### 3 TRABALHOS RELACIONADOS

Nesta seção, serão apresentados os trabalhos relacionados à presente pesquisa. Primeiramente, será apresentado o trabalho encontrado no qual realiza discussões preliminares sobre uma perspectiva sociotécnica ao associar *blockchain* e saúde. Devido às lacunas quanto a essa temática no estado-da-arte, buscou-se apresentar trabalhos nacionais encontrados durante busca na literatura, objetivando também conhecer como se adéquam aos regimentos atuais. Ademais, outros trabalhos foram levantados a fim de que o estado da fosse explorado de uma forma geral.

Considerando uma perspectiva sociotécnica com discussões com foco mais teórico, sem a apresentação de uma solução, Wong et al. (2018) sugerem que a discussão sobre *blockchain* na área da saúde pode levar em consideração fatores sociotécnicos complexos. Os autores enfatizam o potencial de *blockchain* na saúde no quesito comunicação, porém alertam que tal introdução deve levar, urgentemente, em consideração os impactos da intervenção tecnológica, visto que o uso de *blockchain* tem começado a amadurecer. Segundo os autores, deve-se buscar entender como utilizar de fato a tecnologia para gerar valor às partes interessadas e como as informações armazenadas podem ser úteis e transmitidas em *blockchain*.

Ademais, os outros poucos trabalhos sociotécnicos encontrados não foram relacionados à saúde. Por exemplo, Shin e Ibahrine (2020) analisam o design e o desenvolvimento de iniciativas de *blockchain* na Coreia considerando visões “socioecológicas”, como fenômenos sociais, tecnológicos e culturais que influenciam a sociedade. Os autores realizaram coleta de dados primários através de entrevistas. Além disso, usaram dados secundários, como relatórios públicos do governo, relatórios da indústria e documentos públicos para complementar as análises das entrevistas. Por sua vez, Nabben (2021) discute o que denomina de “*people security*” (“segurança de pessoas” no português), no qual realizam uma análise sociotécnica dos atributos e limitações de confiança e segurança de diferentes tipos de *blockchains* para pessoas.

A seguir, são apresentados os trabalhos com modelagens ou PoCs, porém que não envolvem questões sociotécnicas. Agostinho et al. (2019) apresentam uma solução, baseada em *blockchain*, com o uso de *smart contracts* para o problema de interoperabilidade de dados de médicos como meio de armazenamento. Os autores baseiam-se no trabalho de Yuan e Wang (2018) para a divisão das camadas da

abordagem em: dados, rede, consenso, incentivo, contrato e aplicação. A abordagem faz o uso de assinatura assimétrica para garantir a confidencialidade dos dados entre os participantes da rede, os quais podem ser lidos apenas pela entidade que originou a transação. Os autores desse trabalho apresentaram uma validação inicial através de um experimento preliminar sobre o uso da assinatura assimétrica.

Viana et al. (2020) sugerem um sistema de gerência de prontuário médico por parte dos próprios pacientes em processo de reabilitação física e neuro-funcional. Juntamente com o agente de saúde, o paciente pode gerenciar seus dados referentes à terapia, além de configurar o acesso a outras entidades de saúde em diferentes níveis. O fluxograma de funcionamento inicia-se pela coleta de dados por parte das clínicas para seu armazenamento e, posteriormente, a execução da validação pela *blockchain*. Em seguida, ocorre o gerenciamento de permissões e, por fim, a possibilidade de consulta aos dados. A abordagem implementa dois contratos inteligentes, um para o registro do usuário de forma a associá-lo a uma conta da *blockchain Ethereum*, e outro para gerenciamento das permissões de acesso. Por sua vez, Conceição et al. (2018) propõem uma arquitetura de informações em larga escala para acessar os registros eletrônicos de saúde utilizando contratos inteligentes para mediar as informações. Os autores apresentam requisitos de sistemas *Electronic Health Record* (EHR) nos quesitos de acessibilidade e gerenciamento dos dados, níveis dos dados e anonimização, e sobre questões éticas.

Fan et al. (2018), considerando os problemas de interoperabilidade, introduzem o MedBlock. Nessa proposta, se alguém busca realizar a leitura de um registro deverá conhecer a chave de descriptografia correspondente. Tal proposta garante que os pacientes possam consultar facilmente seus registros médicos passados, mesmo se estiverem armazenados no banco de dados de diferentes hospitais. A arquitetura do sistema é dividida em três camadas: Autoridade Certificadora - que tem a função de remover nós maliciosos do sistema, além de gerar, distribuir e gerenciar certificados digitais; Camada do Usuário - camada de acesso para todos os usuários do sistema e, por fim, Camada de Processamento - composta por servidores e banco de dados dos hospitais. O Medblock consiste em seis módulos: cliente, endorser, orderer, committer, database e ledger.

Zhang et al. (2018) apresentam o FHIRChain, uma arquitetura baseada em *blockchain* que segue o padrão HL7 *Fast Healthcare Interoperability Resources* e

aderente aos requisitos do *Office of the National Coordinator for Health Information Technology* (ONC). Assim, tal proposta dispõe de uma análise dos requisitos de ONC e suas implicações para sistemas baseados em *blockchain*. O FHIRChain é demonstrado por meio do desenvolvimento de um dApp que usa identidades digitais de saúde para autenticar os participantes. Além disso, os autores destacam algumas lições aprendidas do estudo de caso realizado relacionadas à tomada de decisão colaborativa para tratamento remoto de câncer.

A solução proposta por Fuentes (2019) introduz um registro de saúde descentralizado em que os pacientes decidem quais e com quem compartilhar seus dados, minimizando seus custos. Baseado no regulamento de proteção de dados da União Europeia (UE) de 2018, o ClinicAppChain apresenta mecanismos de autenticação, confidencialidade e compartilhamento de dados com permissão. Os autores desenvolveram um protótipo *blockchain* de baixo custo que não envolve o uso de criptomoedas e que possibilita diferentes partes na integração das informações de saúde. Nesse caso, o framework escolhido para desenvolvimento do *blockchain* foi o Hyperledger Fabric. Os ativos utilizados no ClinicAppChain são o EHR, dados pessoais do paciente, perfil público do médico e projetos de pesquisa do pesquisador. Cada ativo tem um ou mais proprietários entre os participantes e possui um conjunto de regras gerais de acesso associadas que limitam quem pode fazer qualquer transação no sistema. Além disso, o trabalho trata do armazenamento de ativos de maneira heterogênea, pelo qual os ativos baseados em texto são armazenados *on-chain* e ativos de mídia *off-chain*.

Shahnaz et al. (2019) apresentam uma estrutura que pode ser usada para a implementação da tecnologia *blockchain* no setor de saúde para EHR fornecendo um armazenamento seguro de registros eletrônicos. Isso é realizado com a definição de regras de acesso granular para os usuários da estrutura proposta. Tal trabalho foca na solução do problema de escalabilidade através do uso de armazenamento *off-chain* dos registros utilizando o mecanismo do *InterPlanetary File System* (IPFS). O framework proposto têm três entidades ou módulos: *User Layer* - camada que permite a interação do usuário com o sistema através de tarefas básicas como criação, leitura, atualização e deleção dos registros médicos; *Blockchain Layer* - essa camada contém o código ou mecanismo de interação do usuário com o DApp que está funcionando na *blockchain*, e por fim *System Implementation* - onde os contratos inteligentes foram implementados. Os contratos inteligentes são usados para dar acesso aos usuários,

o contrato *PatientRecord* realiza as operações de CRUD (acrônimo do inglês *Create, Read, Update and Delete*), enquanto o contrato *Roles* permite o acesso a biblioteca *OpenZeppelin* a qual contém vários outros contratos que definem as regras de acesso do usuário.

McFarlane et al. (2017) propõem o *Patientory*, um sistema que oferece a capacidade entre os pacientes e seus provedores de interagir e se comunicar, sendo capaz de coordenar o atendimento ao paciente através de uma *blockchain*. Tal proposta visa evitar a execução de serviços desnecessários, e duplica testes com redução de custos e melhorias na eficiência do ciclo de cuidado contínuo, ao mesmo tempo adere às regras e padrões da Lei de Portabilidade e Responsabilidade de Seguro (HIPAA). Segundo os autores, a implementação do *Patientory* baseia-se nos principais objetivos que qualquer sistema seguro deveria ter: confidencialidade, integridade, disponibilidade, responsabilidade e garantia de identidade/informação. A fim de atingir os objetivos mencionados para o sistema implementado, os autores o dividiram em diferentes sistemas independentes. Sobre a solução em relação ao armazenamento, os usuários serão capazes de usar a rede para alugar espaço de armazenamento de informações de saúde, e para executar pagamentos e transações nos contratos inteligentes de saúde através do uso de *tokens*. O Quadro 2 apresenta um resumo e comparação das características aplicadas por cada solução.

**Quadro 2 – Tabela comparativa dos trabalhos relacionados.**

	(WONG et al., 2018)	(SHIN; IBAHRINE, 2020)	(NABBEN, 2021)	(CONCEIÇÃO et al., 2018)	(AGOSTINHO et al., 2019)	(VIANA et al., 2020)	(FAN et al., 2018)	(FUENTES, 2019)	(ZHANG et al., 2018)	(SHAHNAZ et al., 2019)	(MCFARLANE et al., 2017)	Este trabalho
<b>Discussão sobre abordagem sociotécnica</b>	✓	✓	✓									✓
<b>Estudo empírico sociotécnico</b>		✓										✓
<b>Domínio brasileiro</b>				✓	✓	✓						✓
<b>Análise de aderência à normas locais</b>									✓	✓	✓	
<b>Técnicas para privacidade dos dados</b>				✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Armazenamento off-chain</b>				✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Controle de acesso / Permissões</b>				✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Discussão sobre desafios de escalabilidade</b>									✓	✓		✓
<b>Implementação da proposta</b>					✓		✓	✓	✓	✓	✓	✓
<b>Disponibilização do código-fonte</b>												✓
<b>Avaliação de desempenho</b>							✓		✓			✓
<b>Avaliação de segurança</b>							✓					✓

Fonte: Elaborado pelo autor.

### 3.1 Conclusões do Capítulo

Este capítulo teve o objetivo de apresentar alguns dos trabalhos relacionados a esta pesquisa. Os três estudos iniciais estão relacionados a trabalhos que discutem questões sociotécnicas, dentre os quais apenas um relaciona-se à saúde. Em seguida, são descritas propostas nacionais através das quais visou-se investigar se tais propostas adequam-se aos requisitos estabelecidos pelas autoridades nacionais. Visto que foram encontradas poucas abordagens nacionais propostas, o presente trabalho mostrou também abordagens internacionais a fim de analisar como as aplicações estão sendo construídas quanto à características de privacidade, controle de acesso, escalabilidade e padrões de dados médicos utilizados em um contexto mais amplo.

Observa-se que foi encontrado apenas um artigo envolvendo questões sociotécnicas ao associar *blockchain* e saúde. Tal estudo apresentou uma discussão preliminar sobre a importância de se discutir tais fatores para agregar valor às partes interessadas, porém, não houve estudo empírico. Outros trabalhos apresentados não envolveram o domínio da saúde. Porém, observa-se que já tem se iniciado estudos e metodologias empíricas envolvendo pessoas a fim de que se possa entender os aspectos sociais ao utilizar *blockchain*, como realizado por Nabben (2021).

Algumas lacunas foram observadas em relação aos trabalhos nacionais investigados (AGOSTINHO et al., 2019; CONCEIÇÃO et al., 2018; VIANA et al., 2020), apesar de apresentarem abordagens para confiabilidade, privacidade e controle de acesso, não sugerem soluções quanto à avaliação na adequação aos requisitos estabelecidos por autoridades nacionais. Em outras palavras, não realizaram uma adequação ao cenário brasileiro alicerçada em regimentos e normas para construção de sistemas de informação em saúde baseados em *blockchain*. Além disso, as abordagens nacionais que propuseram-se a tratar do problema de interoperabilidade não mostraram padrões específicos pelos quais se basearam. Adicionalmente, a questão da escalabilidade da *blockchain* quanto aos dados armazenados não foi discutida.

Ademais abordagens no contexto internacional demonstraram-se mais avançadas. Algumas delas realizam possíveis adequações conforme regimentos internacionais estabelecidos e padrões de interoperabilidade, como adequação ao regulamento de proteção de dados da UE (FUENTES, 2019), e ONC e HL7 (ZHANG et al., 2018). Porém, apesar de alguns trabalhos apresentarem uma solução para armazenamentos

fora da *blockchain* (FUENTES, 2019; SHAHNAZ et al., 2019) não foi identificado um profundo detalhamento e avaliação empírica sobre o problema de escalabilidade.

Considerando tais lacunas a partir dos trabalhos levantados, percebe-se a carência de trabalhos que analisam aspectos colaborativos. Adicionalmente, identifica-se a necessidade de sistemas de informação em saúde desenvolvidos no cenário brasileiro. Porém, tal adequação deve ser fundamentada em reais regulamentações atendendo aos requisitos apresentados por autoridades de saúde e jurídicas nacionais. Além disso, prover a interoperabilidade semântica dos dados a serem manipulados entre diferentes instituições e, por sua vez, o seu devido armazenamento em sistemas escaláveis e robustos para grande demanda de informações clínicas.

Como principais destaques deste trabalho, pode-se considerar a proposta de uma arquitetura desenvolvida e avaliada através de uma abordagem sociotécnica multimétodo. Ressalta-se ainda que toda adequação dos componentes da arquitetura quanto ao controle de acesso, privacidade e armazenamento das informações tem como base o arcabouço regimental brasileiro. Tais contribuições contemplam, principalmente, lacunas como a falta de estudos visando entender aspectos colaborativos ao utilizar PEP atrelado ao uso de *blockchain*, e a escassez de estudos nacionais que buscam se adequar às normas e regimentos locais.

## 4 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo serão apresentados os processos, métodos de pesquisa, e *design* das avaliações para execução do presente trabalho.

### 4.1 Caracterização da Pesquisa

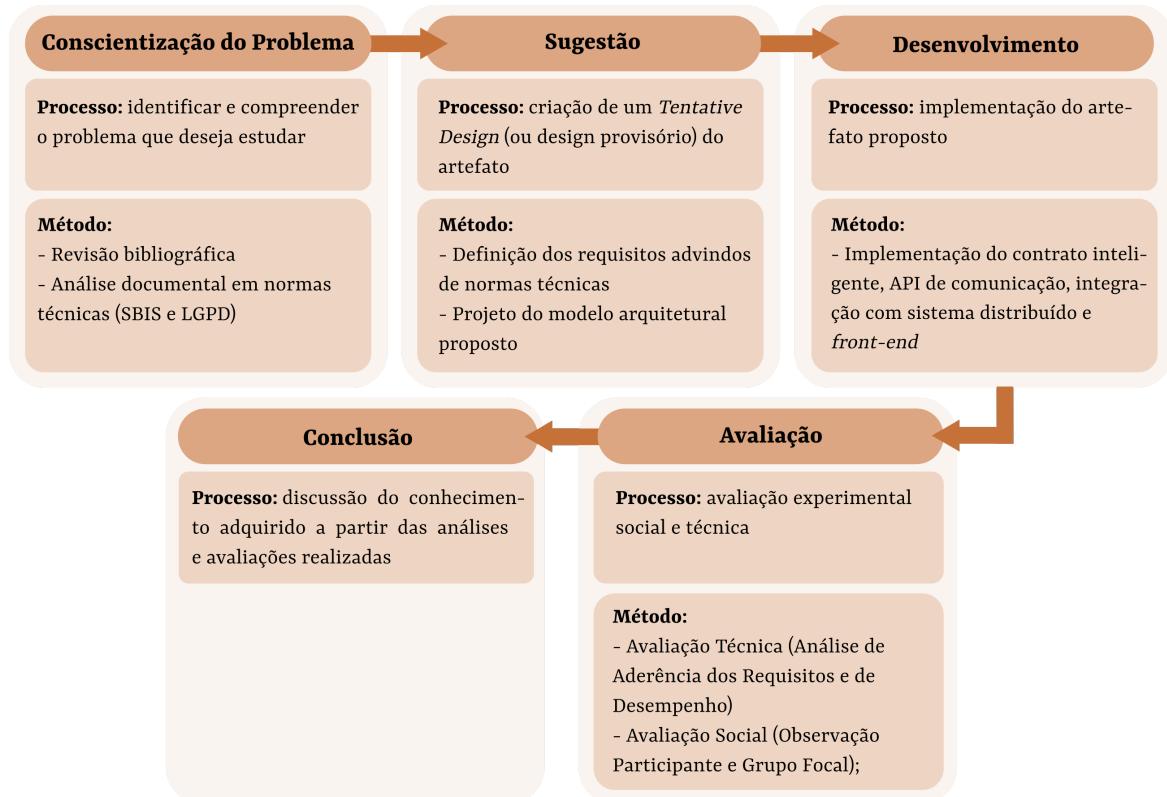
A natureza metodológica desta proposta é classificada como uma abordagem quali-quantitativa do tipo exploratória apoiada em *Design Science Research* (DSR). Conforme Vaishnavi e Kuechler (2004), DSR é um conjunto de técnicas analíticas que permitem o desenvolvimento de pesquisas nas variadas áreas. Tal método de pesquisa tem como objetivo estudar, pesquisar e investigar o artefato e seu comportamento tanto de forma acadêmica como organizacional (BAYAZIT, 2004). Em outras palavras, o DSR visa gerar conhecimentos sobre o projeto em questão e desenvolver soluções para melhorar sistemas, resolver problemas e criar novos artefatos.

Quanto à sua natureza exploratória, o trabalho segue os conceitos propostos por Piovesan e Temporini (1995), que diz uma “pesquisa exploratória, na qualidade de parte integrante da pesquisa principal, como o estudo preliminar realizado com a finalidade de melhor adequar o instrumento de medida à realidade que se pretende conhecer”. Dessa forma, pode-se definir o problema de pesquisa e formular sua hipótese com maior precisão. Por meio disto, em relação à presente pesquisa, propõe-se a apresentação de uma nova abordagem para o desenvolvimento de um PEP baseado em *blockchain*.

Em relação esta pesquisa ser do tipo qualitativa, a sua aplicação refere-se ao fato de que tem uma preocupação fundamental com o estudo e análise do mundo empírico em seu ambiente natural através da análise subjetiva, visto que todas as realidades dadas são importantes e devem ser exploradas (GODOY, 1995). Por fim, a abordagem quantitativa foi escolhida dada a importância de se avaliar quantitativamente sistemas computacionais. De acordo com Godoy (1995), o método quantitativo “preocupa-se com a medição objetiva e a quantificação dos resultados [...] evitando distorções na etapa de análise e interpretação dos dados, garantindo assim uma margem de segurança em relação às inferências obtidas”. Portanto, faz-se necessárias avaliações computacionais e experimentais através da coleta de dados metrificados e quantificáveis para análise de desempenho do artefato.

Com base em Vaishnavi e Kuechler (2004), as cinco etapas da presente pesquisa são apresentadas na Figura 6, sendo composta por: (i) Conscientização do Problema; (ii) Sugestão; (iii) Desenvolvimento; (iv) Avaliação e (V) Conclusão.

**Figura 6 – Procedimentos Metodológicos baseados em Design Science Research.**



Fonte: Adaptado de Vaishnavi e Kuechler (2004).

A primeira fase iniciou-se com a **Conscientização do Problema** na qual se planejou conduzir uma revisão de literatura e análise documental. Com a revisão de literatura, tornou-se possível identificar e analisar estudos relacionados ao desenvolvimento de abordagens referentes à presente pesquisa, além do fornecimento de suporte teórico e técnico para o desenvolvimento do artefato. Quanto à análise documental (BOWEN et al., 2009), que foi uma avaliação de documentos de forma que foi possível extrair o significado dos dados examinados e interpretados, obtendo a compreensão e possibilitando o desenvolver conhecimento empírico. Especificamente, ocorreu o entendimento do arcabouço regimental para adequação da proposta ao cenário brasileiro em termos do desenvolvimento de PEP e alinhamento à LGPD.

Em relação à fase de **Sugestão**, por meio do conhecimento extraído e das

diferentes versões foi proposto, como *tentative design* (BECK et al., 2013), um modelo arquitetural do artefato a ser desenvolvido. Este artefato foi modelado em diferentes camadas, ativos e participantes, e assumiu a forma de uma aplicação *web*.

Em seguida, na fase de **Desenvolvimento**, cujo foco consiste na implementação do artefato propriamente dito, foi realizada a implementação dos seguintes componentes:

1. Um contrato inteligente com a regra de negócio a ser executada na rede *block-chain* utilizada através de diferentes funções;
2. Uma API para comunicação com o contrato inteligente implantado na *blockchain*;
3. A integração com sistemas de armazenamento distribuído através da utilização de bibliotecas específicas;
4. Uma interface *front-end* para a aplicação *web* utilizada pelos usuários.

Na Fase de **Avaliação**, tem-se a condução de uma análise empírica com foco em questões sociotécnicas como os fatores colaborativos (COSTA et al., 2014), aderência de requisitos e desempenho computacional. Especificamente ao que concerne à análise colaborativa, o presente estudo estende o desenho de pesquisa introduzido por Soares et al. (2021). Finalmente, na etapa de **Conclusão**, os resultados do esforço de pesquisa são consolidados e ocorre a discussão do conhecimento adquirido.

## 4.2 Design das Avaliações

Esta seção configura-se com o desenho das avaliações social e técnica, com a descrição dos procedimentos para análises quantitativa e qualitativa.

### 4.2.1 Avaliação Técnica

Na **Avaliação Técnica** tem-se, inicialmente, a análise de aderência dos requisitos advindos de Normas Técnicas (SBIS e LGPD) com o objetivo de avaliá-los frente às funcionalidades do artefato proposto. Nesse caso, foram identificados os possíveis requisitos impactados pela adoção de *blockchain* e, em seguida, pretendeu-se evidenciar, com base numa análise de dados empíricos secundários, as potencialidades e desafios associados. Em especial, foram analisados os documentos e manuais<sup>7</sup> para

<sup>7</sup> <http://www.sbis.org.br/documentos-e-manuais>

a Certificação da SBIS, os quais destinam-se, genericamente, a Sistemas de Registro Eletrônico de Saúde (S-RES). As documentações sugerem que “o conjunto completo de subsistemas e componentes que compõem o S-RES, devidamente configurados de forma a atender aos requisitos especificados no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)”. A partir disso, foram analisados os requisitos impactados ao se utilizar *blockchain* em S-RES. Por sua vez, também ocorreu a análise sob à luz da LGPD (BRASIL, 2018) e, especificamente, para o contexto da saúde, visto que as informações médicas do paciente são consideradas como dados sensíveis. A análise documental foi baseada nos oito passos propostos por Bowen et al. (2009):

1. Reunir os textos relevantes;
2. Desenvolver um esquema de organização e gestão;
3. Fazer resumos dos originais para anotação;
4. Avaliar a autenticidade dos documentos;
5. Explorar a organização e vieses dos documentos;
6. Explorar informações básicas;
7. Fazer perguntas sobre o documento e, finalmente;
8. Explorar o conteúdo.

Os documentos foram lidos várias vezes, e todos os requisitos que poderiam ser impactados pela solução foram dispostos em uma planilha no *Google Sheets*. A partir disso, cada requisito foi analisado profundamente em relação aos componentes da arquitetura proposta, tanto considerando as camadas de uma forma geral, como os componentes específicos contidos nestas. Ao final, pôde-se obter um mapeamento das potencialidades e desafios identificados nos requisitos e princípios em relação às estratégias e características utilizadas para cada um ou um conjunto deles.

Adicionalmente, foi conduzido um experimento computacional de modo que se pudesse investigar quantitativamente as seguintes métricas: tempo de publicação dos dados inseridos e tempo de busca dos dados pesquisados. Ressalta-se que, além do entendimento do desempenho de como a solução se comporta em diferentes casos, tal experimento, de escopo quantitativo, faz-se relevante visto que o desempenho demonstra-se como um requisito de qualidade (ou não-funcional) necessário nos sistemas de forma a impactar diretamente na experiência do usuário.

As características do experimento foram elaboradas baseadas no próprio

funcionamento da arquitetura em relação às camadas e especificidades apresentadas na Seção 5. Posto isto, diferentes configurações quanto à forma de armazenamento, tamanho dos dados inseridos e pesquisados, tipos de operações e cenários realizados puderam ser projetados e executados. Ademais, métricas para análise estatística de dados também foram selecionadas. Toda a configuração do experimento será descrita com maiores detalhes na Seção 6.

#### 4.2.2 Avaliação Social

Em relação à **Avaliação Social**, foi realizado um quasi-experimento baseado na realização de tarefas com um grupo de usuários os quais interagiram sequencialmente com a interface do artefato (NIELSEN, 1994). Experimentos em grupo são relevantes para o presente estudo haja visto que possibilita uma visão complementar e compartilhada do uso da solução em um contexto social. Por sua vez, o usufruto do Grupo Focal (GF) se demonstra útil visto que pode-se coletar, por meio de interação do grupo, *insights* sobre as questões investigadas (MORGAN, 1996).

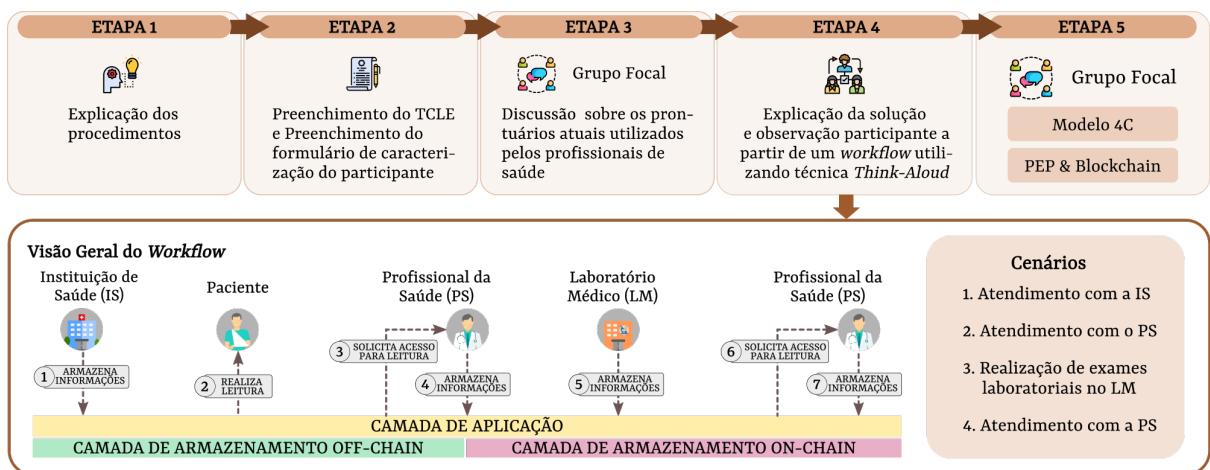
A seleção dos participantes do GF apoiou-se nos seguintes critérios: (i) maior de 18 anos, (ii) profissionais da saúde ou representantes de instituições de saúde e (iii) usuários que pudessem assumir papel de paciente. Tais restrições são baseadas nos tipos de usuários propostos para interação com o artefato (como será apresentado na Seção 5.1), os quais têm permissão legal para o manuseio de um prontuário. O recrutamento dos convidados foi realizado através da rede de contato dos autores e por meio da procura por especialistas no LinkedIn, visto que esta é uma rede social de profissionais e facilitaria a busca por profissionais da saúde, especificamente. Quando o retorno do através do LinkedIn era dificultado, os mesmos especialistas foram procurados em outras redes sociais, como o Instagram. Em seguida, foram enviados os convites individualmente por e-mail. A composição do convite se deu por uma breve descrição do projeto, seus riscos e benefícios, as etapas da coleta de dados e tempo de duração do GF.

Devido ao distanciamento social exigido pela pandemia da COVID-19, o experimento foi supervisionado de forma online através da ferramenta de videochamada *Google Meet*<sup>1</sup>. Nesse sentido, constatou-se que não houve danos importantes, pois a

<sup>1</sup> <https://meet.google.com/>

reação física do usuário poderia ser observada através da *webcam*, a interação com o artefato pelo espelhamento de tela e a discussão entre o grupo. A discussão entre o GF foi intermediada pela autora do presente trabalho, direcionando cada etapa do encontro. Conforme ilustrado na Figura 7, todo processo de avaliação social foi guiado através de um roteiro baseado em cinco etapas:

**Figura 7 – Fluxo da Avaliação Social.**



Fonte: Elaborado pelo autor.

Na **Etapa 1**, tem-se a explicação dos procedimentos, neste momento foram explanadas as etapas do experimento de uma maneira geral. Na **Etapa 2**, todos os participantes leram e assinaram o Termo de Consentimento Livre e Esclarecido (TCLE), através do qual puderam manifestar a sua anuência à participação na pesquisa, o TCLE pode ser encontrado no Apêndice A. Essa etapa também se deu pelo preenchimento do formulário de caracterização do participante (Apêndice B).

Na **Etapa 3** iniciou-se a discussão do GF sobre o uso dos PEPs atuais utilizados pelos profissionais de saúde. Em um primeiro momento, a intenção foi entender os processos ao utilizá-los, questões de privacidade, compartilhamento, benefícios e prejuízos em diferentes contextos. As questões que guiaram o primeiro momento estão presentes no Apêndice G. Foram realizados 2 GFs, cada um composto por quatro participantes seguindo o modelo de usuários proposto para utilização do artefato. A Figura 8 resume a caracterização dos participantes de cada GF, evidenciando os perfis profissionais e formação acadêmica, além de outras informações (os nomes foram omitidos preservando a confidencialidade). O primeiro GF ocorreu no dia 02/06/2021 com início às 17h e o segundo GF ocorreu no dia 04/06/2021 com início às

17h.

**Figura 8 – Caracterização dos Participantes.**

	ID*	Idade	Escolaridade	Área de Formação	Atuação Profissional	Atuação em Saúde
GRUPO FOCAL 1	Paciente1	24 anos	Médio**	Ciência da Computação	Supor te de Operações	-
	PS1	25 anos	Superior	Medicina	Médico(a)	1 ano
	IS1	29 anos	Mestrado***	Enfermagem	Bolsista do CNPq	7 anos
	LM1	32 anos	Especialização	Biomedicina	Biomédico(a)	2 anos e 6 meses
GRUPO FOCAL 2	Paciente2	27 anos	Superior	Ciência da Computação	Supervisor(a) - Gestão e Infraestrutura de TI	-
	PS2	40 anos	Doutorado	Medicina	Médico(a)/Professor(a)	16 anos
	IS2	35 anos	Mestrado	Enfermagem	Orientador(a) do Célula de Urgência e Emergência	14 anos
	LM2	25 anos	Superior****	Biomedicina	Biomédico(a)	1 anos e 6 meses

\* IDs dos participantes que representou o Paciente, Profissional de Saúde (PS), Instituição de Saúde (IS) e Laboratório Médico (LM), respectivamente, em cada Grupo Focal.

\*\* Superior em andamento

\*\*\* Doutorado em andamento

\*\*\*\* Mestrado em andamento

Fonte: Elaborado pelo autor.

Por sua vez, na **Etapa 4**, foi realizada uma breve explicação sobre a tecnologia *blockchain* e a abordagem proposta, visto que a presente pesquisa também visa entender os aspectos subjetivos que a tecnologia presente no artefato poderia causar aos participantes. Logo após, ocorreu o uso do artefato por meio da Observação Participante (COOPER et al., 2004) da realização de tarefas derivadas a partir de um *workflow* de modo que os usuários usufruíssem da técnica do *Think-Aloud* (RUBIN; CHISNELL, 2008). Esta técnica possibilita o pensamento em voz alta que é um método usado para coletar dados em testes de usabilidade no design e desenvolvimento de produtos. O guia para condução da Observação Participante contendo cenários e suas respectivas tarefas encontram-se disponíveis no Apêndice C ao F.

Finalmente, na **Etapa 5**, ao finalizar a execução dos cenários de uso com a ferramenta, uma nova discussão foi realizada orientando-se a partir de duas perspectivas: (i) os fatores de comunicação, coordenação, colaboração e cooperação delineados no Modelo 4C (COSTA et al., 2014); e (ii) o contexto de aplicação, isto é, o uso de

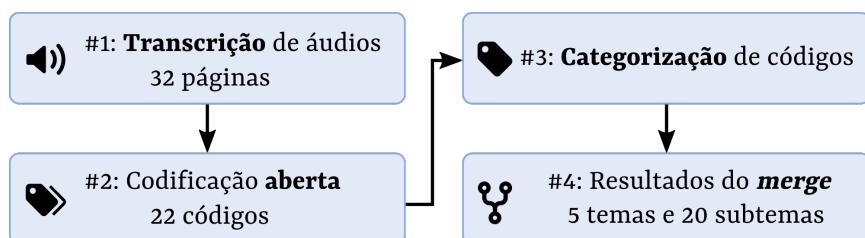
Prontuários Eletrônicos do Paciente baseados em *blockchain*. As questões utilizadas para orientar a discussão são apresentadas no Apêndice G.

As perspectivas mencionadas foram aplicadas em relação à interação dos participantes com o artefato implementado. Especificamente, em relação à Etapa 4, estabeleceu-se uma visão geral do *workflow* ilustrativo para derivação e execução dos cenários específicos em conformidade às normas vigentes (BRASIL, 2002b). Identificou-se, portanto, cinco perfis de usuário, são eles: o Paciente, o Profissional da Saúde (PS), a Instituição de Saúde (IS) e o Laboratório Médico (LM). Os tipos de participantes estão sendo descritos com mais detalhes na Seção 5.1, enquanto que o *workflow* para elaboração das tarefas realizadas por eles pode ser encontrado na Seção 5.3.4.

#### 4.2.2.1 Análise dos Dados do Grupo Focal

As etapas do processamento e da redução de dados foram apresentadas na Figura 9, inspiradas em Groeneveld et al. (2021). Primeiramente, as gravações dos GFs foram transcritas de áudio para texto (1). Em um segundo momento, as transcrições foram lidas várias vezes a fim de realizar uma codificação aberta do texto, como o apoio de ATLAS.ti<sup>2</sup>, uma ferramenta de análise de conteúdo, resultando em 22 códigos (2). A identificação dos códigos, inicialmente, foi baseada nas perspectivas abordadas anteriormente, que envolve o Modelo 4C e *blockchain* no contexto de PEPs, ou seja, uma codificação temática. Adicionalmente, novos códigos foram identificados também após a observações de padrões nas falas dos participantes. Em seguida, os códigos foram classificados em uma etapa de “categorização de códigos” (3), resultando em 20 subtemas e 5 temas principais (4) após a junção dos resultados de ambos os GFs.

**Figura 9 – Passos do Processamento de Dados do Grupo Focal.**



Fonte: Adaptado de Groeneveld et al. (2021).

<sup>2</sup> <https://atlasti.com/>

Ao total, oito participantes contribuíram com 212 minutos de discussão, totalizando 32 páginas de transcrição, com fonte Arial, tamanho 12. Cada GF com quatro participantes, o primeiro com duração total de 100 minutos e 14 páginas transcritas e o segundo com duração total de 112 minutos, com 18 páginas transcritas. Utilizando *emergent-systematic* (ONWUEGBUZIE et al., 2009) para análise de ocorrências, semelhante ao que foi utilizado por Groeneveld et al. (2021), os GFs foram organizados de maneira que foi possível verificar se os temas que surgiram no primeiro grupo também surgiram no segundo grupo, e vice-versa.

### 4.3 Conclusões do Capítulo

Este capítulo descreveu os procedimentos metodológicos adotados no presente estudo, iniciando-se na descrição das características da pesquisa, abordagens escolhidas e definição dos processos utilizados. Ao utilizar DSR o trabalho foi dividido em etapas, iniciando-se da conscientização do problema e tendo como conclusão os achados das avaliações técnica e social aplicadas sobre a arquitetura modelada e proposta. Os passos dos tipos de avaliações foram apresentados, incluindo um detalhamento sobre o experimento realizado com humanos a partir de GFs.

## 5 SOLUÇÃO PROPOSTA

A solução proposta tem como objetivo a criação de uma arquitetura, baseada em *blockchain*, que permite a inserção e gerenciamento de registros médicos referentes aos pacientes. Tal solução propicia ao paciente que este tenha o controle do acesso aos seus dados médicos quanto ao compartilhamento dessas informações com entidades terceiras, podendo autorizar ou não o compartilhamento. Esta arquitetura proposta busca agregar os benefícios da tecnologia *blockchain* em consonância aos requisitos da SBIS e questões legais da LGPD, ao atendimento das leis vigentes em relação à proteção dos dados e a melhoria da interoperabilidade das informações compartilhadas.

### 5.1 Papéis envolvidos na solução

Sabendo que dados clínicos referentes aos pacientes são informações sensíveis e que, segundo à Resolução CFM nº 1.638/2002, “compete à instituição de saúde e/ou ao médico o dever de guarda do prontuário”, a presente abordagem busca delimitar os papéis envolvidos na proposta. Além disso, em relação aos locais em que o prontuário do paciente deve estar disponível, a resolução prescreve que ambulatórios, enfermarias e serviços de emergência portem tais dados para possibilitar um tratamento adequado ao paciente. Considerando um fluxo comum, geralmente os médicos prescrevem exames para a detecção de possíveis diagnósticos. Os pacientes realizam exames em laboratórios e depois retornam ao médico, em grande parte dos casos, portando esses resultados em papel. Esse ciclo pode acontecer diversas vezes e com diferentes especialidades durante toda a vida do paciente.

Dada a identificação dos integrantes, propõe-se as seguintes categorias que irão interagir com a solução proposta:

- **Paciente** – indivíduo cuidado por um profissional da área da saúde;
- **Profissional da Saúde (PS)** – profissional cuja área de atuação está relacionada às ciências da saúde;
- **Instituição de Saúde (IS)** – estabelecimento que assegura assistência médica completa e preventiva e, por fim;
- **Laboratório Médico (LM)** – local onde testes patológicos são realizados com objetivo de obter informações sobre a saúde de um paciente.

## 5.2 Ativos e seu armazenamento na rede

Dados médicos são gerados em diferentes formatos e provenientes das mais distintas fontes e, ao serem associados a um paciente, podem gerar seu histórico clínico, isto é, seu prontuário. O prontuário requer um conjunto mínimo de informações que devem ser obrigatoriamente preenchidos, vide: identificação completa do paciente (nome, sexo, data de nascimento, nome da mãe, naturalidade e endereço), anamnese, exame físico e exames complementares com resultados e/ou hipóteses diagnósticas e tratamento prescrito e evolução diária do paciente. Além disso, deve constar nome legível, assinatura e número de inscrição no seu registro de classe (BRASIL, 2002b).

Preliminarmente, este trabalho propõe um ativo genérico a ser inserido denominado na abordagem de “Registro”, como apresentado na Figura 10. Os elementos que o compõem foram levantados considerando os participantes que irão manipulá-lo e o tipo de registro a ser inserido. Além disso, a modelagem dos de registro foi inspirada em recursos do padrão de interoperabilidade FHIR. O sistema, apesar de não integrar ao FHIR, utilizou-se dessa fundamentação na modelagem para facilitar uma futura integração completa com o FHIR. Portanto, atualmente, tem-se tabelas no banco de dados com seus respectivos atributos inspirados nos seguintes recursos (FHIR, 2019):

1. **Patient Resource**: os dados nestes recursos incluem informações sobre o paciente. Os seus atributos centram-se na informação demográfica necessária para apoiar os procedimentos administrativos, financeiros e logísticos;
2. **Practitioner Resource**: o profissional cobre todos os indivíduos envolvidos no processo de saúde e parte de suas responsabilidades formais sobre o paciente;
3. **Medication Administration Resource**: este recurso cobre a administração de todos os medicamentos e vacinas;
4. **Observation Resource**: as observações são um elemento central na área da saúde, usadas para apoiar o diagnóstico, monitorar o progresso, determinar linhas de base e padrões. A maioria das observações são simples afirmações de pares de nome/valor com alguns metadados, mas algumas observações agrupam outras observações logicamente, ou mesmo são observações de múltiplos componentes;
5. **DiagnosticReport Resource and Media**: um relatório de diagnóstico é um conjunto de informações geralmente fornecido quando a investigação é concluída. As informações incluem uma combinação de resultados atômicos, relatórios de

texto, imagens e códigos;

6. **QuestionnaireResponse Resource**: lista completa ou parcial de respostas a um conjunto de perguntas preenchidas ao responder a um questionário.

Ressalta-se que, nesta abordagem, a quantidade e os tipos de recursos podem ser generalizados, visto que existem muitos tipos. No entanto, para a implementação desta solução, por se tratar de uma PoC, foram selecionados apenas os recursos listados acima, baseando-se em um *workflow* ilustrativo genérico.

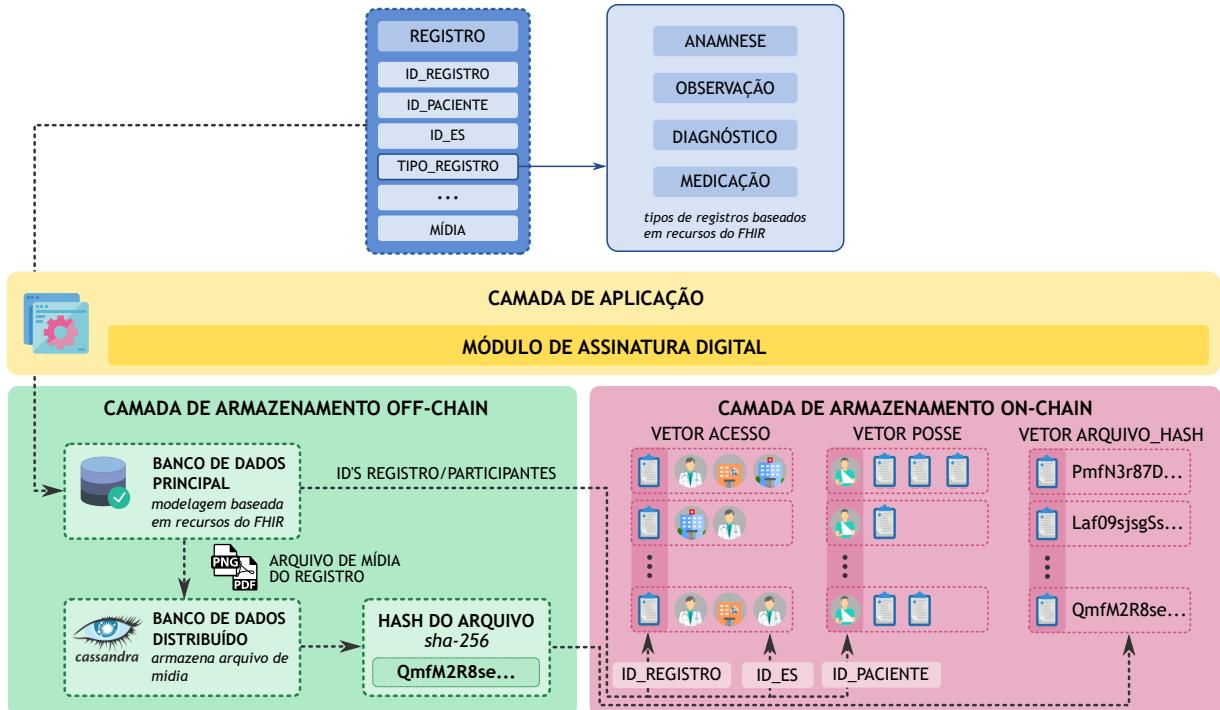
Posto isso, na Figura 10 o Registro é composto, primariamente, pelos atributos `idRegistro`, `idPaciente`, `idES`, estes dois últimos são referências para o paciente detentor das informações clínicas e a Entidade de Saúde (ES) que armazenou o Registro, respectivamente. Nesse caso, a ES refere-se ao PS, LM e IS. Por sua vez, os tipos de registros são baseados nos recursos do FHIR mencionados anteriormente, os quais estão sendo representados por `tipoRegistro`. Por exemplo, o `tipoRegistro` indica se o Registro é uma Anamnese, Exame, Observação ou Medicação. Especialmente, para cada tipo de recurso existem atributos específicos, o que demanda a criação de novos atributos para cada tipo de registro armazenado. Por exemplo, para o registro do tipo Medicação, deve ser registrado o tipo de medicação, dosagem, frequência diária e outras informações. Por fim, a mídia é o arquivo gerado na compilação das informações (e.g. laudo do resultado de um exame laboratorial).

### 5.3 Arquitetura de Software e Implementação

A organização da arquitetura baseia-se em duas estratégias de armazenamento utilizando a tecnologia *blockchain*: *on-chain* e *off-chain*. O primeiro refere-se a todos os dados brutos sendo armazenados na própria *blockchain*. Por sua vez, o segundo é relacionado à terceirização do armazenamento de alguns dados brutos fora da *blockchain*, enquanto que seus ponteiros e/ou suas referências são armazenados nela (SHUKLA; SAMET, 2020). A Figura 10 apresenta o ativo a ser adicionado e a arquitetura composta por três camadas, as quais serão detalhadas nas próximas seções:

1. Camada de Armazenamento *Off-chain*;
2. Camada de Armazenamento *On-chain*; e
3. Camada de Aplicação.

**Figura 10 – Visão Geral da Arquitetura de Software.**



Fonte: Elaborado pelo autor.

Nesta seção, antes da descrição das camadas, serão apresentadas as principais ferramentas e tecnologias utilizadas para implementação da PoC representativa da arquitetura proposta, as quais estão sendo descritas no Quadro 3:

**Quadro 3 – Perspetiva Tecnológica.**

Tecnologia	Descrição
<b>Solidity</b>	Linguagem de programação utilizada para escrever contratos inteligentes em aplicativos DApps, primariamente criada para programação na rede Ethereum. É uma linguagem com semelhanças com as linguagens JavaScript e C.
<b>Web3.js</b>	Coleção de bibliotecas que permitem a interação com um nó Ethereum local ou remoto usando HTTP, IPC ou WebSocket. Tais bibliotecas possibilitam, por exemplo, o envio de Éther de uma conta para outra, leitura e gravação dos dados de contratos inteligentes.
<b>Truffle e Ganache</b>	Truffle é um ambiente de desenvolvimento, framework de teste e pipeline de ativos para Ethereum. Ganache é um blockchain local para desenvolvimento rápido e faz parte da suite de desenvolvimento do Truffle. Ganache pode ser usado para implantar contratos, desenvolver aplicativos e executar testes.
<b>Remix</b>	IDE que permite desenvolver, implantar e administrar contratos inteligentes para Ethereum como blockchains.
<b>Rinkeby</b>	Rinkeby é a principal rede de teste de blockchain da Ethereum que se comporta de forma semelhante à rede principal (mainnet) da Ethereum. Normalmente usada por desenvolvedores para executar "testes" em seus aplicativos ou softwares baseados na blockchain Ethereum, de forma que não utilizam a crypto com valor real.
<b>Node.js e Express</b>	Node.js pode ser definido como um ambiente de execução Javascript server-side. Já Express.js é uma estrutura da web baseada no módulo Node.js HTTP principal e em componentes chamados middlewares. .
<b>MySQL</b>	MySQL é um Banco de Dados relacional (RDBMS – Relational Database Management Systems) com um modelo de cliente-servidor.
<b>Apache Cassandra</b>	Projeto do sistema de banco de dados distribuído altamente escalável de segunda geração, que reúne a arquitetura do DynamoDB, da Amazon Web Services e modelo de dados baseado no BigTable, do Google.
<b>Laravel</b>	Laravel é uma ferramenta de programação para desenvolvimento web baseado em PHP muito interativa e intuitiva. Framework projetado para melhorar a qualidade do software, simplificar a autenticação, facilitar o roteamento, facilitar o acesso e aumentar o poder da estrutura do site, possibilita amplas funções.
<b>HTML e CSS</b>	HTML é comumente utilizado para a criação de páginas online e aplicações da WEB. Os navegadores atuais recebem documentos em HTML que são processados renderização e apresentação do conteúdo online. Por sua vez, o CSS é mecanismo para adicionar estilo (cores, fontes, espaçamento, etc) ao documento HTML.

Fonte: Elaborado pelo autor.

### 5.3.1 Camada Armazenamento *On-chain*

A Camada de Armazenamento *On-chain* é referente às informações e operações que serão armazenadas e executadas na *blockchain* Ethereum (BUTERIN et al., 2013). Inicialmente, um contrato inteligente, implementado com a linguagem Solidity, armazena referências dos registros de cada paciente a fim de associar a posse de tais documentos. Além disso, o contrato inteligente permite o armazenamento das referências de cada participante da rede que pode ter acesso a um dado registro do paciente. O Pseudo-algoritmo 1, referente ao contrato inteligente implementado, será detalhado a seguir.

---

#### **Algoritmo 1:** Contrato Inteligente ControleRegistro

---

**Função** incluirPosse(*idRegistro*, *idPaciente*, *arquivoHash*):

Verifica se *msg.sender* é diferente de *administrador*  
*vetorPosse*[*idPaciente*][*idRegistro*] = true  
 inserir *hash* em *vetorArquivoHash*[*idRegistro*]

**Fim Função**

**Função** incluirAcesso(*idRegistro*, *idES*):

Verifica se *msg.sender* é diferente de *administrador*  
*vetorAcesso*[*idRegistro*][*idES*] = true

**Fim Função**

**Função** removerAcesso(*idRegistro*, *idES*):

Verifica se *msg.sender* é diferente de *administrador*  
*vetorAcesso*[*idRegistro*][*idES*] = false

**Fim Função**

**Função** recuperarRegistro(*idRegistro*, *idUser*):

Verifica se *msg.sender* é diferente de *administrador*  
**if** *vetorPosse*[*idUser*][*idRegistro*] == true || *vetorAcesso*[*idRegistro*][*idUser*] == true **then**  
**return** *vetorArquivoHash*[*idRegistro*]  
**else return** Usuário não tem acesso a esse Registro.

**Fim Função**

---

Através do contrato inteligente ControleRegistro é possível executar algumas funções relacionadas ao armazenamento das informações. Inicialmente, foram implementados três vetores: *vetorPosse*, *vetorAcesso* e *vetorArquivoHash* (ver Figura 10). O primeiro é manipulado quando um Registro é inserido, pois integrante da rede que o insere, referencia o detentor dos dados clínicos, ou seja, o Paciente.

Portanto, neste vetor são inseridos todos os Pacientes e, para cada um deles, os seus respectivos Registros. O segundo vetor está associado ao controle de acesso, no qual estão inseridos todos os Registros que os usuários da rede têm permissão de acesso. Já no vetorArquivoHash são inseridos todos os *hashs* referentes aos hashes dos arquivos armazenados na Camada de Armazenamento *Off-chain*. Existem três variáveis usadas como parâmetro das funções, são elas: *idRegistro* e *idES* que armazenam referências do banco de dados principal, e o *arquivoHash*, *hash* criptográfico da mídia armazenada.

Observa-se que há uma verificação no início de todas as funções apresentadas no algoritmo, como na linha 2, que checa se o *msg.sender* é diferente do administrador do sistema. A variável *msg.sender* indica quem é o proprietário do contrato implementado, isto é, o endereço de quem submeteu o contrato à rede Ethereum. Assim, a presente abordagem garante que as funções do contrato inteligente somente serão executadas pela Camada de Aplicação através das requisições realizadas pelo sistema. Tal estratégia evita que chamadas sejam realizadas diretamente ao contrato por outros meios que não sejam pela Camada de Aplicação.

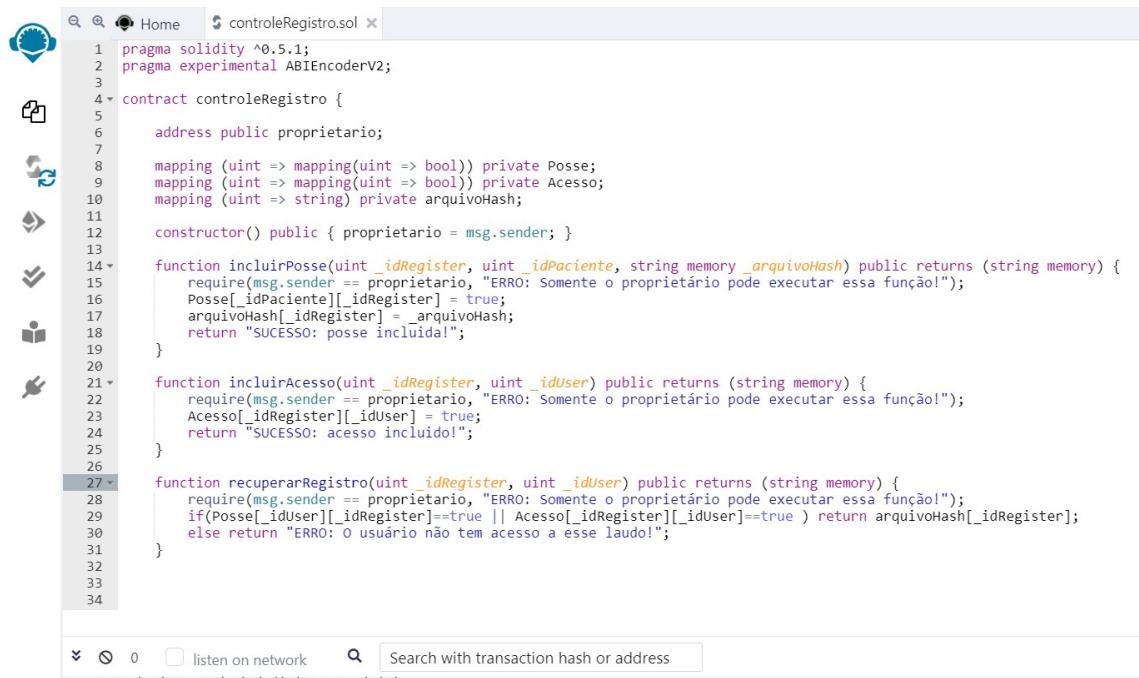
A primeira função do contrato inteligente é a *incluirPosse*, a qual permite associar o índice do Registro ao índice de determinado Paciente no *vetorPosse*, ambos são passados por parâmetro. Tal operação informa que a posse do Registro com *idRegistro* é do Paciente com o respectivo *idPaciente* atribuindo o valor *true* a essa posição (linha 3). Por sua vez, o *arquivoHash* do conteúdo inserido, que também é passado por parâmetro na função, está sendo armazenado na posição cujo o índice referencia o Registro adicionado (linha 4). Em relação à segunda função *incluirAcesso*, esta associa um Registro aos participantes que podem acessá-lo. Dessa forma, tal funcionalidade trata a respeito do controle de acesso a cada Registro. Ou seja, a função recebe como parâmetro um *idES* e um *idRegistro* indicando que determinado participante da rede pode ter acesso ao dado Registro. Para isso, foi atribuído na posição do *vetorAcesso* [*idRegistro*] [*idES*] um valor *true* (linha 8). Esta função será chamada quando o Paciente decidir autorizar o acesso de uma entidade de saúde a uma informação clínica de sua propriedade.

A terceira função, denominada de *removerAcesso*, tem o objetivo de desautorizar o acesso de uma entidade de saúde (*idES*) a um Registro (*idRegistro*). Ao invés de remover, visando a otimização do contrato a fim de minimizar os custos para

que não seja necessário reallocar todas as posições do vetor, está sendo atribuído o valor `false` na posição do `vetorAcesso[idRegistro][idES]` (linha 12). Por sua vez, a quarta função `recuperarRegistro`, recupera o *hash* do documento referente ao Registro armazenado no `vetorArquivoHash[idRegistro]`. Logo, apenas retorna o `arquivoHash` se o usuário que estiver solicitando tiver a posse ou acesso autorizado pelo proprietário do Registro solicitado (linhas 16 e 17). Ressalta-se que a função recebe `idUser` pois tanto o Paciente quanto a ES poderá chamar a função, porém para este último o registro retornará apenas se tiver as devidas permissões.

Uma versão do contrato inteligente na linguagem de programação Solidity (versão 5.1) pode ser visualizada na Figura 11. A implementação foi realizada na IDE Remix<sup>1</sup> online, como pode ser visto na Figura 11, apresentando as principais funções implementadas. A IDE Remix foi utilizada por proporcionar praticidade ao implementar contratos inteligentes, sendo possível a execução de diferentes recursos, como a compilação e possibilidade de simular transações à *blockchains* das funções implementadas no respectivo contrato, além da integração com a carteira do usuário.

**Figura 11 – IDE Remix e o Contrato Inteligente em Solidity**



```

1 pragma solidity ^0.5.1;
2 pragma experimental ABIEncoderV2;
3
4 contract controleRegistro {
5     address public proprietario;
6
7     mapping (uint => mapping(uint => bool)) private Posse;
8     mapping (uint => mapping(uint => bool)) private Acesso;
9     mapping (uint => string) private arquivoHash;
10
11     constructor() public { proprietario = msg.sender; }
12
13     function incluirPosse(uint _idRegister, uint _idPaciente, string memory _arquivoHash) public returns (string memory) {
14         require(msg.sender == proprietario, "ERRO: Somente o proprietário pode executar essa função!");
15         Posse[_idPaciente][_idRegister] = true;
16         arquivoHash[_idRegister] = _arquivoHash;
17         return "SUCESSO: posse incluída!";
18     }
19
20
21     function incluirAcesso(uint _idRegister, uint _idUser) public returns (string memory) {
22         require(msg.sender == proprietario, "ERRO: Somente o proprietário pode executar essa função!");
23         Acesso[_idRegister][_idUser] = true;
24         return "SUCESSO: acesso incluído!";
25     }
26
27     function recuperarRegistro(uint _idRegister, uint _idUser) public returns (string memory) {
28         require(msg.sender == proprietario, "ERRO: Somente o proprietário pode executar essa função!");
29         if(Posse[_idUser][_idRegister]==true || Acesso[_idRegister][_idUser]==true ) return arquivoHash[_idRegister];
30         else return "ERRO: O usuário não tem acesso a esse laudo!";
31     }
32
33
34

```

Fonte: Elaborado pelo autor.

A fim de integrar o contrato inteligente na *blockchain* com o sistema e possibilitar as devidas requisições aos participantes da rede, foi necessário o desenvolvimento

<sup>1</sup> <http://remix.ethereum.org/>

de uma *Application Programming Interface* (API) para tal comunicação. Por sua vez, a API foi desenvolvida utilizando *Node.js* e *Express.js*, e para comunicação com a *blockchain* foi utilizada a biblioteca *Web3.js*.

Na Figura 12, um provedor foi instanciado o qual tem por função abstrair uma conexão com a *blockchain* Ethereum para emitir consultas e enviar transações de alteração de estado assinadas. Nesse caso, para fins de simulação, a rede de teste Rinkeby está sendo utilizada. Nela pode-se utilizar Ether “falso” para simular as transações. A terceira linha contém a *Application Binary Interface* (ABI) do contrato inteligente que está sendo utilizado. A ABI é uma interface ou modelo do contrato que informa ao usuário quais métodos estão disponíveis nele. A linha 4 contém o endereço do contrato e a linha 5 o mnemônico. Este último, juntamente com a chave privada, são gerados quando a carteira do usuário é criada. As chaves pública e privada da conta do usuário na Ethereum são geradas com base em um mnemônico de doze palavras.

**Figura 12 – Conexão com a *blockchain* utilizando *Web3.js***

```

1  const HDWalletProvider = require('@truffle/hdwallet-provider');
2  const Web3 = require('web3');
3  const abi = JSON.stringify([ { "constant": false, "inputs": [ { "internalType": "uint256", "name": "_idR
4  const contractAddress = "0xC58Cd31aE6a80530DC69bb05B6f6498db038CE9A"
5  const mnemonic = " "
6  const infura = 'https://rinkeby.infura.io/v3/59eb9f1e90104e8eac3b13b2e68c8059';
7
8  const provider = new HDWalletProvider(
9    (mnemonic),
10   (infura)
11 );
12
13 const web3 = new Web3(provider);
14 const instance = new web3.eth.Contract(
15   |   JSON.parse(abi),
16   |   (contractAddress)
17 );
18
19 instance.setProvider(provider);
20
21 module.exports = {instance, web3};

```

Fonte: Elaborado pelo autor.

A Figura 13 apresenta um exemplo de uso da *Web3.js*. Ao inserir um registro na *blockchain*, primeiramente uma função que checa o documento na *blockchain* é executada. Caso um dado registro não esteja na *blockchain*, então será possível a sua inclusão. Caso contrário, uma mensagem é retornada ao usuário. A inserção do registro se dá através de comandos da *Web3.js*, como o *instance.method*, pelo qual é possível se comunicar com as funções desse contrato em específico. Observa-se que ao chamar a função, deve-se colocar o endereço (em “from”) da carteira utilizada para

possibilitar que as transações sejam efetuadas.

**Figura 13 – Chamada da função incluirPosse por meio da *Web3.js***

```

124  try {
125    if (checkRecord == true) {
126      return res.send({ "success": false, "message": `Record with the same ID already
127      registered to Patient!` });
128    } else {
129      var firstTimeChain = moment();
130      connectWeb3.instance.methods.incluirPosse(idRegister, idES, arquivoHash).send({
131        from: '0xD328E59ef45f08DC69Cd9f11BF2DB2125e7B0D49',
132        gas: 9999999,
133      }).then((record) =>{
134        connectWeb3.web3.eth.getBlock(record.blockNumber).then(function(block_info) {

```

Fonte: Elaborado pelo autor.

Semelhantemente, os métodos da biblioteca *Web3.js* são utilizados para invocar as demais funções do contrato inteligente à medida que estas forem sendo chamadas pelos usuários por meio da Camada de Aplicação apresentada com mais detalhes na Seção 5.3.3. A implementação da integração da API com a *blockchain* utilizando *Web3.js* pode ser encontrada no repositório GitHub<sup>2</sup> do presente trabalho.

### 5.3.2 Camada de Armazenamento *Off-chain*

Considerando a necessidade de manter a privacidade de dados sensíveis e dadas as limitações de escalabilidade da blockchain, esta abordagem propõe uma camada *off-chain* para armazenamento dos dados relacionados ao prontuário. O Registro, apresentado na Seção 5.2, referencia informações de Bancos de Dados Tradicionais e para um Banco de Dados Distribuído. Quando um Registro é inserido na rede através da requisição /inserirRegistro da Camada de Aplicação, primeiramente é armazenado em um Banco de Dados Principal, o qual é representado por uma tabela contendo os atributos (colunas) apresentados na Figura 10, possuindo *idES* e *idPaciente* como chaves (identificadores) que relacionam o Registro à tabelas que representam a entidade de saúde que inseriu o registro e ao paciente detentor das informações clínicas.

Por sua vez, o arquivo de mídia, de diferentes formatos, gerado ou anexado com as informações do Registro, é armazenado em um banco de dados distribuído, especificamente, o Apache Cassandra. O Apache Cassandra (LAKSHMAN; MALIK, 2010) é um dos bancos de dados NoSQL mais populares desenvolvidos pelo Facebook.

<sup>2</sup> <https://github.com/pamellasds/pep-blockchain-poc>

É um sistema totalmente descentralizado e oferece ótimo desempenho, durabilidade e tolerância a falhas sem comprometer a disponibilidade. O Cassandra possui sua linguagem de consulta denominada CQL (do inglês *Cassandra Query Language*) para interagir com o sistema.

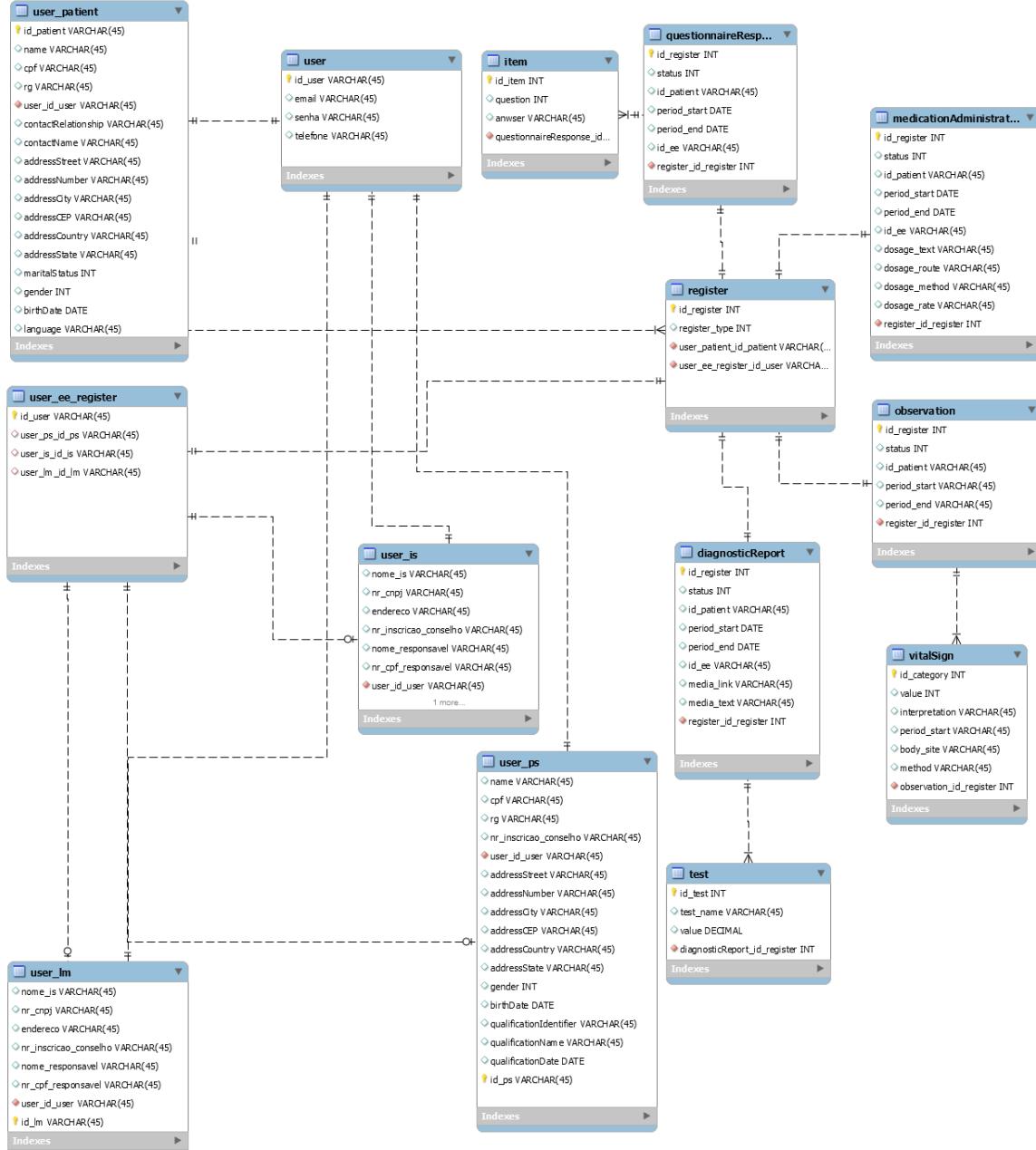
Existem diferentes sistemas de armazenamento, como visto na Seção 2.3. A presente proposta escolheu o Cassandra dadas as suas características e vantagens técnicas mencionadas anteriormente. Entretanto, além de utilizar-se de tais benefícios, a presente proposta visa adequar-se aos regimentos nacionais e técnicos. Dentre as possibilidades de sistemas de armazenamento (RAIKWAR et al., 2020), o Cassandra também foi escolhido por não ser um sistema imutável como outros. Isso proporciona a adequação ao “Direito de esquecimento”, por exemplo, estabelecido pelas leis de proteção aos dados sensíveis. Tal direito possibilita ao titular dos dados a exclusão de informações que o mesmo requerer dentro de um sistema.

O arquivo de mídia da Camada de Armazenamento *Off-chain* é convertido em um *hash* por meio do algoritmo de SHA-256. Por sua vez, este *hash* será armazenado na Camada de Armazenamento *On-chain*. Visto que na *blockchain* o *hash* ficará armazenado de forma imutável, esta técnica possibilitará futuras verificações de integridade do Registro original armazenado, servindo como sua impressão digital. Além disso, forma-se então um ponteiro que faz a referencia do arquivo original que está na Camada de Armazenamento *Off-chain* para a Camada de Armazenamento *On-chain*, além dos identificadores advindos do Banco de Dados Principal.

Para conexão com o banco de dados tradicional foi utilizado o MySQL, o qual foi integrado ao sistema por meio do framework Laravel da linguagem PHP. Por meio deste, os ativos da rede e os participantes foram modelados baseados nos componentes e atributos estabelecidos pelo padrão de interoperabilidade FHIR. A Figura 14 a seguir apresenta a modelagem do banco de dados relacional modelado para a Camada de Armazenamento *Off-chain*.

Em relação ao armazenamento no BDD, foi utilizado o Apache Cassandra atualmente como um serviço em nuvem mantido pelo DataStax Astra. O Cassandra é um banco de dados NoSQL, não relacional e colunar. Um banco NoSQL não emprega os conceitos tradicionais de banco de dados relacional, possuindo um *schema* bem flexível (*schemaless*). Porém, isso não impede que sejam utilizadas linguagens semelhantes ao SQL para interagir com sistemas NoSQL. Nesse caso, a linguagem

**Figura 14 – Modelagem Relacional baseada no FHIR.**



Fonte: Elaborado pelo autor.

CQL é utilizada para interagir com o Cassandra. O Cassandra realiza o armazenamento de chave-valor pelo qual os valores são armazenados e indexados por meio de uma chave. O BDD Cassandra é colunar pois, diferente dos bancos de dados relacionais que armazenam os dados em linhas (*rows*), persiste os dados por colunas criando um relacionamento através de um id. Adicionalmente, os dados podem ser persistidos no formato JSON.

Além disso, o Apache Cassandra é segmentado em *keyspaces*, *tables* (column families), *rows* e *columns*. Assim, fez-se necessária a criação de um *keyspace*,

o qual também define a replicação de dados em nós. A Figura 15 apresenta as colunas do *keyspace* criado para esta camada, o qual armazenará apenas os ids do registro, de paciente e da entidade de saúde que armazenou o registro, e o arquivo de mídia no formato base64, além da data de inserção.

**Figura 15 – Keyspace medical\_record.**

keyspace_name	table_name	column_name	clustering_order	column_name_bytes	kind	position	required_for_liveness	type
medical_record	medical_record	data	none	0x64617461	regular	-1	False	timestamp
medical_record	medical_record	media_base64	none	0x6d656469615f626173653634	regular	-1	False	text
medical_record	medical_record	patient_id	none	0x70617469656e745ff6964	regular	-1	False	text
medical_record	medical_record	ps_id	none	0x70735ff6964	regular	-1	False	text
medical_record	medical_record	register_id	none	0x72656769737465725f6964	partition_key	0	False	text

Fonte: Elaborado pelo autor.

O presente trabalho utilizou o *Node.js driver* disponibilizado pelo DataStax Astra para conectar-se ao banco de dados Cassandra. Este driver é disponibilizado para diferentes linguagens, visto que a API do presente artefato é implementada com o Node.js, foi escolhido o *driver* específico. Tal conexão pode ser vista na Figura 16.

**Figura 16 – Conectando ao Apache Cassandra pelo Node.js Driver.**

```

131
132  const client = new Client({
133    cloud: { secureConnectBundle: 'api/secure-connect-medical-record.zip' },
134    credentials: { username: ' ', password: ' ' },
135    keyspace: 'medical_record'
136  });
137
138  await client.connect();

```

Fonte: Elaborado pelo autor.

Como pode-se observar, foram definidos o nome de usuário para o ID do cliente do token de aplicativo, a senha do cliente do token do aplicativo e o caminho para o seu SCB (*secureConnectBundle*), este último é um pacote de credenciais de conexão para o admin o qual foi baixado da conta. O *snippet* do código apresentado na Figura 16 cria uma instância do cliente para se conectar ao banco de dados Cassandra.

Com o cliente instanciado pode-se então realizar as operações de leitura, escrita e remoção de dados no Apache Cassandra. As Figuras 17, 18 e 19 mostram *snippets* de código de um registro inserido, recuperado para leitura e deletado no BDD. Observa-se que para cada operação são necessárias a implementação de *queries* de consulta ao banco por meio da linguagem CQL. Com os parâmetros e com as devidas *queries* para cada operação, o método *execute* do *node.js driver* recebe os respectivos

parâmetros conforme o tipo de consulta.

**Figura 17 – Inserção com Node.js Driver ao BDD Cassandra.**

```
164 |     const params = [idRegister, idUser, idES, Date.now(), media_base64];
165 |     const query = `INSERT INTO medical_record (register_id, patient_id, ps_id, data, media_base64)
166 |                               VALUES (?, ?, ?, ?, ?)`;
167 |
168 |     await client.execute(query, params, { prepare: true });
169 |
170 |     await client.shutdown();
```

Fonte: Elaborado pelo autor.

**Figura 18 – Leitura com Node.js Driver ao BDD Cassandra.**

```
438     await client.connect();
439
440     const register = await client.execute(`SELECT register_id, patient_id, ps_id, data,
441     media_base64 FROM medical_record WHERE register_id = '${idRegister}'`);
442
443     await client.shutdown();
```

Fonte: Elaborado pelo autor.

**Figura 19 – Remoção com Node.js Driver ao BDD Cassandra.**

```
511     await client.connect();
512
513     const register_search = await client.execute(`SELECT * FROM medical_record WHERE
514                                                 register_id = '${idRegister}'
515                                                 and patient_id = '${idPatient}' ALLOW FILTERING`);
516
517     if(!register_search.rows.length){
518         return res.send({"success": false, "message": "Record "+idRegister+" not registered for Patient "
519                         +idPatient, "result": register_search.rows});
520     } else {
521         const register = await client.execute(`DELETE FROM medical_record
522                                                 WHERE register_id = '${idRegister}'`);
523
524         await client.shutdown();
525     }
526 }
```

Fonte: Elaborado pelo autor.

### 5.3.3 Camada de Aplicação

Esta camada consiste de uma interface entre o usuário e as Camadas de Armazenamento *On-chain* e *Off-chain*. Assim, é possível realizar requisições por parte dos integrantes, além de outras funcionalidades para satisfazer aos requisitos da SBIS, como o uso de assinatura digital. Esta proposta visa destacar como esta camada pode se comunicar com as outras a fim de acessar funcionalidades referentes ao armazenamento na *blockchain*. Os participantes definidos na Secção 5.1, como o

Paciente, PS, LM, IS podem interagir através das seguintes requisições:

- `/inserirRegistro`: Permite ao participante o envio de um Registro para a rede. Apenas o PS, LM e IS podem realizar a inserção de um Registro visto que cabe apenas estas entidades a emissão desses documentos legalmente.
- `/lerRegistro`: Permite ao PS, IS, LM e Paciente a leitura de um Registro da rede. Nesse caso, esta requisição retorna os dados clínicos para visualização.
- `/autorizarAcesso` ou `/desautorizarAcesso`: O Paciente libera acesso para o PS, LM ou IS da rede a um determinado Registro. Neste caso, uma entidade terceira não poderá escolher o registro a ser visualizado. O próprio paciente tem a lista de histórico de exames e irá liberar ao médico aquele que melhor se adequar a situação real. O Paciente pode também desautorizar a leitura de um Registro.
- `/assinarDigitalmente`: Possibilita ao médico a realização de sua assinatura digital dos documentos produzidos e registrados por ele.

O **Módulo Assinatura Digital** é proposto com o objetivo de adaptar a abordagem a alguns requisitos de segurança da SBIS em um segundo nível, para permitir que informações de saúde em mídia eletrônica também possam ser emitidas com o mesmo grau de legalidade que os documentos de mídia físicos (como papéis ou filmes). Além disso, a legalidade desses documentos pode ser atendida nessa abordagem pois a SBIS segue as especificações da Infraestrutura de Chaves Públicas (ICP-Brasil), uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão no Brasil. As resoluções da ICP-Brasil especificam o uso dos serviços de assinatura a fim de proporcionar o “não repúdio, identificação e confidencialidade, bem como para o uso de certificados de ponto” (MIRANDA et al., 2019). A ICP-Brasil é composta por uma cadeia de Autoridades Certificadoras (ACs). Esta última constitui-se de uma entidade, pública ou privada, responsável pela emissão, distribuição e gerenciamento dos certificados digitais. Já existe um conjunto<sup>5</sup> de ACs credenciadas para exercer tais papéis, visto que cumprem os critérios estabelecidos pelo Comitê Gestor da ICP-Brasil.

Este módulo é composto por um serviço que realiza a comunicação com os recursos técnicos de desenvolvimento disponibilizados pelas ACs. Algumas ACs privadas dispõem de documentações que possibilitam a integração com suas APIs através de um conjunto de rotinas e padrões para uso de seus serviços, sem envolver-

<sup>5</sup> <https://www.iti.gov.br/icp-brasil/estrutura>

se em detalhes na implementação da aplicação própria da AC. Sendo assim, esse módulo é adaptável conforme a(s) AC(s) escolhida(s) para integrarem-se à abordagem. Neste módulo, o anexo em mídia é inserido no Registro depois de sua assinatura digital, quando esta é solicitada através da requisição /assinarDigitalmente.

Como mencionado anteriormente, a Camada de Aplicação foi implementada com o objetivo de possibilitar que o usuário, através da interface, realize requisições de comunicação com a *blockchain*. Dessa forma, diferentes rotas foram implementadas para receber informações advindas da interface e inseridas pelos usuários da solução. Além da implementação das rotas na API. A Camada de Aplicação também foi composta pela interface Front-End, a qual foi implementada utilizando HTML, CSS, os *frameworks* Bootstrap e Laravel, e PHP. Baseado nos diferentes tipos de entidades de saúde e em alguns dados que o FHIR estabelece que sejam capturados, foram criadas telas de cadastros específicas.

### **5.3.3.1 Interface de Usuário**

Esta seção apresenta a interface implementada na Camada de Aplicação para interação dos diferentes participantes que usam o sistema e suas responsabilidades. Além disso, pode-se visualizar diferentes cenários de uso do sistema.

#### *5.3.3.1.1 Visão das Entidades de Saúde*

Em relação ao tipo de usuários que são ES, ou seja, PS, IS e LM, devem preencher suas informações em seus respectivos formulários de cadastro no sistema, como apresentados nas Figuras 20 e 21.

O usuário logado no sistema é possibilitado de realizar diferentes tipos de registros médicos para um paciente, em “Registrar Laudo” as opções de registros são apresentadas. O formulário de cada registro contém campos baseados em alguns atributos requeridos pelo FHIR para os recursos apresentados na Seção 5.2. A Figura 22 apresenta o formulário de cadastro de Anamnese, através do qual se tem uma série de perguntas referentes à queixa principal e histórico de doença do paciente. Nas Figuras 23, 24 e 25 tem-se a demonstração do registro de Observação, Exame e Medicção, respectivamente. Em relação às informações solicitadas na Observação, são referentes aos dados como sinais vitais que podem indicar, por exemplo, a temperatura,

**Figura 20 – Tela de Cadastro do PS.**

Prontuário Eletrônico do Paciente

Cadastrar Profissional da Saúde

**Dados Pessoais**

Nome  E-mail

Data de Nascimento  Gênero  Estado Civil

CPF  RG  Telefone

**Endereço**

CEP

Logradouro  Número  Bairro

Cidade  Estado  País

**Dados Profissionais**

Profissão  N° de Reg. no Conselho  Data de Registro

Fonte: Elaborado pelo autor.

**Figura 21 – Tela de Cadastro do LM e da IS.**

Prontuário Eletrônico do Paciente

Cadastrar Instituição de Saúde

**Dados da Instituição**

Nome  E-mail

CNPJ  N° de Reg. no Conselho  Data de Registro

**Endereço**

CEP

Logradouro  Número  Bairro

Cidade  Estado  País

**Dados do Responsável**

Nome  CPF

Senha

Fonte: Elaborado pelo autor.

a pressão sanguínea, dentre outras informações. Já o registro de Exame refere-se às informações resultantes de exames clínicos, como colesterol, glicose, etc. Por isso, solicita-se o nome do teste e seu respectivo valor. Especificamente, o LM tem apenas acesso ao registro de Exames, dentre os tipos de registros implementados. Por fim, o registro de Medicação é referente às medicações que o PS ou IS irá prescrever para

o paciente. Informações como o nome do remédio, o método, a dose e observações podem ser inseridas pelo usuário.

**Figura 22 – Tela de Cadastro do Registro de Anamnese.**

Fonte: Elaborado pelo autor.

**Figura 23 – Tela de Cadastro do Registro de Observação.**

Fonte: Elaborado pelo autor.

**Figura 24 – Tela de Cadastro do Registro de Exame.**

Fonte: Elaborado pelo autor.

**Figura 25 – Tela de Cadastro do Registro de Medicação.**

Fonte: Elaborado pelo autor.

Além das funcionalidades de cadastro de registros, todos os tipos de ES podem listar todos os registros dos pacientes aos quais têm acesso, e a lista de pacientes que o médico já submeteu algum registro médico ou de algum paciente que liberou o acesso de determinado registro de sua posse. Na Figura 26, na lista de pacientes, cada paciente é identificado pelo seu nome, data do último registro, um botão para informações mais detalhadas do paciente e um botão que direciona para

seus registros específicos. Por sua vez, na Figura 27, na lista de registros de todos os pacientes, tem-se o tipo de registro, o nome do paciente a qual pertence o registro, data do registro, tipo de acesso, e um botão que possibilita realizar o download do registro.

**Figura 26 – Tela de Listagem de Pacientes.**

Prontuário Eletrônico do Paciente			
<a href="#">Home</a> <a href="#">Registros</a> <a href="#">Pacientes</a> <a href="#">Registrar Laudo</a> <a href="#">Olá</a>			
Nome do Paciente	Último Registro	Informações do Paciente	Registros
João Silva	12/03/2021	<a href="#">i</a>	<a href="#">gp</a>
<b>Nome do Paciente</b>	<b>Último Registro</b>	<b>Informações do Paciente</b>	<b>Registros</b>

Mostrando página 1 de 1 [Anterior](#) [1](#) [Próximo](#)

Fonte: Elaborado pelo autor.

**Figura 27 – Tela de Listagem de Registros.**

Prontuário Eletrônico do Paciente				
<a href="#">Home</a> <a href="#">Registros</a> <a href="#">Pacientes</a> <a href="#">Registrar Laudo</a> <a href="#">Olá</a>				
Mostrando 10	Registros por página	Buscar:		
Tipo de Registro	Nome Paciente	Data de Registro	Acesso	Registro
Anamnese	João Silva	2021-05-01 23:18:40	Liberado	<a href="#">f</a>
Observação	João Silva	2021-05-01 23:18:40	Liberado	<a href="#">f</a>
Tipo de Registro	Nome Paciente	Data de Registro	Acesso	Registro

Mostrando página 1 de 1 [Anterior](#) [1](#) [Próximo](#)

Fonte: Elaborado pelo autor.

### 5.3.3.1.2 Visão do Paciente

A Figura 28 apresenta o formulário de cadastro utilizado pelo paciente. Todas as informações solicitadas são baseadas nos modelos de recursos baseados no FHIR. Devido às limitações do escopo de implementação da PoC e, visto que são muitas informações sugeridas, a Figura 28 apresenta uma parte delas.

Ao preencher todas as informações e clicar na confirmação de cadastro, o usuário deve ser cadastrado com sucesso. Ao acessar “Login”, o usuário pode entrar com suas credenciais de e-mail e senhas cadastrados no sistema. Ao estar logado, o menu terá a opção “Registros”, como pode ser visto na Figura 29, onde o

**Figura 28 – Tela de Cadastro do Paciente.**

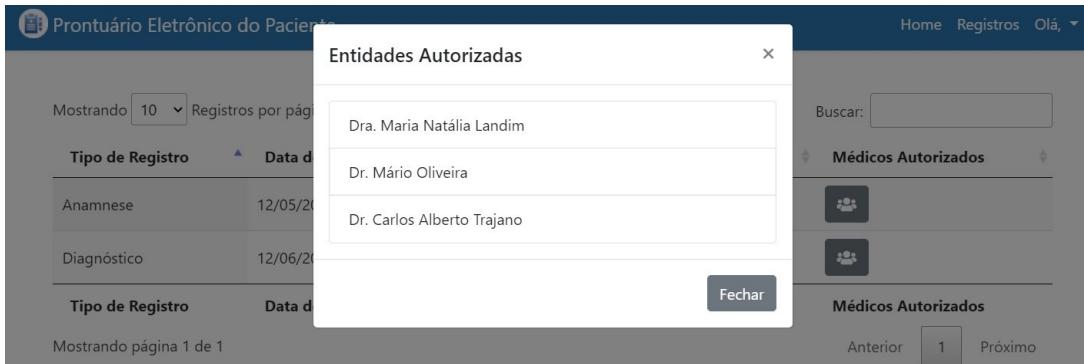
Fonte: Elaborado pelo autor.

usuário acessa os seus registros já cadastrados no sistema por alguma entidade de saúde. Nessa tela, além dos registros do paciente listados, o paciente poderá realizar o controle de acesso de suas informações médicas. Ao clicar em “Liberar” ou “Negar”, é possível inserir o identificador da ES a ser autorizada ou desautorizada a acessar o registro. Assim, o registro estará disponível no perfil de quem foi autorizado, e será desabilitado caso o paciente retire o acesso. Por meio do botão localizado na coluna “Médicos Autorizados”, o usuário poderá visualizar a lista de ES que o mesmo autorizou para ter acesso a determinado registro, como pode ser visto na Figura 30.

**Figura 29 – Tela de Registros do Paciente.**

Fonte: Elaborado pelo autor.

**Figura 30 – Tela de ES autorizadas.**

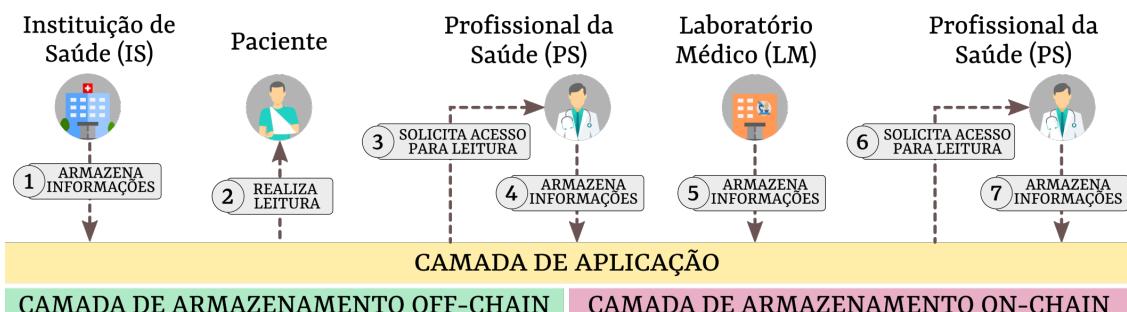


Fonte: Elaborado pelo autor.

#### 5.3.4 Demonstração do Workflow Ilustrativo

A Figura 31 apresenta um workflow ilustrativo utilizado para a demonstração da solução proposta, podendo ser generalizada para fluxos diferentes. Ressalta-se que um detalhamento deste fluxo foi utilizado no experimento social apresentado na Seção 7 para execução dos cenários.

**Figura 31 – Demonstração da Abordagem.**



Fonte: Elaborado pelo autor.

No Passo 1, supondo que o paciente tenha ido para a IS receber um atendimento, o representante da IS irá realizar os procedimentos iniciais e registrar as informações coletadas do paciente, como os sinais vitais. O Paciente poderá, a qualquer momento, realizar a leitura de seu histórico ou informações clínicas registradas, este último através da requisição /lerRegistro a qual realiza a chamada da função do contrato recuperarRegistro() (Passo 2).

Por sua vez, o paciente é encaminhado ao PS que, no Passo 3, através da requisição /autorizarAcesso, autoriza ao PS o acesso a suas informações registradas anteriormente. Assim, com o identificador do PS, a solução associa-o a um Registro

específico. Esta requisição chamará a função `incluirAcesso()` do contrato. Com o acesso liberado, o PS visualiza as informações concedidas a fim de entender o histórico clínico do paciente. No Passo 4, o PS solicita todas as informações necessárias para preencher uma Anamnese referente ao paciente e realiza o armazenamento por meio da requisição `/inserirRegistro` (Passo 4).

Considerando que o PS solicitou um exame laboratorial para o paciente que irá até um LM realizá-lo. Ao finalizar a produção dos resultados dos exames solicitados, o LM armazena, no Passo 5, os resultados referenciando o paciente como sendo o detentor de tal Registro. Isso possibilitará que apenas o Paciente tenha controle sobre suas informações, uma vez gravado em *blockchain*. Novamente, o Paciente volta ao PS o qual realiza a leitura dos exames após o Paciente ter liberado o acesso e registra a medicação adequada (Passos 6 e 7).

#### 5.4 Conclusões do Capítulo

Este capítulo apresentou a solução proposta do presente trabalho iniciando-se pela definição dos participantes da rede e dos ativos a serem armazenados. Então, a visão geral da arquitetura de software e sua implementação foram descritas, separando-a em três camadas: Camada de Armazenamento *On-chain*, Camada de Armazenamento *Off-chain* e Camada de Aplicação. Para cada camada, foram descritos seu funcionamento, estrutura e tecnologias utilizadas, de forma que buscou-se justificar cada componente utilizado. A regra de negócio do contrato inteligente da solução foi apresentada na Camada de Armazenamento *On-chain*, onde as funções de todo o pseudocódigo do contrato inteligente a ser utilizado foram descritas. As tecnologias foram apresentadas, inicialmente, integrando-as na explicação de cada camada, através da qual buscou-se apresentar a formação da camada de maneira teórica e prática.

Quanto à apresentação da Camada de Aplicação, buscou-se demonstrar as visões de cada tipo de usuário do sistema. Por fim, este capítulo visou apresentar uma demonstração ilustrativa sobre o funcionamento do fluxo da solução proposta. O fluxo mostrado apresentou uma situação geralmente recorrente na vida do paciente, quando este realiza consultas e submete-se a exames. Esta demonstração objetivou mostrar a integração e funcionamento entre as camadas da abordagem proposta.

## 6 AVALIAÇÃO TÉCNICA

Neste capítulo serão apresentadas as avaliações técnicas realizadas no presente estudo. Tem-se duas dimensões de análise, em que na primeira busca-se identificar as potencialidades e desafios de aderência aos requisitos advindos de normas técnicas nacionais, como SBIS e LGPD. Por outro lado, estabelece-se um experimento computacional visando entender o desempenho da PoC implementada e como tal requisito de qualidade pode afetar na experiência do usuário.

### 6.1 Avaliação de Aderência aos Requisitos advindos de Normas Técnicas Nacionais

Nesta seção será realizada uma avaliação quanto aos requisitos oriundos do Manual de Certificação da SBIS e identificados na LGPD em comparação com as camadas e componentes da arquitetura proposta.

#### 6.1.1 Requisitos de Conformidade segundo a Certificação da SBIS

Nesta seção serão apresentados o subconjunto de requisitos advindos do Manual de Certificação da SBIS (2019) alcançados pela solução proposta. Dessa forma, foram extraídas e apresentadas as potencialidades e os desafios encontrados ao confrontar a solução ao subconjunto. Uma descrição mais detalhada das estratégias utilizadas está sendo apresentada a fim de justificá-las com base no manual.

Para que um S-RES seja credenciado, necessita-se que os requisitos de segurança, estrutura, conteúdo e funcionalidades sejam conforme os critérios especificados. Em relação aos requisitos de segurança, o Manual de Certificação da SBIS (2019) classifica em dois níveis: Nível de Garantia de Segurança 1 (NGS1) e Nível de Garantia de Segurança 2 (NGS2). No NGS1 não pretende-se a eliminação do papel, o registro é impresso e a assinatura manuscrita do profissional deve ser aplicada.

Por sua vez, para NGS2, além dos requisitos de NSG1 atendidos, devem-se adicionar certificações de assinatura e certificação digital segundo critérios da ICP-Brasil. Quanto aos requisitos de estrutura e conteúdo (ESTR.) e funcionalidades (FUNC.), o manual classifica de acordo com sua área: (i) assistencial, S-RES ao cuidado a pessoa como sistemas para consultórios, clínicas, hospitais, pronto atendi-

mento e unidades básicas de saúde, ou (ii) básica, S-RES voltado a parte específica ou processos do cuidado ao indivíduo, como serviços de prescrição, imunização, *home-care*, serviços de diagnóstico e terapia, telemedicina, saúde ocupacional ou repositórios de dados demográficos e clínicos.

O manual da SBIS lista e descreve todos os requisitos e sub-requisitos relacionados aos grupos mencionados, contendo, ao todo, 58 requisitos. Ao defrontar a solução proposta neste trabalho aos requisitos descritos no manual, identificou-se que um subconjunto deles pode ser impactado pelas estratégias utilizadas. Ressalta-se que esta avaliação visa apresentar os potenciais requisitos que podem ser atrelados ao uso do *blockchain*, visto que não são todos os 58 requisitos que necessitam dessa intersecção. Na Tabela 4 são apresentados os potenciais requisitos a serem impactados pelo uso da solução.

**Quadro 4 – Subconjunto dos potenciais requisitos impactados pelas estratégias utilizadas.**

ID	Requisitos de Conformidade	Descrição
<b>NGS1.02</b>	Identificação e autenticação de pessoas	Permitir que os usuários possam ser identificados e autenticados, além de protegidos contra falhas
<b>NGS1.04</b>	Autorização e controle de acesso	Conceder autorizações para acesso dos dados por terceiros e controlar o acesso de pessoas ao sistema
<b>NGS1.05</b>	Disponibilidade do RES	Garantir que os dados possuam cópia de segurança para manter a integridade dos dados
<b>NGS1.07</b>	Segurança de Dados	Salientar que os dados devem ser armazenados em um Sistema de Gerenciamento de Banco de Dados com validação de acesso aos dados
<b>NGS1.12</b>	Privacidade	Garantir o consentimento, por parte do paciente, no compartilhamento de suas informações pessoais de saúde somente para pessoas autorizadas
<b>NGS1.13</b>	Autenticação de usuário utilizando certificado digital	Apresenta os critérios e normas para o uso de certificados digitais em nível de segurança 1
<b>NGS2.01</b>	Certificado digital	Apresenta os critérios e normas para o uso de certificados digitais em nível de segurança 2
<b>NGS2.02</b>	Assinatura digital	Aponta itens de validação e formatos das assinaturas digitais
<b>NGS2.04</b>	Digitalização de documentos	Informar as assinaturas que devem estar presentes nos documentos digitalizados e autorizações que permitam a digitalização desses documentos
<b>ESTR.04</b>	Dados clínicos	Regulamenta como os dados clínicos devem ser tratados
<b>FUNC.02</b>	Problemas/condições de saúde e outras questões	Garantir que os dados de um paciente sejam armazenados de forma cronológica e acessíveis para consultas
<b>FUNC.17</b>	Médico-legal	Trata da manutenção da cronologia de eventos, assegurando que dados retroativos possam ser registrados
<b>FUNC.18</b>	Atores	Delimitação do papel de cada pessoa com autorização para interagir com o sistema com as devidas restrições para cada
<b>SGED.01</b>	Gerais	Trata dos arquivos que devem ser suportados pelo sistema assim como obter os dados clínicos e os métodos de indexação dos arquivos

Fonte: Elaborado pelo autor.

Em relação às **Potencialidades**, nas Seções 6.1.1.1 a 6.1.1.6 discute-se detalhes de como a solução proposta busca atender os requisitos de conformidade da Tabela 4. Tal análise de caráter descritivo é realizada confrontando o referencial teórico relativo aos documentos analisados, sobretudo quanto ao Manual de Certificação da SBIS. Por outro lado, tem-se também a análise do requisito considerado ainda como **Desafio**, como apresentado na Seção 6.1.1.7.

#### ***6.1.1.1 Identificação e autenticação de pessoas / Autorização e controle de acesso / Privacidade / Atores***

O requisito de ‘Identificação e autenticação de pessoas’ (NSG1.02) e ‘Autorização e controle de acesso’ (NSG1.04) devem impedir o acesso ou visualização do PEP por pessoas não autorizadas, além do gerenciamento adequado dos diferentes papéis envolvidos. Tais ações podem ser realizadas através de mecanismos de configurações das permissões e restrições de acesso. Adicionalmente, requisita-se a delegação de poderes, através do qual se deve conter minimamente informações que identifiquem o delegante, o delegado, o período de vigência, o tipo de acesso, dentre outras. Por sua vez, a questão de ‘Privacidade’ (NGS1.12), referente à privacidade, requer que a solicitação do consentimento no uso dos dados do usuário seja realizada. Inclui-se também o registro do propósito de uso das informações pessoais de saúde. O requisito relacionado à ‘Atores’ (FUNC.18) refere-se aos tipos de usuários do sistema. Dentre as normas, solicita-se que seja realizada a identificação de fornecedor da informação, assim como os dados mínimos deste. Deve-se garantir que toda a informação registrada no PEP seja atribuída a um ator responsável, independentemente se este foi o autor da informação ou não.

Em suma, tais requisitos apresentam questões quanto ao controle de acesso das informações pelos diferentes atores do sistema. Ressalta-se que a presente solução tem como principal objetivo garantir que o próprio paciente tenha controle dos seus dados, gerenciando todos os acessos no compartilhamento para terceiros. Portanto, confrontando as características dos requisitos NGS1.04, NGS1.12 e FUNC.18, este trabalho sugere que o paciente possa delegar determinadas ações aos profissionais que este deseja compartilhar suas informações clínicas. Isso possibilita que tais registros sejam identificados por seus responsáveis, sejam eles o detentor das informações,

como também aos usuários terceiros habilitados.

Ao realizar uma comparação com a solução apresentada, através do Contrato Inteligente percebe-se que a configuração de controle de acesso dar-se-á pelas funções que manipulam o `vetorPosse` e/ou `vetorAcesso` do contrato inteligente, a saber: `incluirPosse()`, `incluirAcesso()`, `removerAcesso()` e `recuperarRegistro()`. Como apresentado na Seção 5.3.1, tais vetores armazenam identificadores referentes aos dados de usuários e de registros armazenados no BDD (`idRegistro`, `idUsuario`). Esta escolha mantém dados confidenciais fora da cadeia e armazenam ponteiros de troca de referências na cadeia (ZHANG et al., 2018).

Dessa forma, este mecanismo possibilita o atendimento de dois sub-requisitos da certificação: concessões de autorização, relacionadas à segurança dos dados e restrições de acesso ao RES adicionadas pelo paciente, referente à privacidade. Tais requisitos podem ser contemplados visto que o paciente pode inserir ou remover autorizações de acesso à seus registros clínicos aos atores específicos do PEP.

As concessões são através da função `incluirAcesso()` ou `removerAcesso()`. Ambas foram implementadas para modificar a informação sobre o acesso de uma parte ao registro no `vetorAcesso[idRegistro][idES]`, sendo `incluirAcesso()` atribuição para booleano verdadeiro, representando permissão de acesso para o usuário solicitante e `removerAcesso()` atribuição booleana para falso indicando que o usuário em questão não deve ter acesso aos dados do paciente. O sub-requisito de acesso ao RES pelo paciente é satisfeito com a função `recuperarRegistro()`. Esta verifica se o solicitante tem a posse dos dados ou tem acesso permitido aos dados retornando, em caso de sucesso, as informações referentes ao registro do paciente armazenado no BDD são apresentadas.

#### **6.1.1.2 Disponibilidade do RES**

O requisito de ‘Disponibilidade do RES’ (NGS1.05) diz respeito à disponibilidade do S-RES. Este demanda que os sistemas possibilitem a restauração de cópias de segurança de forma que contenham informações suficientes para restauração. Tal requisito pode ser atendido devido à descentralização da rede e persistência dos dados, visto que os nós estabelecem conexão com vários outros nós da rede e mantém os blocos de informações de maneira distribuída. Dessa forma, os dados continuarão

disponíveis, pois as informações poderão ser acessadas a partir das outras cópias existentes. Tais características garantem que os usuários do S-RES utilizem as informações registradas na *blockchain* sempre que for necessário, mesmo se um ou mais nós forem desativados.

Além disso, um dos sub-requisitos do NGS1.05 é a integridade na recuperação dos dados. Tal atendimento é possível pois o `vetorArquivoHash` armazena o *hash* de todos os documentos inseridos. Este *hash* é uma impressão digital criptográfica exclusiva do documento armazenado inicialmente, o que garante uma futura verificação da integridade das informações na geração e na restauração da cópia de segurança.

As mídias geradas em cada tipo de registro do paciente são codificadas pelo algoritmo de hash SHA-256 e armazenadas em *blockchain* através da Camada de Armazenamento *On-chain*. SHA significa *Secure Hash Algorithm* e foi projetado pela National Security Agency (NSA) (ROY, 2005). É um hash criptográfico unilateral e altamente seguro pois a mensagem criptografada por este algoritmo nunca pode ser descriptografada (JAHAN et al., 2020; HAQUE et al., 2020). A partir disso, pode-se então, verificar a integridade dos dados comparando o hash computado (a saída de execução do algoritmo) a um valor de hash conhecido, esperado e inalterado. Neste caso, calcular o hash de um arquivo baixado e comparar o resultado com um resultado hash publicado anteriormente na *blockchain* pode mostrar se a mídia foi modificada ou adulterada.

#### **6.1.1.3 Problemas/condições de saúde e outras questões / Médico-legal**

Os requisitos relacionados à ‘Problemas/condições de saúde e outras questões’ (FUNC.02) e ‘Médico-legal’ (FUNC.17), de um modo geral, solicita que os dados do paciente sejam apresentados de maneira holística. De forma que seja possível buscar um entendimento integral do que ocorre com a saúde do paciente. Deve-se registrar todo o período de vida do sujeito da atenção, incluindo a condição de saúde e intervenções, que devem ser obrigatoriamente visualizadas de forma cronológica em relação ao registro de tempo do evento.

Como o S-RES deve possibilitar a ordem cronológica das informações (IBARRA et al., 2019) e que tais requisitos dizem a respeito disso, a presente solução atende-os visto que *blockchain* possibilita o armazenamento com registro de tempo.

Na estrutura de dados `vetorPosse` definida na Seção 5.3.1, são atribuídas todas as referências dos registros relacionados a cada paciente. Essas referências são inseridas no vetor à medida que um participante armazena um registro na rede através da requisição `/inserirRegistro` disponibilizada na Camada de Aplicação. Para cada paciente referenciado em um índice do `vetorPosse`, um conjunto de registros armazenados em lista estão dispostos cronologicamente conforme inseridos, sendo também análogo para o `vetorArquivoHash`. Tais características são atendidas por meio da lógica do contrato inteligente aplicada na Camada de Armazenamento *On-chain*.

Além disso, destaca-se também a característica intrínseca à própria tecnologia *blockchain*, que é o fato de que esta realiza apenas operações *append-only*. Isto é, apenas de anexação, armazenando um conjunto de transações ordenadas por tempo, ou seja, cronologicamente (RAMACHANDRAN et al., 2020). Dessa forma, as transações históricas não podem ser excluídas ou modificadas sem invalidar a cadeia de *hashes*. Isso impede a violação da cronologia das inserções dos registros clínicos realizados na *blockchain*, mantendo uma rastreabilidade dos registros com suas devidas informações (LUU et al., 2016).

#### **6.1.1.4 Dados clínicos / Gerais**

Os requisitos de ‘Dados clínicos’ (ESTR.04) e ‘Gerais’ (SGED.01) remetem-se, no geral, à estrutura dos dados clínicos e à forma como estes registros são armazenados. Os principais ativos a serem inseridos e visualizados contêm uma série de informações e métodos relacionados aos exames e procedimentos realizados. Estas informações geralmente são compiladas em arquivos de diferentes formatos. Considerando as limitações de escalabilidade, tal requisito é atendido na Camada de Armazenamento *Off-chain*. As informações brutas dos registros do paciente são armazenadas no Banco de Dados Principal cuja modelagem segue o padrão relacional, também solicitado por estes requisitos. Tal modelagem baseia-se, de forma preliminar, no modelo FHIR como apresentado na Seção 5.2, considerando as variadas estruturas clínicas de diferentes tipos de laudos médicos.

Por sua vez, os arquivos de mídia referentes aos exames produzidos são guardados em um BDD conforme mostrado na Seção 5.3.2. Esta escolha de *design*, como já mencionado, visa mitigar problemas de escalabilidade, visto que atualmente

pode-se tornar inviável armazenar um arquivo completo em *blockchain*. Portanto, no contrato inteligente, o `vetorPosse` armazena todas as referências de todos os dados clínicos armazenados no Banco de Dados Principal e no BDD, e o `vetorArquivoHash` todos os *hashes* do documento clínico. Assim, esses links podem ser armazenados em uma transação de *blockchain* e estariam disponíveis para acesso aos dados clínicos. Deve-se mencionar também que o uso de BDDs agregados à *blockchain* possibilita o armazenamento de diferentes formatos de mídia de forma distribuída.

#### **6.1.1.5 Segurança de Dados**

O requisito ‘Segurança de Dados’ (NGS1.07) sugere que os dados devem estar estruturados de tal forma que seja possível a importação de dados. Dentre as características, deve-se garantir a verificação de integridade dos dados, a utilização de SGBD, dentre outras.

O uso de *blockchain* na solução pode contribuir com a implementação nas seguintes exigências de segurança de dados exigidos pela certificação: i) impedir alteração e exclusão de dados ii) verificação de integridade dos dados e iii) utilização de Sistema de Gerenciamento de Banco de Dados (SGBD). A imutabilidade, intrínseca ao *blockchain*, proporciona a não exclusão e alteração de transações já submetidas, o que garante que ações de correção ou edição preservem os dados. O `vetorArquivoHash` é manipulado apenas para operações de inserção nas funções do contrato inteligente. A verificação da integridade acontece semelhante ao NGS1.05, em relação ao `vetorArquivoHash`. Por fim, a utilização de gerenciamento de SGBD pode ser alcançada na Camada de Armazenamento *Off-chain*.

#### **6.1.1.6 Autenticação de usuário utilizando certificado digital / Digitalização de documentos**

Os requisitos associados a tais temáticas são NGS1.13, NGS2.01, NGS2.02 e NGS2.04. As determinações para o uso de certificado digital e assinatura digital são satisfeitas através do uso do Módulo Assinatura Digital. Os usuários poderão incluir certificados digitais, tornando-se aptos para realizar assinaturas digitais em documentos que, agregada com a assinatura dos responsáveis pela digitalização do documento, terão mais uma camada de confiabilidade.

#### **6.1.1.7 Escalabilidade e performance (FUNC.12)**

Como já mencionado, a *blockchain* ainda enfrenta desafios quanto à escalabilidade. Existem três aspectos que envolvem essa problemática: taxa de transferência, armazenamento e rede (XIE et al., 2019). Tal limitação dar-se devido à redundância de um grande número de nós de processamento que mantém, cada um deles, uma cópia completa do *ledger* distribuído. Para mitigar tal problema, esta solução propõe a adoção da Camada de Armazenamento *Off-chain*. Entretanto, o alto *throughput* e a baixa latência tem o potencial de causar um gargalo na rede, pois são necessárias mais verificações à medida que o número de transações e nós aumentam (AGUIAR et al., 2020). Em outras palavras, ao trabalhar com sistemas de saúde, o alto *throughput* pode afetar no registro de um diagnóstico. Quanto à latência, como os sistemas de saúde podem ser acessados com frequência, atrasos podem afetar a análise de um exame, por exemplo. Além disso, tentar minimizar problemas de escalabilidade pode implicar em *trade-offs* que envolvem e afetam outras características relevantes da *blockchain*.

A fim de alcançar uma performance adequada através artefato proposto e, adicionalmente, usufruir dos benefícios do uso de *blockchain*, propõe-se o uso da técnica *Off-chain* implementada na Camada de Armazenamento *Off-chain* descrita na Seção 5.3.2. Com o uso dessa técnica, não há a necessidade de realizar a inserção dos registros brutos em *blockchain*. A Camada de Armazenamento *On-chain* armazena os ponteiros para os dados brutos dos registros armazenados na Camada de Armazenamento *Off-chain*.

#### **6.1.2 Requisitos de Conformidade segundo a Lei Geral de Proteção de Dados**

Nesta seção, serão apresentadas as análises relacionadas aos princípios da LGPD em contraste com a solução proposta. Sabe-se que, com a implantação desta lei, as empresas devem adequar-se aos requisitos necessários para proporcionar a devida proteção dos dados de seus clientes. Em suma, a lei impõe que as organizações introduzem:

[...] O tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (LGPD).

Tais tratamentos devem ser realizados de tal forma que os agentes que realizarão o tratamento precisam criar medidas de segurança, técnicas e administrativas adequadas para proteger os dados sensíveis de acessos que não foram autorizados pelos titulares. Além disso, deve lidar com “situações accidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

Conforme Garcia et al. (2020), para que uma organização atenda de forma contínua e sustentável aos requisitos do LGPD, é necessário implementar um sistema de gestão que permeia todas as áreas de negócios, incluindo processos, pessoal e tecnologia. Sabendo disto, ressalta-se que, neste trabalho, objetiva-se analisar a solução proposta utilizando a tecnologia *blockchain* em consonância apenas aos **requisitos técnicos** inferidos da LGPD. Dessa forma, princípios e normas administrativas e de negócios não serão analisados no presente trabalho.

Diferentes metodologias já têm sido apresentadas e criadas para a implantação adequada da LGPD nas empresas considerando processos, negócios, tecnologias (GARCIA et al., 2020), como por instruções técnicas que podem servir como uma ferramenta de controle para execução (ROCHA et al., 2019), por exemplo. Para fins de generalização da solução, este trabalho realizará um paralelo entre as questões básicas da *General Data Protection Regulation* (GDPR) e dos itens da LGPD a qual teve sua criação inspirada na GDPR (LORENZON, 2021), lei que está em vigor na Europa. Ambas as leis prezam pelo adequado processamento dos dados pessoais nos mais variados âmbitos e processos da organização. A seguir, na Tabela 5, princípios e direitos selecionados da LGPD e da GDPR, e que podem ser analisadas frente à solução proposta estão sendo apresentados.

Assim como a análise realizada na Seção 6.1.1 em relação aos requisitos de certificação da SBIS, uma análise semelhante será realizada quanto aos itens selecionados da LGPD/GDPR dos quais a solução pode contemplar.

**Quadro 5 – Subconjunto dos potenciais princípios impactados pelas estratégias utilizadas.**

Princípio	Resumo	LGPD	GDPR
<b>Minimização de dados</b>	Os dados devem ser relevantes e necessários para o efeito.	Art. 6º (1) (2) (3)	Art. 5º (1) lit c; Art. 25º
<b>Anonimização</b>	Implementação e utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.	Art. 5º (3) (11); Art. 12º	Art. 5º; Art. 32; Art. 34; Recital 26
<b>Limitação de armazenamento</b>	Os dados devem ser armazenados em uma forma que permita a identificação do titular dos dados não mais do que o tempo necessário.	Art. 15º	Art. 5º (1) lit e;
<b>Integridade e confidencialidade</b>	Os dados devem ser processados de forma a garantir a segurança e proteção adequadas contra o processamento não autorizado.	Art. 6º (IV) (VII); Art. 46º	Art. 5º (1) lit f;
<b>Consentimento</b>	O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular.	Art. 5º (VII); Art. 8º	Art. 4º (11); Art. 6º (1) lit a; Art. 7º
<b>Direito ao esquecimento</b>	O titular dos dados pode obter do controlador a exclusão de dados pessoais, quando, e. g. os dados não são mais necessários, o titular dos dados retira seu consentimento ou os dados pessoais foram coletados ilegalmente.	Art. 5º (XIV)	Art. 17º
<b>Direito de acesso</b>	Fornecer ao titular acesso aos seus dados pessoais, garantindo a portabilidade desses dados a um outro controlador.	Art. 18º	Art. 15º
<b>Direito à informação</b>	Garantir ao titular a visibilidade em torno do que venha a ser realizado com os seus dados pessoais.	Art. 18º	Art. 13º
<b>Portabilidade de dados</b>	O titular dos dados tem o direito de receber seus dados pessoais em um formato estruturado, comumente usado e legível por máquina e de transmitir esses dados a outro controlador.	Art. 18º	Art. 20º

Fonte: Elaborado pelo autor.

#### **6.1.2.1 Minimização de dados pessoais / Anonimização / Limitação de armazenamento**

Têm-se conceitos como a anonimização, baseado no princípio da minimização dos dados, segurança e prevenção, e a ocorrência de incidente de segurança dos dados e a necessidade de informação à autoridade nacional com o objetivo de preservar maiores danos e prejuízos às pessoas físicas proprietárias destas informações (RUARO; GLITZ, 2020). Além disso, o princípio da minimização levanta que as informações pessoais devem ser adequadas, apropriadas e limitadas conforme o fim para as quais serão executadas. O objetivo é reduzir a quantidade de dados, apresentando somente os que são essenciais para um determinado produto ou serviço.

Sabe-se que são variados os tipos de registros e dados manipulados em sistemas médicos. A Seção 5.2 apresenta alguns tipos desses recursos, que são os

utilizados na própria solução (Anamnese, Medicação, Exame, dentre outros). Em cada tipo de recurso há uma série de informações a serem armazenadas, as quais são imprescindíveis para o acompanhamento médico à vida do paciente, devido ao nível de detalhamento necessário. Observa-se, então, uma certa problemática quanto à minimização de dados relacionados à saúde, dada a importância de seu detalhamento.

No entanto, considerando o uso de *blockchain* na solução, a técnica de armazenar apenas o *hash* do arquivo contempla o fato de que deve-se restringir a quantidade de dados a serem apresentados a depender do propósito de uso. Nesse caso, a solução utiliza a Camada de Armazenamento *Off-chain* para o armazenamento das informações completas e autorizadas pelo paciente, enquanto que na Camada de Armazenamento *On-chain* apenas o resumo das informações representadas por meio de um *hash* é guardado em *blockchain*. Além disso, tem-se a identificação do detentor do registro de forma anonimizada em *blockchain*, visto que são armazenados apenas os ponteiros para o banco de dados principal onde estão as informações completas. Portanto, mesmo que informações sejam compartilhadas entre diferentes partes, tem-se o tratamento de anonimidade e minimização das informações de forma a garantir a privacidade do paciente. A solução também abrange o princípio de Limitação de Armazenamento, o qual diz respeito à retenção de informações básicas do paciente.

#### **6.1.2.2 *Integridade e Confidencialidade / Consentimento***

Como mencionado na Tabela 5, estes critérios ressaltam que o processamento deve ser feito de forma a garantir segurança, integridade e confidencialidade adequadas. Este ponto pode ser atendido de forma semelhante como foi descrito em 6.1.1.1 e 6.1.1.2 para o atendimento dos requisitos técnicos da certificação SBIS. Do ponto de vista da lei, a integridade pode ser entendida como o fato de que a informação não deve ser alterada ou excluída sem autorização prévia de alguém autorizado. Sobre a confidencialidade, tem-se a restrição da informação, que não pode ser divulgada para um usuário, entidade ou processo que não foi previamente autorizado (BARCELOS, ).

Quanto à integridade dos dados, a Camada de Armazenamento *On-chain* armazenará permanentemente o *hash* que servirá como uma identidade criptográfica das informações do registro original. Caso haja algum tipo de alteração no registro original, o valor *hash* irá mudar completamente. Dessa forma, será possível verificar

se ocorreu alguma alteração das informações iniciais. Em relação à exclusão das informações, sabe-se que a *blockchain* apenas armazena informações e não possibilita a exclusão das mesmas.

A solução visa alinhar-se a um conceito central das leis GDPR e LGPD, as quais indicam, segundo Hasselgren et al. (2020), que “a propriedade dos dados de saúde deve ser dos pacientes, permitindo que eles tenham maior autonomia sobre seus dados”. Sendo assim, nesta solução, todo controle de acesso se dá por meio das decisões do titular do ativo, o paciente, sobre o uso dos seus próprios dados clínicos. Para tal, as regras de negócios associadas a questões pertinentes à confiabilidade e consentimento estão sendo implementadas na Camada de Armazenamento *On-chain*.

Através da Camada de Aplicação, por meio de uma interface, o paciente irá habilitar ou desabilitar o acesso aos registros específicos para determinados profissionais da saúde. Tal decisão, de que *um Profissional da Saúde X poderá ter acesso à um Registro Y*, será armazenada em *blockchain* através da Camada de Armazenamento *On-chain*, como apresentado em 6.1.1.1. Dessa forma, o Paciente terá uma lista de registros gravados em *blockchain*, e para cada registro, as entidades de saúde habilitadas. Todo controle na *blockchain* é feito por meio de identificadores de cada usuário, os quais são referenciados para o banco de dados na Camada de Armazenamento *Off-chain*. Dessa forma, a identificação dos participantes e ativos serão apresentados de forma confidencial em *blockchain*.

#### **6.1.2.3 Direito ao esquecimento**

O direito ao esquecimento trata-se da escolha que o titular de um dado ou fato pessoal tem para vê-lo “apagado, suprimido ou bloqueado”, especialmente pelo seu decurso no tempo que, de alguma maneira, ferem seus direitos fundamentais (CHEHAB, 2015). Em outras palavras, este direito garante aos titulares dos dados que seus dados serão excluídos ou desativados corretamente quando não forem mais usados ou quando sentirem que é necessário solicitar a exclusão (REIS, ).

Uma das principais características da *blockchain* é a imutabilidade das informações armazenadas, o que faz com que não seja possível realizar alterações e exclusões de dados que já foram armazenadas nos blocos na cadeia, como já expressado na Seção 6.1.1.5. Por sua vez, o princípio abordado nesta seção é uma

das principais questões que geram controvérsia quanto ao uso de *blockchain*, visto que o dado deve ser apagado adequadamente quando o titular solicitar tal direito.

Para mitigar esse conflito, a solução utilizou estratégias semelhantes às aplicadas nos outros princípios. A saber, como já ressaltado, os dados completos de cada registro do paciente que estão armazenados na Camada de Armazenamento *Off-chain* podem ser removidos do BDD, visto que a tecnologia desta camada não apresenta restrição na remoção de dados, os quais podem ser completamente removidos. Na Camada de Armazenamento *On-chain*, serão armazenados apenas os IDs dos participantes e o *hash* das informações brutas o qual é irreversível, visto que foi convertido pelo algoritmo SHA-256. Ao remover os dados brutos da Camada de Armazenamento *Off-chain*, os hashes e identificadores contidos na Camada de Armazenamento *On-chain* não terão mais a capacidade de referenciar qualquer informação contida no BDD. Sendo assim, perde-se totalmente a referência das informações contidas em blockchain com àquelas armazenadas na Camada de Armazenamento *Off-chain*.

#### **6.1.2.4 *Direito de acesso / Direito à informação / Portabilidade dos dados / Identificação dos responsáveis pelo tratamento***

Nos parágrafos segundo, quinto e sétimo do artigo 18 da LGPD assegura que o controlador forneça ao titular acesso aos seus dados pessoais e disponibilize a portabilidade desses dados a um outro controlador. O *direito de acesso* permite que o paciente possa acessar todos os seus dados pessoais que estão sendo coletados e tratados pelo controlador. Quanto ao *direito à informação*, faz com que o titular tenha o direito de receber informações sobre as entidades públicas e privadas com as quais o controlador compartilha dados. No que diz respeito à *portabilidade dos dados*, deve-se facilitar o compartilhamento dos dados pessoais do paciente a outro fornecedor de serviço ou produto, por meio de requisição expressa e examinados os segredos comercial e industrial, de acordo com o regimento do órgão controlador.

Como visto em 6.1.2.2, o Paciente terá controle de acesso sobre todos os seus dados armazenados no sistema. Isto é facilitado pela solução pois quando uma entidade de saúde insere uma informação, o paciente detentor sempre deverá ser associado ao registro. Por sua vez, automaticamente, o sistema apresentará o registro inserido pela entidade de saúde como sendo parte de conjunto de laudos do paciente,

o qual terá acesso direto. Tal informação de que o detentor/titular do registro é o próprio paciente será gravada na Camada de Armazenamento *On-chain*.

Dessa forma, o paciente terá acesso aos seus registros clínicos armazenados em *blockchain*. Além disso, visto que o registro foi associado ao paciente e tal associação foi gravada em *blockchain*, o paciente passa a ter total controle sobre seu registro médico. Por sua vez, o paciente poderá compartilhar seus registros com outras entidades de saúde, autorizando ou desautorizando o acesso aos seus dados. Ao autorizar o acesso de um registro a uma entidade de saúde, as informações poderão ser visualizadas pela entidade instantaneamente. Ao contrário, caso o paciente desautorize o acesso, automaticamente, o profissional de saúde não poderá acessar as informações que outrora lhe foram disponibilizadas. Todas as decisões, por parte do paciente, sobre o compartilhamento ou não de seus registros com outras partes serão armazenadas em *blockchain*, através da Camada de Armazenamento *On-chain*.

Quanto à estrutura das informações para a visualização destas, o sistema delimita os tipos de registro e estruturas baseados em alguns recursos dispostos no padrão FHIR. Portanto, mesmo que as entidades sejam advindas de diferentes organizações, o sistema delimita a estrutura de como os dados serão apresentados entre os diferentes participantes do sistema. Na situação em que a troca de informação seja entre diferentes sistemas, a solução visa também amenizar a dificuldade desta portabilidade ao utilizar recursos do FHIR. Dessa forma, tal compartilhamento de dados pode ser facilitado caso haja a necessidade de troca de informações com outros sistemas que utilizam a modelagem FHIR.

## 6.2 Avaliação de Desempenho

Nesta seção, tem-se uma avaliação com objetivo de verificar o desempenho da solução quanto à estratégia *Off-chain* utilizada a partir da arquitetura em camadas proposta. Como contextualizado na Seção 2.3, necessita-se mitigar problemas relacionados à escalabilidade dos quais ainda são desafios no desenvolvimento de sistemas baseados em *blockchain*, ainda mais no que se refere aos sistemas de saúde. Além disso, os dados sensíveis dos pacientes devem ser armazenados de forma a proteger suas informações. Adicionalmente, tendo em vista as questões sociotécnicas do presente trabalho, observou-se a necessidade de uma análise preliminar de

como sistemas com baixo desempenho podem afetar diretamente a Experiência do Usuário (UX, do inglês *User eXperience*), inclusive no ambiente hospitalar. As seções a seguir discorreram sobre os detalhes do estudo empírico computacional, como as configurações, as coletas de dados por meio da execução dos testes e os resultados da avaliação computacional.

### 6.2.1 Configurações do Experimento Computacional

Para realização dos testes de desempenho fez-se necessária a implementação de uma PoC, especificamente, um dApp comunicando-se com o contrato inteligente implantado em uma *blockchain* local da *Ethereum*, como mencionado no Capítulo 5.3.1.

Os testes foram aplicados sobre duas funções do contrato inteligente, as quais foram escolhidas pois manipulam diretamente o ativo em questão, o Registro. Tais funções são: 1) `inserirRegistro` e 2) `lerRegistro`. Dessa forma, objetivou-se simular, respectivamente, a realização das seguintes operações: o armazenamento de um conjunto de dados referentes a um registro médico do paciente no formato de mídia convertida em *base64* e a busca de um registro específico, também no formato *base64*, referente a um dado paciente. Ressalta-se que a escolha do arquivo em formato *base64* está sendo utilizada para fins de teste nas camadas da arquitetura implementada. Além disso, é um método que vem sendo frequentemente utilizado para codificação de dados para transferência na internet, e pode representar um arquivo de mídia de forma codificada. Com isso, pretende-se simular cenários mais verídicos quanto aos registros armazenados.

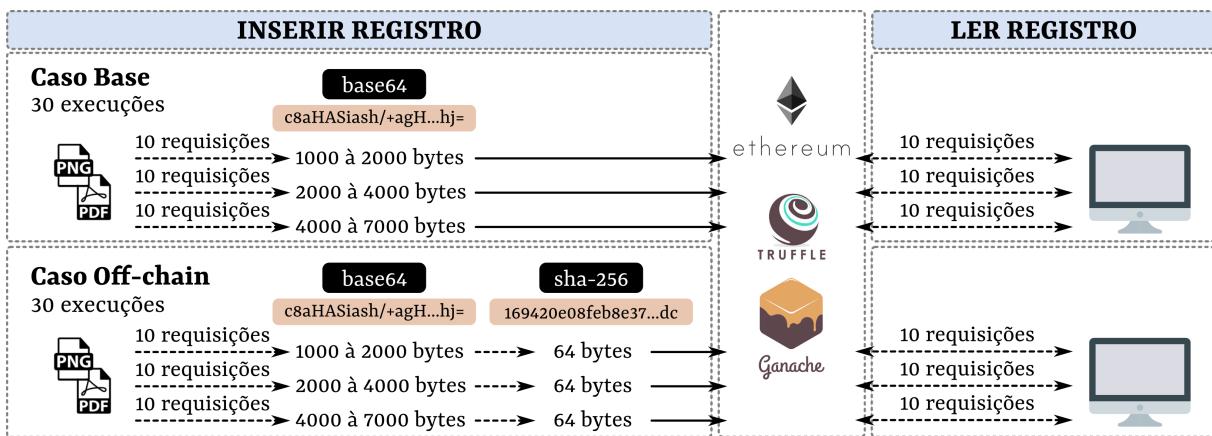
Além das categorias de operações a serem executadas, faz-se necessária a criação de dois tipos de casos, são eles:

1. **Caso Base**, pelo qual o registro no formato *base64* é inserido totalmente na *blockchain*, ou seja, simula todo arquivo de mídia sendo armazenado em *blockchain*;
2. **Caso Off-chain**, solução que representa a arquitetura proposta, através da qual apenas os *ids* do registro e dos participantes são armazenados em *blockchain*, além do *hash* do arquivo, sendo que o arquivo original é armazenado no BDD.

Por sua vez, a fim de analisar diferentes tamanhos de arquivos sendo armazenados no artefato em cada caso, simulam-se registros com os respectivos tamanhos: (i) arquivos de 1000 *bytes* à 2000 *bytes*; (ii) arquivos de 2000 *bytes* à 4000 *bytes*;

e (iii) arquivos de 4000 *bytes* à 7000 *bytes*. Apesar de tais tamanhos representarem arquivos razoavelmente pequenos, pode-se realizar, de forma representativa, a comparação entre os dois casos. Para cada tamanho de arquivo, os testes foram executados 30 vezes para lidar com possíveis *outliers* das métricas coletadas. Além disso, em cada execução 10 requisições foram simuladas nas operações. A configuração de experimento completa está sendo ilustrada na Figura 32.

**Figura 32 – Configurações do Experimento.**



Fonte: Elaborado pelo autor.

O Quadro 6 elenca as métricas utilizadas e suas respectivas descrições a respeito dos procedimentos de coleta. Essas métricas foram extraídas a partir de *scripts* que coletavam informações advindas das informações de cada transação realizada em *blockchain*, e foram armazenadas em arquivos do tipo *Comma-Separated Values* (CSVs). Os testes realizados foram executados em uma máquina de 16GB de memória RAM e SSD de 256 GB, com um processador *Intel Core i7* (8a geração) e com uma conexão de internet banda larga de 20 Mbps.

**Quadro 6 – Procedimentos de Coletas das Métricas**

Métrica	Processo de Coleta
<b>Tempo de Publicação</b>	O tempo de publicação foi calculado pela diferença no tempo entre a requisição de inserção dos dados e quando a transação minerada em um bloco.
<b>Tempo de Busca</b>	Refere-se ao tempo entre a requisição de busca sobre um registro na <i>blockchain</i> por meio de seu respectivo id e o retorno das informações. De maneira semelhante, o cálculo é realizado no BDD.

Fonte: Elaborado pelo autor.

Para cada métrica e os respectivos tamanhos de arquivos foram aplicados testes estatísticos de Wilcoxon (WC), que identifica a ocorrência de diferença estatística

entre as amostras considerando um nível de confiança de 95% utilizando-se da correção de Bonferroni; e Vargha-Delaney ( $\hat{A}_{12}$ ), o qual retorna o número relativo de vezes que um tipo de caso (*off-chain* e *base*) produziu valores superiores ao outro.

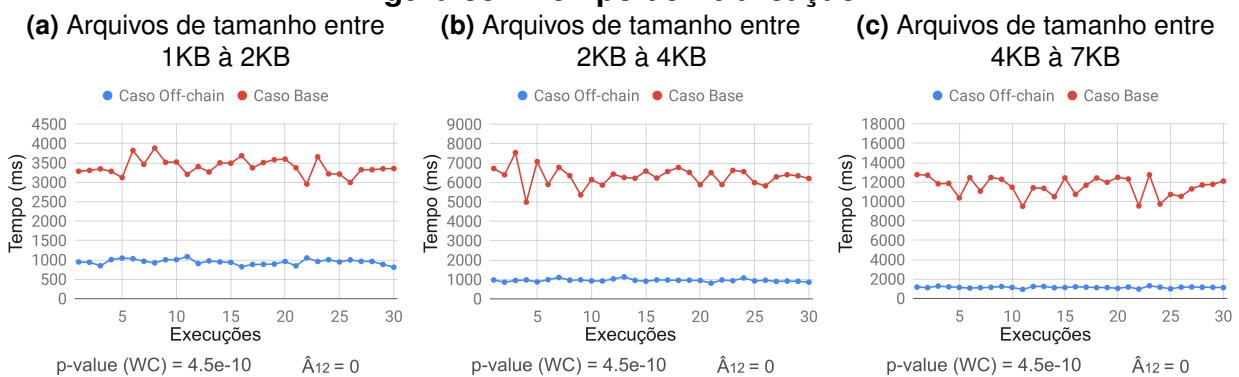
### 6.2.2 Resultados e Análises

Nesta seção, serão apresentados os resultados dos testes de desempenho a partir das métricas coletadas para os diferentes tamanhos de arquivo, e suas respectivas análises em relação ao Caso *Base* e o Caso *Off-chain*.

#### 6.2.2.1 *Tempo de Publicação*

Constata-se um intervalo de tempo decorrido entre a requisição da operação de armazenamento e a publicação desta transação em um bloco, ou seja, quando este é minerado. Na Figura 33a, referente à arquivos de tamanho entre 1KB e 2KB, os tempos vão até aproximadamente 3882 ms, tendo como média das execuções 3397 ms para a publicação de cada transação no Caso *Base*. Enquanto para o Caso *Off-chain* os tempos tem o máximo de até 1082 ms, e a média das execuções 947 ms.

**Figura 33 – Tempo de Publicação.**



Já Figura 33b, referente à arquivos de tamanho entre 2KB e 4KB, o tempo máximo atingiu 7540 ms e teve como média das execuções 6307 ms para o Caso *Base*. Por sua vez, no Caso *Off-chain*, o tempo máximo obtido foi 1133 ms e a média das execuções foi de 952 ms. Por fim, na Figura 33c, referente à arquivos de tamanho entre 4KB e 7KB, o tempo máximo atingiu 12770 ms, tendo como média das execuções 11543 ms para a publicação de cada transação no Caso *Base*. Já para o Caso *Off-chain*, o tempo máximo obtido foi de 1306 ms e a média das execuções 1141 ms.

Observa-se que em todos os tamanhos de arquivo, o Caso *Off-chain* apresenta médias aproximadas, entre 947 ms e 1306 ms, o que era esperado visto que a proposta, em todas as situações, codifica o arquivo para 64 *bytes*. Por sua vez, o tempo de inserção para o Caso Base sempre tende a aumentar à medida que o tamanho do arquivo aumenta. Para todas as situações, existem evidências estatísticas que mostram que o tempo de publicação do Caso Base é显著mente maior que o do Caso *Off-chain* em 100% das execuções para todos os tamanhos de arquivos, visto que o *p-value* mostra-se inferior à 0,5 e o  $\hat{\Delta}_{12}$  equivale à 0. Em outras palavras, o tempo de publicação/mineração do Caso *Off-chain* foi mais rápido que o Caso Base.

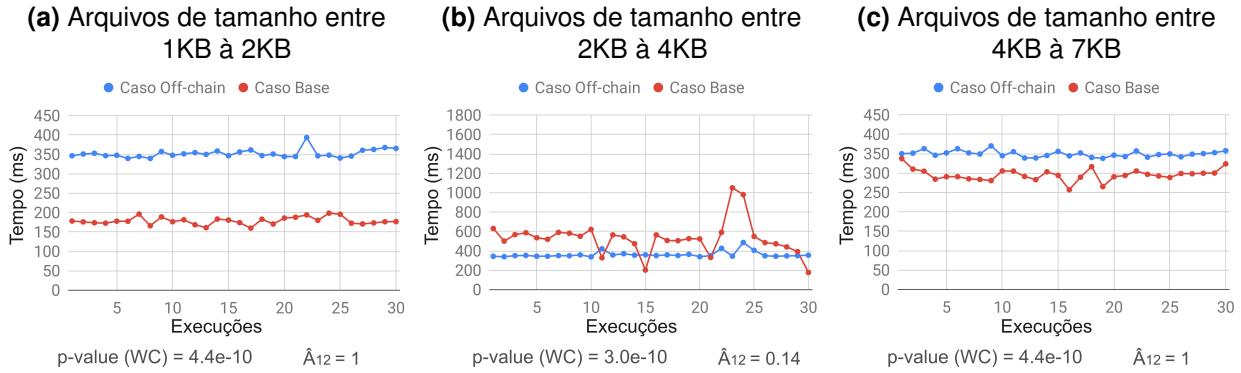
Em todos os tamanhos do arquivo, o tempo de inserção das informações no Caso *Off-chain* tem sido aproximadamente de 3x a 10x mais rápido que o Caso Base. Para este último caso, ressalta-se que o baixo desempenho pode prejudicar a eficiência do funcionário (profissional de saúde), e reduzir a experiência do cliente e a eficiência do processo, impactando diretamente no domínio em questão (CONSULTING, 2014). Tais processos devem ser realizados com eficácia visto que podem impactar diretamente na vida do paciente. Como será visto no Capítulo 7, os profissionais de saúde registram tudo que realizam com o paciente. Sendo assim, faz-se necessário que o sistema execute os procedimentos em um contexto hospitalar para atender a demanda dos profissionais ao passo que estes e o paciente usufruam das características de segurança da tecnologia *blockchain*. Pode-se constatar que estratégias como as utilizadas no presente trabalho possibilitam estes requisitos serem executados de maneira mais eficiente para o usuário do sistema.

#### **6.2.2.2 Tempo de Busca**

Através da Figura 34a pode-se perceber que o tempo de busca tem um máximo de 199 ms e uma média de 179 ms no Caso Base, e um máximo de 394 ms e uma média de 352 ms no Caso *Off-chain*. Observa-se também que o tempo de busca de um dado ficou em até 1050 ms, com uma média de 530 ms no Caso Base de arquivos com tamanhos entre 2KB e 4KB, como demonstrado na Figura 34c. Por sua vez, no Caso *Off-chain*, obteve-se um máximo de tempo de busca igual à 486 ms, com a média equivalente a 362 ms. Finalmente, observando a Figura 34b, tem-se um tempo máximo de busca de 337 ms, com uma média de 296 ms no Caso Base. Por

sua vez, no Caso *Off-chain*, obteve-se um máximo de tempo de busca igual a 370 ms, com a média igual a 349 ms.

**Figura 34 – Tempo de Busca.**



Nas situações da Figura 34a e 34c, o Caso *Off-chain* demonstra-se com o maior tempo de busca em relação ao Caso Base. A partir disso, supõe-se que o tempo de resposta é menor no Caso Base porque os dados estão sendo buscados diretamente na *blockchain*. Enquanto que, para os dados do Caso *Off-chain*, estes estão sendo pesquisados no BDD externo, demandando um maior tempo. Nessas duas situações os casos são significativamente diferentes, com o Caso *Off-chain* tendo maiores valores de tempo de busca em 100% das execuções em relação ao Caso Base. Por outro lado, a Figura 34c apresenta um comportamento diferente dos demais, pois o Caso *Off-chain* obteve um tempo maior em 14% das execuções em relação ao Caso Base. Além disso, o Caso Base apresenta uma maior variação nos valores de tempo de resposta.

Constatou-se que o desempenho de leitura ainda pode ser melhorado para que a experiência dos pacientes e dos profissionais da saúde não seja prejudicada em algum momento em suas solicitações. Apesar disso, o tempo de busca por informações do registro ainda está dentro do aceitável, visto que está variando de 349 ms à 352 ms para os tamanhos de arquivos apresentados. Pesquisas mostram que os tempos de latências necessárias para renderização de uma página, por exemplo, devem ser menores que dois segundos e, caso os usuários atinjam três segundos de espera, 40% deles podem “abandonar” a aplicação (GOMEZ, 2011).

### 6.3 Conclusões do Capítulo

Como apresentado, foi possível analisar a solução quanto aos requisitos técnicos estabelecidos pela SBIS e normas de proteção de dados sensíveis baseadas na LGPD. Nesses casos, se conseguiu listar um subconjunto de requisitos que poderiam ser atingidos ao atrelar blockchains aos PEPs em seu desenvolvimento e implantação. Tais requisitos se referem desde aspectos da garantia de segurança, estruturação do conteúdo a ser armazenado, bem como as funcionalidades. Dessa forma, considerou-se que as potencialidades podem ser exploradas conforme as camadas da solução apresentada. Adicionalmente, observou-se que o desafio de escalabilidade pode ser mitigado com o uso de estratégias *Off-chain* através da Camada de Armazenamento *Off-chain*. Além disso, princípios básicos da LGPD pareados ao da GDPR podem ser atendidos ao utilizar estratégias também em relação às camadas mencionadas.

Ademais, realizou-se um experimento preliminar de desempenho a fim de demonstrar e avaliar o uso de estratégias *off-chains*, considerando o desafio apresentado na Seção 6.1.1. Tal análise também se faz relevante para uma breve discussão sobre a experiência do usuário quanto ao desempenho da solução ao registrar e recuperar uma informação, visto que é um requisito de qualidade de suma importância para os sistemas de informação em saúde.

## 7 AVALIAÇÃO SOCIAL

Neste capítulo serão apresentadas as discussões e os *insights* encontrados a partir dos temas e subtemas identificados através dos GFs, como pode ser visto no Quadro 7. Tal análise e a respectiva classificação de temas e subtemas identificou 5 temas e 20 subtemas. Observou-se que o GF 1 discutiu 90% de todos os subtemas encontrados, enquanto que o GF 2, 75%. O GF 2 discutiu 83,3% dos subtemas que o GF 1 abordou. Assim, foi possível identificar as problemáticas em relação ao uso dos prontuários atuais, assim como a percepção dos participantes quanto aos aspectos colaborativos e os benefícios ao utilizar-se PEPs atrelados à novas tecnologias como a *blockchain*. As próximas seções apresentam o compilado das opiniões dos participantes e os achados identificados para análise da solução proposta.

**Quadro 7 – Ocorrência de Subtemas nos Grupos Focais.**

Tema	Subtema	Ocorrência nos Grupos Focais	
		1	2
Uso atual do PEP	Falta de integralidade e interoperabilidade das informações entre diferentes unidades	✓	✓
	Registro de todas as informações possíveis sobre o paciente é muito relevante e comum entre os profissionais de saúde	✓	✓
	Controle de acesso às informações do paciente entre os profissionais e entidades de saúde	✓	✓
	Fluxo e hierarquia de atividades nos registros dos pacientes entre os profissionais de saúde		✓
	Armazenamento e gerenciamento atual de registros por parte do paciente	✓	✓
Modelo 4C	Compartilhamento e visualização de informações do paciente por parte dos profissionais	✓	✓
	Disponibilidade e prevenção de perda das informações sobre o segmento do paciente	✓	
	Conscientização dos profissionais de saúde / Interprofissionalidade	✓	✓
PEP & Blockchain	Imutabilidade, rastreabilidade e auditoria das informações aumenta segurança de todas as partes	✓	✓
	Alterações de informações dentro do prontuário		✓
	Acesso e facilidade na disponibilidade das informações	✓	✓
	Controle de acesso e segurança da informação do paciente	✓	
Melhoria da Qualidade	Qualidade de processos e do trabalho	✓	✓
Lições Aprendidas e Oportunidades	Controle de acesso e LGPD	✓	✓
	Liberdade de acesso por profissionais de saúde para agirem em situações de emergência	✓	
	Dificuldade de lidar com a tecnologia	✓	✓
	Dificuldade de implantação	✓	
	Integração com sistemas automatizados	✓	✓
	Registro dos acessos a uma prescrição específica	✓	
	Nível de assistência médica	✓	✓

Fonte: Elaborado pelo autor.

### 7.1 O uso atual de PEPs pelos profissionais de saúde

Cada GF teve um primeiro momento de discussão relacionada ao uso atual dos PEPs. Dessa forma, identificou-se algumas experiências abordadas pelos parti-

pantes do experimento. Um dos principais pontos relatados foi a **falta de integralidade e interoperabilidade das informações entre diferentes unidades**. Em relação à integralidade das informações, o participante PS1 relata que “*nunca tem essa integralidade registrada, porque eu não sei o que o outro profissional faz [...] Eu não via evolução de pacientes nem de outros postos da região, nem de especialistas*” (PS1). Percebeu-se que a dificuldade em se ter informações suficientes do paciente de forma integral prejudica diretamente no entendimento de sua evolução. Ressalta-se que tal dificuldade tem sido observada principalmente em instituições públicas visto que, em redes privadas, o acesso a algumas informações pode ser facilitada, como diz o PS2: “*pelo menos os que eu conheço a gente tem acesso, por exemplo, a outras consultas que o paciente foi, aí a gente vê o que é que colega escreveu, quais foram as condutas*” (PS2).

Todavia, a principal problemática ocorre quando as unidades de saúde estão em locais diferentes, gerando uma dificuldade quanto à interoperabilidade das informações. Nem todas as instituições, por exemplo, possuem sistemas eletrônicos para PEPs, tornando o esforço para unir informações entre diferentes unidades ainda considerável, além de prejudicar a comunicação entre os profissionais de saúde, como apresentado pelo PS1, que diz “*a gente tem essa dificuldade de está encaminhando os dados para outra unidade, justamente por isso, porque não tem o sistema online, integrado, e dificulta muito a comunicação*” (PS1), e endossado pelo IS1:

Por exemplo, se eu tenho um paciente na atenção básica, ele é inserido na minha unidade, mas ele estando acompanhado por um CAPES, são os serviços do mesmo município, no mesmo contexto, mas nós não temos. Nós não temos informações do prontuário daquele paciente que vem da unidade, o que a gente sabe muitas vezes é alguma receita que o paciente traz, informações dadas pelo próprio paciente, no caso (IS1).

Tal situação reflete em outra temática importante que é o fato de que o **registro de todas as informações possíveis sobre o paciente é muito relevante e comum entre os profissionais de saúde**. A maioria dos profissionais são treinados a escreverem todos os procedimentos realizados com o paciente, fazendo com que a comunicação entre os profissionais “[...] se dá muito por escrito em termos de

*parecer*” (PS2). Não apenas considerando o ato de registrar informações do paciente para os devidos manejos com sua saúde, mas também como respaldo do trabalho e dos serviços prestados pelo próprio profissional, como informa o IS1: “*a forma da gente comprovar o nosso serviço que a gente ta fazendo com o paciente, é a partir da anotação do registro*” (IS1). Portanto, percebe-se que, mesmo com tantas informações sendo registradas, deve-se ter meios eficazes de integrá-las entre os profissionais e entre instituições diferentes a fim de mitigar problemáticas relacionadas à interoperabilidade.

Por outro lado, quando os dados estão disponíveis em cada instituição e podem ser acessados, deve-se considerar a questão de privacidade e o **controle de acesso às informações do paciente entre os profissionais e entidades de saúde**. Faz-se necessário o entendimento da seguinte questão: até que ponto o paciente tem o controle de seus dados armazenados por um hospital ou um laboratório? O PS1 informa que “*não tem nenhuma privacidade pra quem trabalha no hospital*” (PS1), além disso os profissionais “*tem acesso aos dados, por exemplo, do que outros médicos escrevem no prontuário, tanto físico né, quando é impresso, como nos sistemas*” (PS2). Já em alguns países, como relatado pelo PS2, apenas o médico pode ter acesso aos prontuários e que, considera-se até um “absurdo”, por exemplo, o acesso por parte de estudantes de medicina que iniciam suas práticas no hospital.

Vale refletir que, apesar da extrema necessidade do compartilhamento de informações entre os profissionais, é necessário o devido manuseio e controle do acesso das informações do titular, visto que são informações consideradas sensíveis pela LGPD. Por sua vez, através das visões do LM1 e LM2, o acesso às informações se torna mais burocrática e menos comum, até porque, como ressalta o LM2: “*é pouco comum que a gente também saia do próprio laboratório e vá atrás do prontuário do paciente para poder entender a causa*” (LM2). Geralmente o laboratório “*solicita uma assessoria médica*” (LM1), entrando em contato com o médico responsável pelo paciente para solicitação de dados necessários.

Ressalta-se que os PEPs atuais devem lidar também com o **fluxo e hierarquia de atividades nos registros dos pacientes entre os profissionais de saúde** em curto e a longo prazo. Dependendo dos processos, existe uma certa “coordenação” de algumas atividades entre os diferentes tipos de profissionais da saúde. O IS2 apresenta tal situação da seguinte maneira:

Contexto de que o médico prescreve informação de médico para médico nas prescrições e evoluções médicas, e também de médico para enfermeiro, a gente checa as evoluções e depois de prescrito a gente apraza e vai atuando de acordo com a prescrição no decorrer do dia e pode haver mudanças em que o médico ali faz a mudança e comunica ao enfermeiro para que apraza. O técnico, em seguida, executa alguma medicação que deve ser administrada (IS2).

Outra discussão fundamental nos GFs foi sobre o **armazenamento e gerenciamento atual de registros por parte do paciente**. Apesar do uso difundido de PEPs, o prontuário em papel ainda se faz presente em muitas instituições de saúde. O Paciente1 e o Paciente2 relatam que suas experiências na maior parte ainda é com prontuários em papel, como diz o Paciente1: “[...] até hoje eu ainda tenho guardado o envelope, porque pra onde eu for, em questão de saúde, eu fico levando” (Paciente1). Apesar disso, observou-se que ainda não há uma gerência completa de seus registros, visto que o Paciente2 informa: “não faço uma gestão muito elaborada, assim tenho o documento do cartão de vacinação quando é pra vacinas, mas pra exames, internação, essas coisas... Por exemplo, exames eu guardo por um tempo, depois eu descarto” (Paciente2). Assim, pode-se constatar algumas situações: (i) muitas das informações do paciente podem ser perdidas, deixando uma certa “lacuna” no registro de seu histórico médico; (ii) ainda são poucos os sistemas que permitem o próprio paciente gerenciar suas informações e o controle de acesso com quem eles as compartilharão; (iii) conscientização por parte do próprio paciente a respeito sobre o devido controle de seus dados sensíveis ainda é algo pouco considerado.

## 7.2 Modelo 4C de Colaboração

O Modelo 4C é um modelo fundamentado em quatro pilares referentes ao trabalho colaborativo: comunicação, coordenação, colaboração e cooperação. Este tem sido um modelo utilizado para desenvolvimento e análise do uso de sistemas colaborativos. Compreende-se desde a troca de mensagens até gestão e coordenação de tarefas desenvolvidas em conjunto por meio de um espaço partilhado (COSTA et al., 2014). Dessa forma, após apresentação e uso da solução através da observação participante, como mostrado na Etapa 4 (Seção 4.2.2), busca-se entender os aspectos

colaborativos em tais pilares, assim como outras perspectivas sociais identificadas.

Tendo em vista a discussão sobre o **compartilhamento e visualização de informações do paciente por parte dos profissionais**, ao indagar os participantes a respeito de como a solução poderia estar contribuindo quanto à comunicação entre os profissionais a partir do compartilhamento de informações do paciente, os participantes ressaltaram os pontos positivos identificados. O PS1 informou que, caso o uso de tal solução seja “difundido” entre os profissionais, “*iria ficar muito mais fácil mesmo, e a gente não iria perder a informação do paciente*” (PS1). Segundo Costa et al. (2014), a única forma de se obter indícios do sucesso da comunicação é através do discurso e das ações (e reações) do receptor.

Assim, percebe-se que a perda de informações do paciente é um dos principais problemas que causam dificuldade na comunicação entre os profissionais, visto que os dados que não chegam ao receptor de forma adequada, de forma a prejudicar a continuidade do cuidado a um paciente. Conforme Mourão e Neves (2007), o acesso e o compartilhamento de informações agiliza o atendimento e possibilita a troca de informações entre médicos e entre médicos e pacientes. Através da presente proposta, essa comunicação é facilitada pelo uso da tecnologia *blockchain* pois além de dificultar a perda de informações devido suas características de persistência de dados, possibilita a troca de informações entre diferentes partes de forma segura.

O PS2 enfatiza que esta solução: “[...] ajuda a equipe demais se essa interação vier com o diálogo correto e, dessa forma que a gente tá pondo, isso é excepcional na realidade” (PS2). O PS2 destacou também o fato de como os registros no PEP podem estar estruturados. O presente trabalho se baseia no padrão FHIR para implementação na solução (como pode ser visto na Seção 5.2), tal integração pode contribuir para a organização de informações do médico, por exemplo, ao preencher um registro do tipo ‘Anamnese’. Ao utilizar registros semiestruturados, além de permitir melhorar a interoperabilidade entre sistemas diferentes que contenham estruturas semelhantes de seus registros, situações recorrentes também podem ser mitigadas, como: “*com relação à letra do médico, obviamente. Muitas vezes a gente não entende o que os outros escrevem*” e “*às vezes em um plantão, o profissional está cansado, com certeza ele pode não perguntar tudo*” (PS2).

Em relação à passagem de plantão, contexto também discutido pelo IS1, já tem sido bastante presente na literatura (GONÇALVES et al., 2016; NASCIMENTO et

al., 2018; SCHORR et al., 2020), dada a sua importância, visto que nesse momento se deve “*traçar o plano de cuidados aos pacientes, sendo esta a primeira comunicação da equipe e um dos momentos mais importantes do dia no serviço*” (SCHORR et al., 2020). Além disso, uma organização adequada no compartilhamento das informações do paciente entre a equipe médica, pode facilitar na investigação de diagnósticos. Tal ferramenta pode contribuir para que um profissional, por exemplo, saiba o parecer de outro profissional (PS1). Do ponto de vista do LM1, por sua vez, este informa que a solução pode melhorar no acesso às informações do paciente entre diferentes laboratórios, quando necessário, apesar das diferentes metodologias, pode direcionar o analista “na hora que ele vai laudar o exame” (LM1).

Observou-se que a solução em questão também pode promover a **disponibilidade das informações do paciente e prevenção de perda das informações sobre o segmento do paciente**, conforme ressaltado pelo PS1: “[...] *informações que às vezes o paciente não lembra, às vezes, perdeu um exame ou não leva*” (PS1), o que impacta também na diminuição da perda de informações. Visto que as informações estarão disponibilizadas em diferentes réplicas através da *blockchain*, tal mecanismo facilita o acesso às informações entre o paciente e o médico, pois pode ser possível recuperar as informações a partir de outras cópias.

Por outro lado, tal discussão leva-se a um tema além do uso da tecnologia, que é a **conscientização dos profissionais de saúde e a interprofissionalidade**. Tal constatação se dá pela fala dos participantes: “*caso tenha esse uso sim difundido, e os médicos tenham a consciência, falo pela minha área, de colocar os dados direitinho nesse sistema*” (PS1) e “[...] *ajuda muito nessa questão da comunicação. Porque, infelizmente, os profissionais de saúde não conseguem ainda atuar nessa questão da interprofissionalidade, que é algo urgente, desde sempre, acredito*” (IS1). A interprofissionalidade pode ser entendida como uma relação interdependente dentro de um ambiente de trabalho, a qual exige colaboração entre os agentes que compõem esse serviço, em busca de um objetivo em comum (ARAUJO, ). Assim, percebe-se que interprofissionalidade depende da colaboração e cooperação entre os profissionais que manuseiam as informações do paciente, de forma que possam desenvolver o trabalho em conjunto. A colaboração peer-to-peer (P2P) usando a tecnologia *blockchain* pode levar a uma nova era do ecossistema de saúde inteligente (ONIK et al., 2019), podendo auxiliar a equipe multiprofissional e/ou a multi-institucional nas melhores tomadas de

decisão para a garantia do cuidado ao paciente.

Quanto à coordenação, de acordo com (COSTA et al., 2014), é um pilar que “organiza a equipa, negociando/atribuindo tarefas para serem realizadas por determinada ordem, de forma a cumprir os objetivos propostos”. Sendo assim, foi possível perceber que, dependendo do fluxo, podem existir configurações das quais representam determinadas ordens e hierarquias, como visto na Seção 7.1. O IS1 informou que um médico pode prescrever informações para um enfermeiro, por exemplo, este, por sua vez, deve realizar procedimentos conforme o que foi prescrito. O pilar coordenação pode apresentar também interdependência de atividades, o que significa que a equipa são mutuamente interdependentes.

A solução utilizada permitiu que cada perfil realizasse suas atividades específicas, de forma que o registro de cada participante influenciava nas ações do outro, como pode ser visto nos Apêndices C ao F. No cenário utilizado, o PS tinha acesso ao que o IS e o LM haviam registrado, por exemplo, e por meio dessa ordem, o PS realizou sua atividade final que seria dependente das informações contidas nos registros anteriores. Dessa forma, por meio da *blockchain*, é possível ter até mesmo o rastreamento sobre a ordem das ações de todos os procedimentos que estão sendo realizados com o paciente.

Segundo Dhagarra et al. (2019), a falta de avaliação sobre o nível de engajamento entre as partes interessadas nas estruturas atuais e a falta de cooperação, colaboração, comunicação e coordenação é um dos principais obstáculos na adoção de blockchain em saúde. A presente solução contribui na investigação de como a *blockchain* pode estar contemplando tais pilares do modelo 4C ao integrar-se aos PEPs.

### 7.3 PEP baseado em Blockchain

A presente seção discutirá sobre as características técnicas que a *blockchain* possibilita ao ser integrada aos PEPs. Por meio da discussão, percebeu-se que a **imutabilidade, a rastreabilidade e a auditoria das informações aumentam a segurança de todas as partes**, desde o paciente até o profissional de saúde e suas respectivas instituições de trabalho. Através da imutabilidade é possível gerar rastreabilidade das ações nos registros do paciente, consequentemente, favorece na eficiência de auditorias dos dados armazenados. O IS1 percebeu que a imutabilidade

da *blockchain* “garante a segurança do paciente e a atuação do profissional. O respaldo do profissional [...] Porque o registro é informação, é o respaldo do seu trabalho” (IS1), e o PS1 endossa: “eu acho bom por questão mesmo do paciente e da gente pra estar judicialmente protegido né?” (PS1). Ambos relatam que, mesmo que os métodos sejam realizados com o paciente, os próprios profissionais também se protegem com tal recurso.

O PS2 apresenta que, de fato, erros dos dois lados podem ocorrer: “[...] às vezes, dá problema, o paciente pode dizer que informou uma coisa e não tá registrado, ou o contrário, o médico dizer que registrou e não tá lá escrito” (PS2). Assim, percebe-se que, como as informações estariam de maneira imutável, atualmente, seria difícil alguém discordar dos registros e procedimentos realizados com o paciente que foram adicionados na *blockchain*. Como já mencionado, tal benefício ocorre devido a estrutura de cadeia em blocos interligados criptograficamente e organizados em forma cronológica (ver Seção 2.1). Este ponto se faz relevante, visto que há fatos nos quais realmente existem condutas irregulares, dessa forma pode-se utilizar a tecnologia para recorrer judicialmente, por exemplo, como mencionado acima pelo PS1. A literatura endossa tal afirmação por apresentar trabalhos que utilizam as chamadas “evidências digitais” (XIONG; DU, 2019; PETRONI; FRANCO, 2018) que, agora podem ser registradas em *blockchain* e recuperadas para serem utilizadas diretamente em órgãos judiciais (LIU et al., 2019).

Outro fato relevante em relação às auditorias é que, segundo o IS2, os hospitais, geralmente privados, periodicamente realizam auditorias das informações procurando “prontuário que tenha uma prescrição errada” ou “fora do contexto” (IS2). Quando tais erros são identificados, ocorrem as retificações para uma versão da qual deveria ser a correta. Em relação às auditorias atuais, são aplicadas multas dependendo do caso (IS2). O uso de *blockchain* garantiria uma maior segurança e complementariedade aos tipos auditorias existentes. Ressalta-se que tanto a LGPD como a SBIS, avaliadas pelo presente trabalho nas Seções 6.1.1 e 6.1.2, estabelecem requisitos relacionados a possibilidade de se realizar auditorias pelos órgãos estabelecidos. Por sua vez, através da imutabilidade, o LM1 afirma que os laboratórios terão mais cautela ao registrar seus resultados, como será discutido na Seção 7.4.

Um ponto considerado pelos profissionais na discussão foi que, mesmo que haja a imutabilidade, deveria ser possível realizar **alterações de informações**

**dentro do prontuário.** Tanto após a auditoria, caso exista algum erro reportado que necessite de correção, como durante o fluxo de atendimento ao paciente. O IS2, por exemplo, informa que o “*profissional tem acesso a mudar uma determinada questão dentro do prontuário, o médico faz a prescrição, uma enfermeira apraza*” (IS2). Apesar de que o escopo de implementação da PoC no presente trabalho não possibilita a modificação em um mesmo documento, constata-se que é totalmente possível executar tal ação, sendo que cada modificação gera novas versões de um mesmo documento. Assim, tem-se toda a trilha de alterações realizadas sobre um documento. O IS2 ainda ressaltou que “*toda mudança que for executada, ela tem que tá vinculada à senha de acesso às credenciais daquele profissional né, porque aí ele entrou com sua senha de acesso, ele mudou e ele ta responsável eticamente pela modificação*” (IS2). A solução pode contemplar esta funcionalidade, pois como apresentado em 5.3.1 e avaliado em 6.1.1, o identificador de cada profissional que insere informações na *blockchain* é vinculado aos identificadores dos registos e do paciente em questão, além disso, cada registro é adicionado na ordem cronológica. Dessa forma, tal associação é registrada e não pode ser alterada.

Discutiu-se também sobre o **acesso e facilidade na disponibilidade das informações**, tendo em vista a característica de distribuição e replicação das informações entre diferentes nós de uma rede *blockchain*. O Paciente1 ressalta que a solução pode auxiliar no acesso às informações, pois “*independente do que acontecer, aquilo vai tá disponível nos outros membros da rede. Aí, é mesmo que não esteja acessando lá naquela hora, ta registrado*” (Paciente1). Segundo o IS1, pode ser que a solução seja interessante para os pacientes que tenham interesse e curiosidade de está sempre com as suas informações, por exemplo. De fato, existem pessoas com doenças crônicas que necessitam de auxílio médico no decorrer de sua vida, possivelmente estas que já têm experiência em gerenciar seus exames de alguma forma, poderiam ser beneficiadas com a solução, inclusive para ter o registro de sua evolução.

O PS2 percebeu que a característica de disponibilidade é importante para não perder informações do paciente, e considera como “um mecanismo pra aumentar a segurança” (PS2) justamente pela importância das informações do paciente registradas. Um ponto levantado pelo IS2 é que, atualmente, existem muitas perdas, principalmente quando os prontuários são em papel, visto que tem vida útil. O mesmo ressalta que “é importante esse registro digital [...] por exemplo, depois de 10 anos, o SUS não

*tem mais que ter aquele registro no papel, o papel pode ser eliminado, pode ir pra um arquivo, então isso vai mudar né, quando eu tenho esse registro*” (IS2). Vale ressaltar que ao utilizar PEPs com bancos de dados tradicionais, a informação ainda pode ser perdida ou apagada. A solução de PEP com *blockchain* permite que a informação fique permanentemente registrada na rede.

Como já explanado, a disponibilidade das informações na *blockchain* ocorre pois, mesmo que um nó sofra uma falha, é possível recuperar as informações das outras réplicas. Dessa forma não se tem um único ponto de falha, como ocorre em sistemas tradicionais nos quais, geralmente, a informação é armazenada apenas em um servidor central. O IS1 afirma já ter passado por situações em que perdeu informações registradas no sistema em um período do dia e que precisou realizar as anotações manuscritas e, mesmo assim, quando o sistema funcionava novamente, tudo que foi anotado deveria ser registrado no sistema. A ênfase do LM2 se alinha ao mesmo pensamento já explanado em relação à disponibilidade de informações, perda de dados e possíveis retrabalhos: “*creio que isso é sim uma possibilidade muito boa, de você ter seus dados em diversos locais e não ter a dependência, e não ter o registro somente a um único, e você ter que refazer tudo de novo*” (LM2).

Por fim, enfatizando, mais uma vez, o uso de *blockchain* relacionado à questão de segurança, um último subtema identificado em relação é sobre o **controle de acesso e segurança da informação do paciente**. O Paciente1 informa que a possibilidade de liberar e negar acesso é uma etapa importante que pode influenciar na segurança de dados do paciente. Por outro lado, identificaram-se desafios dependendo do contexto em que estiver o paciente, como será discutido na Seção 7.5.

#### 7.4 Melhoria na Qualidade

Como mencionado na Seção 7.3, a imutabilidade é uma das principais vantagens da *blockchain* pois proporciona a rastreabilidade e auditoria das informações. Tal característica pode influenciar diretamente não somente na qualidade e integridade dos dados, e na diminuição de procedimentos manuais sujeitos a erros (LARRY et al., 2021), como também na **qualidade de processos e do trabalho**. Conforme Zhang et al. (2019), uma implementação de *blockchain* na área da saúde pode ter grandes impactos em outras áreas, como gerenciamento de atendimento ao cliente, processos

internos para garantia de qualidade, verificações de segurança ou parcerias externas.

O LM1 ressalta que os laboratórios médicos serão mais cuidadosos nos processos e que tais características permitem ao paciente realizar as devidas verificações dos seus próprios procedimentos: “*os laboratórios vão ter um pouco mais de cautela, fazerem, liberarem esses resultados, que deveria ser o normal. O normal é que já tenha cautela. Mas, é, isso deixa escrita eternamente e facilitando o acesso ao paciente a esse erro*” (LM1). Este participante relata ter presenciado casos em que um laboratório registrou conclusões a respeito da saúde do paciente erroneamente, e que a presente solução “forçaria” o laboratório ter mais atenção quanto aos processos. Já o IS1 enfatiza que todos os registros que os profissionais de saúde realizam em prontuários servem como comprovação de seus serviços e trabalho.

Tais relatos coincidem com o que foi apresentado por Zhang et al. (2019), os quais dizem que o *blockchain* na saúde pode melhorar a qualidade das informações, visto que as partes interessadas podem acessar dados completos. Além disso, devido à possibilidade de auditabilidade dos dados, pode-se favorecer a qualidade de serviço quanto à confiabilidade, de forma a impactar a satisfação do paciente. Do ponto de vista das instituições, os sistemas imutáveis com data e hora, por exemplo, à prova de violação, melhorarão os recursos de auditoria e relatórios das organizações, reduzindo custos e remediando antecipadamente possíveis falhas.

Por fim, o PS2 observou que o uso de padrões nos registros pode melhorar na qualidade do que é apontado pelos profissionais em determinadas situações, como ocorre frequentemente na troca de plantões: “*talvez até na maneira que você coloca as perguntas pra gente preencher, tem como melhorar a própria qualidade da anamnese principalmente dependendo do contexto*” (PS2).

## 7.5 Lições Aprendidas e Oportunidades

A discussão entre os participantes após o uso da solução também acrescentou pontos importantes a serem observados e melhorados no presente trabalho.

O **controle de acesso pelo paciente e a LGPD** proposto pela solução foi um dos pontos relevantes observados pelos profissionais de saúde. Alguns participantes levantaram o questionamento sobre o controle de acesso por parte do paciente caso este não esteja nas condições ideais para manusear a solução. O IS2 apresentou

a seguinte situação: “[...] suponhamos que o(a) Paciente2 não autorizou ninguém a olhar os dados dele(a), então de repente ele(a) está lá na emergência, faz uma dipirona e convulsa, né? Eu não tenho o histórico dela porque ela não autorizou” (IS2). Atualmente, na presente solução, o paciente tem total gerência de suas informações, podendo escolher quem autorizar a visualização de suas informações ou desautorizá-las. Percebeu-se que, em situações de emergência, o uso da solução pode ser prejudicada, visto que pode dificultar o acesso aos registros retroativos por parte dos profissionais que ainda não foram autorizados. Dessa forma, como sugere o LM2, essas circunstâncias podem dificultar “*o controle a cerca do paciente e dos próprios manejos que tem que ser tomado*” (LM2).

Ao analisar tal impasse, percebeu-se que pode ser mitigado através da introdução de novos contratos inteligentes que trate, por exemplo, de questões administrativas, o que foge do escopo atual do presente trabalho. No experimento, a Instituição de Saúde (IS) executou tarefas semelhantes às que o Profissional de Saúde (PS) realizou. Mas, é totalmente factível estender as funcionalidades da IS para uma versão mais institucional. Dessa forma, é possível que a IS possa gerenciar os PSs que trabalham nela. Sendo assim, se o paciente autoriza o controle de acesso de suas informações para uma IS, todos os profissionais dela podem ter acesso ao(s) registro(s) do paciente. Outra solução, sugerida pelo LM1, foi a possibilidade de envio de termos formais para a *blockchain* garantindo que uma IS seja autorizada a acessar os registros do paciente. Com o termo gravado em *blockchain*, garante-se que uma decisão formal do paciente foi registrada e que pode se estender a toda uma equipe multiprofissional, possibilitando uma melhor **liberdade de acesso por profissionais de saúde para agirem em situações de emergência**.

Outra situação levantada pelos participantes foi a questão da **dificuldade de lidar com a tecnologia**. O Paciente2 observa que “[...] teria esses dois pontos: de ele tá inconsciente e de ele também está consciente, mas não saber mexer, não saber trabalhar com a tecnologia que ele tem em mãos” (Paciente2). A PS1 relata que “nem todo paciente vai entender esse fluxo” pois tem “pacientes extremamente pobres, que não tem acesso a educação” (PS1). De fato, tal problemática se faz presente em muitos setores, áreas e domínios onde ocorre uma transformação digital. Este desafio relaciona-se com a alfabetização digital, visto que o pouco letramento formal de alguns cidadãos dificulta a inclusão digital da sociedade (BROGNOLI; FERENHOF,

2020), sendo necessárias políticas públicas eficazes para tais propósitos. Porém, isso não ocorre apenas com os pacientes, pois segundo o IS1 “existem também alguns profissionais que têm dificuldades” (IS1). Portanto, fazem-se necessários os recursos adequados para o treinamento de profissionais, como endossado pelo IS1: “*requer um treinamento, requer uma capacitação da equipe de saúde pra tá usando esse prontuário de uma forma adequada*” (IS1). Ressalta-se que o próprio esforço do profissional e constante atualização tecnológica é essencial. Conforme Passos (2019), o maior impacto da tecnologia nas atividades dos médicos é a necessidade de entender que as informações em um ambiente hospitalar organizado é o alicerce da gestão de cuidado ao paciente.

Ainda sobre transformação digital, um dos impasses observados foi a **dificuldade de implantação**. O Paciente1 ressalta que “[...] *isso soluciona totalmente essa problemática, mas quando você investe toda essa solução do ponto de vista tecnológico, não vai ser completamente perfeito*” (Paciente1). A adoção de *blockchain*, de fato, ainda apresenta desafios os quais envolvem fatores institucionais relacionados desde as normas e culturas das organizações, regulamentos e leis existentes, e a governança (JANSSEN et al., 2020). Além disso, uma infraestrutura de qualidade e os requisitos técnicos atendidos adequadamente são de suma importância para a devida implantação da tecnologia, visto que o bom andamento da transformação digital depende também de uma infraestrutura de qualidade (BROGNOLI; FERENHOF, 2020). O presente trabalho realiza a avaliação técnica com regulamentações importantes, tanto considerando o desenvolvimento de PEPs, através da verificação dos requisitos técnicos estabelecidos pela SBIS, como na questão da privacidade de dados da LGPD (ver Seção 6.1.2 e 6.1.1). Tais análises podem contribuir no entendimento de uma das possibilidades de como a adoção de *blockchain* em PEPs pode ocorrer ao basear-se no arcabouço regimental brasileiro, e como isso pode afetar as organizações e as pessoas.

Considerando que a implementação do presente trabalho é uma PoC, a forma como ocorreram os registros advindos do LM foi limitada. Porém, discutiu-se a possibilidade de utilizar o sistema também para **integração com sistemas automatizados** do LM. Como informado pelo LM1, o sistema que eles utilizam para análise e geração dos resultados de exames “[...] *envia esses resultados para o servidor de interfaceamento e o servidor pega esses resultados do paciente e manda pro sistema*

*hospitalar*" (LM1). A presente solução possibilita tal comunicação, visto que na Camada de Aplicação podem ser adicionados módulos os quais se comunicam com APIs externas, por exemplo. Dessa forma, ao receber dados externos, após os devidos tratamentos, pode ser possível a inserção de informações advindas dessas APIs na *Camada de Armazenamento On-chain* e na *Camada de Armazenamento Off-chain*.

Por sua vez, especificamente sobre auditoria de informações, uma sugestão a ser considerada também é o fato de a solução armazenar o **registro dos acessos a uma prescrição específica**, por exemplo. Ou seja, cada acesso dos profissionais a um registro do paciente seria armazenado em *blockchain*, como considerado pelo LM1: "[...] *a gente pode auditar aquilo ali e ver quem foi a última pessoa que teve acesso*" (LM1). Atualmente, tem-se o log de inserções, visto que cada registro é gravado com data e hora. Todavia, é possível também implementar o registro de logs do usuário que acessou um registro para realizar a leitura, por exemplo.

Por fim, considerando o que já foi discutido, principalmente sobre o uso da solução em casos de emergência, os profissionais fizeram importantes ponderações quanto à adequação da presente proposta nos **níveis de assistência médica** adequados. O IS1 questiona "para que nível de assistência" (IS1) a solução funcionaria. O LM1 apresenta que a solução é ideal para pacientes eletivos "*que são aqueles que periodicamente vão e voltam ao hospital, né. Ele se encaixa perfeito nele*" (LM1). Em outras palavras, pacientes eletivos são aqueles que realizam procedimentos médicos que são programados, ou seja, não são considerados de urgência e emergência. O LM2 sugere que a solução é apropriada para a comunicação entre diferentes instituições, assim como a questão do controle de acesso e privacidade dos pacientes, devendo ser necessários mecanismos para lidar com situações de emergência quando se tratando de atendimento "intra-instituições".

## 7.6 Conclusão do Capítulo

Este capítulo apresentou a discussão extraída dos GFs sobre aspectos sociais a respeito de constructos colaborativos e *blockchain* atrelados aos PEPs. O resultado da discussão adveio, primeiramente, a partir de uma sequência de etapas da metodologia apresentada na Seção 4.2.2. A partir dos subtemas identificados foi possível relacioná-los com a solução proposta e a literatura.

Visto que se buscou entender o funcionamento dos prontuários atuais, tanto em papel como eletrônicos, constatou-se que um dos principais problemas que afetam a comunicação entre os profissionais é a falta de interoperabilidade e integralidade das informações entre diferentes unidades. Adicionalmente, os participantes relatam que o registro das informações é uma das tarefas relevantes a serem realizadas pelos profissionais de saúde. Em relação ao controle de acesso das informações do paciente dentro do hospital, pôde-se perceber que é relativo dependendo do contexto. Ressaltou-se que pode haver diferentes ordens e fluxos ao realizar o registro de informações da saúde do paciente por profissionais de diferentes hierarquias.

Quanto à análise do Modelo 4C em relação aos constructos colaborativos, foi possível perceber que o compartilhamento das informações pela solução utilizando *blockchain* pode impactar diretamente na comunicação, coordenação, cooperação e coordenação entre os profissionais da saúde e suas atividades em conjunto. Tal solução pode melhorar a comunicação, compartilhamento e cooperação, mitigando a perda de informações entre entidades. Além disso, através da modelagem baseada no uso de padrões de interoperabilidade, pode-se melhorar a estrutura da informação, tornando-as mais legíveis, além de deixar as trocas de plantões mais eficientes.

Constatou-se que apesar do uso da solução melhorar nos aspectos mencionados, se faz necessária a conscientização dos profissionais de saúde e a melhoria da interprofissionalidade para que os fluxos possam ser executados corretamente. Além disso, especificamente quanto ao constructo coordenação, a solução também pode proporcionar o registro imutável das ações registradas por parte dos profissionais da saúde considerando a ordem dos fluxos e respectivas hierarquias.

A solução apresentada pode proporcionar a imutabilidade das informações, consequentemente a rastreabilidade e futuras auditorias, protegendo não apenas o paciente, mas também os profissionais. Apesar de utilizar-se dessa característica, percebeu-se que se faz necessário possibilitar a criação de novas versões do mesmo registro, caso necessite de alterações. A característica de distribuição da rede influencia na facilidade de acesso por parte dos integrantes às informações e também pode evitar a perda de informações como ocorre em prontuários em papel, os quais contém vida útil. Constatou-se que boa parte dos subtemas identificados remetem-se à segurança dos envolvidos no registro de informações de saúde. Adicionalmente, a imutabilidade das informações pode influenciar na melhoria da qualidade dos processos tanto do

ponto de vista institucional como do indivíduo.

Por fim, foram elencadas algumas lições aprendidas e oportunidades quanto às características da solução e as possíveis melhorias. A principal consideração diz respeito ao controle de acesso por parte do paciente e os limites da LGPD quando o paciente estiver em situações críticas. Tais limitações indicam que a utilização da solução deve ser para contextos e níveis de atendimentos específicos. Consequentemente, novas funcionalidades deverão propiciar mais liberdade aos profissionais de saúde nessas circunstâncias. A dificuldade de lidar com a tecnologia, assim como a de implantação de soluções como essas foram consideradas.

Deve-se propiciar também a integração com sistemas automatizados já existentes, visto que existem sistemas específicos de geração de resultados de exames, como é o caso dos sistemas laboratoriais. Outro ponto importante é o registro de acessos, o qual pode servir também para futuras auditorias.

## 8 AMEAÇAS À VALIDADE

Nesta seção, discute-se sobre as potenciais ameaças que podem influenciar na validade deste trabalho, desde os tratamentos e obtenção dos resultados, até a análise destes. Identificou-se ameaças tanto no experimento técnico quanto no social. Além disso, baseando-se em Wohlin et al. (2012), as ameaças que podem afetar a validades do trabalho são descritas a seguir.

Em relação às ameaças internas, na avaliação computacional, os registros do paciente inseridos foram gerados aleatoriamente, não contendo dados reais ou formatos de mídia, como .pdf, por exemplo. Apesar disso, foi possível representá-lo pela codificação base64, tendo em vista que esta tem sido utilizada para transferência de arquivos codificados em strings. Além disso, o objetivo foi representar a carga de trabalho e suas respectivas latências.

No que concerne ao experimento social, pode-se considerar que a quantidade de etapas, a longa duração do experimento e o horário em que foi realizado poderiam causar fadiga e prejudicar o desempenho na participação e engajamento dos participantes na discussão. Para mitigar tal questão, um experimento piloto foi realizado para verificar o fluxo das etapas definidas e seu respectivo tempo de execução. Dessa forma, foi possível otimizar o fluxo e eliminar as atividades que poderiam ser redundantes na execução. Deve-se considerar também que algumas situações ou tratamentos especiais causados nos participantes podem gerar algum tipo de alteração comportamental. Ao saberem que estão sendo estudados, podem ser influenciados durante os testes, demonstrando o efeito Hawthorne (MCCAMBRIDGE et al., 2014). Para mitigar tais circunstâncias, os participantes receberam uma explicação sobre a abordagem, mas não sobre os pressupostos que foram investigados.

Quanto às ameaças externas, o experimento de desempenho da PoC permitiu inserir tamanhos de arquivos entre 1KB à 7KB, apesar de que, na realidade, os arquivos podem ter tamanhos consideráveis. Mesmo assim, as informações inseridas na *blockchain* sempre apresentaram tamanhos similares independente do tamanho do arquivo, já que são armazenados ids e *hashs* na Camada de Armazenamento *On-chain*. Referente à análise de aderência nas normas técnicas, observou-se que, por se basear no arcabouço regimental brasileiro, a generalização para outros países pode ser prejudicada. Apesar disso, a análise sobre a LGPD, por exemplo, foi alinhada

com os princípios da GDPR, que tem sido uma lei da qual os países têm se inspirado. Além disso, os mecanismos utilizados na formação da arquitetura em si, podem servir como base para outras estruturas. Em relação ao experimento social, pode-se ressaltar o número reduzido de participantes e GFs. Entretanto, conforme Pizzol (2004), o tamanho ótimo para um GF deve permitir a participação efetiva dos participantes e a discussão adequada dos temas. Isto foi contemplado na avaliação, visto que profissionais da saúde com diferentes especialidades participaram do experimento e puderam relatar suas experiências e opiniões. Quanto ao número de GFs, Debus (1994) sugere pelo menos duas sessões para cada variável considerada relevante para o tema em questão ou até que a informação obtida deixe de ser nova. Como visto no Quadro 7, vários subtemas dos GFs foram discutidos em ambos os grupos, gerando uma certa convergência, visto que os profissionais têm realidades parecidas nos sistemas de saúde atuais.

No que concerne às ameaças de conclusão, na avaliação técnica, a rede *blockchain* utilizada pode ter alterações de latências nos diferentes instantes de tempos avaliados, mesmo que com pequenas variações. Por esse motivo, foram realizadas 30 execuções considerando a média e os desvios padrões, em cada cenário do tamanho de arquivo e tipos de operações (escrita e leitura). No experimento social, um ponto importante a ser considerado é que os GFs foram realizados à distância, virtualmente, fora do ambiente controlado, o que pode afetar a resposta devido a interferências, como ruídos, configuração ou influência do ambiente computacional. Ressalta-se que, apesar do grupo pequeno, o experimento teve três especialidades diferentes da saúde, apresentando um razoável nível de heterogeneidade, cumprindo os requisitos necessários para execução do fluxo de tarefas na interface web.

Por fim, quanto às ameaças de construção, poderiam ter sido adicionadas mais métricas referente às características internas da *blockchain*. Porém, as duas métricas utilizadas são relevantes para o contexto social discutido no trabalho, visto que podem impactar diretamente na experiência do usuário. Por sua vez, referindo-se ao experimento com os participantes, os que representaram o Paciente eram da área da computação. Dessa forma, eles poderiam identificar os testes realizados mais facilmente devido aos seus conhecimentos técnicos prévios. Isto poderia influenciá-los a reduzir os erros na avaliação, fazendo com que os resultados não fossem naturais.

## 9 CONSIDERAÇÕES FINAIS

O PEP é uma estrutura que descreve e registra eventos e serviços médicos realizados aos pacientes ao longo de sua vida de forma a facilitar a tomada de decisões para definir os devidos tratamentos e processos (POSSARI, 2005). Nesse sentido, um ponto crítico a ser observado é a segurança da informação, visto que os dados do paciente devem receber tratamento adequado a fim de preservar a privacidade (MUYLDER et al., 2019). Considerando tais particularidades, o usufruto de *blockchain* no contexto de PEP tem se posicionado como proeminente tendo em vista a capacidade única de registro imutável de eventos digitais de forma transparente, segura e resiliente.

Embora a integração de PEP e *Blockchain* seja promissora, pode-se deparar com impasses ao considerar a adequação às normas, cultura e regulamentos institucionais. Consequentemente, a fim de se alinhar adequadamente, o PEP precisa ser devidamente certificado por entidades credenciadas e, adicionalmente, garantir privacidade aos dados do paciente. Por outro lado, identifica-se também a necessidade de entender como tal tecnologia pode influenciar e afetar o trabalho dos profissionais de saúde quanto aos constructos colaborativos, haja vista que o uso de *blockchain* atrelado à PEPs pode transformar os processos atuais, desde implantação tecnológica quanto as interações interpessoais.

O presente trabalho teve como principal contribuição prover uma análise detalhada sobre a adoção de *blockchain* para o contexto do PEP no cenário brasileiro sobre uma perspectiva sociotécnica. Nesse sentido, constatou-se benefícios aos quesitos de segurança e privacidade das informações clínicas compartilhadas entre diferentes entidades. Além disso, promoveu-se discussões técnicas sobre a adoção de estratégias *off-chain*, arquitetura de software e a definição do contrato inteligente. Adicionalmente, análises a partir de uma experimento social por meio de GFs puderam ser concretizadas.

### 9.1 Contribuições

As contribuições deste estudo são sintetizadas e apresentadas a seguir:

- a) Análise do arcabouço regimental para adequação do uso de *blockchain* em PEPs:** este trabalho gerou uma análise significativa das normas técnicas para o desenvolvimento de PEPs anual de certificação da SBIS e em relação

à proteção de dados do paciente (LGPD). Assim, verificou-se a viabilidade do uso de *blockchain* no domínio da saúde, de forma que fosse possível introduzir tal tecnologia respeitando regulamentações em um dado contexto. Tais análises podem servir de base para adequação de normas locais em outros países.

- b) **Proposta de arquitetura:** o estudo e a análise de aderência às normas técnicas forneceram bases consistentes para a modelagem da arquitetura de software apresentada na presente solução. A partir disso, diferentes camadas de uma arquitetura de software puderam ser projetadas e definidas utilizando-se dos diferentes componentes computacionais para compor a sua estrutura. Essas camadas foram projetadas não somente para o uso de *blockchain*, mas considerando as devidas necessidades do sistema, usando também técnicas off-chains.
- c) **Metodologia sociotécnica multi-método:** como já mencionado, a literatura é escassa no que diz respeito aos trabalhos que utilizam a metodologia sociotécnica no contexto de *blockchain*. Especificamente, nenhum trabalho sobre PEPs atrelados ao uso de *blockchain* abordou uma avaliação no contexto colaborativo. Adicionalmente, o uso de DSR possibilitou etapas bem definidas da pesquisa, possibilitando uma ênfase, principalmente, na fase de avaliação na qual foi possível utilizar diferentes métodos e processos, como é o caso do uso de GFs em trabalhos com viés mais técnico.
- d) **Implementação da PoC:** outra contribuição foi a demonstração da arquitetura proposta através da implementação de uma PoC. Toda *stack* de ferramentas utilizada para implementação foi apresentada respectivamente para cada camada, servindo como orientação no desenvolvimento de tais tecnologias. Além disso, com a PoC foi possível realizar análises em três perspectivas: (i) na identificação desta quanto à aderência às normas técnicas nacionais; (ii) no experimento computacional e (iii) utilização da interface pelos possíveis usuários do sistema.

## 9.2 Limitações

Acredita-se que os objetivos planejados para esta pesquisa foram atingidos no decorrer do desenvolvimento. No entanto, as limitações a seguir foram identificadas:

- a) O acesso ao código fonte de outras soluções é dificultado, dadas as restrições de propriedade que os pesquisadores estabelecem. Além disso, muitos dos

trabalhos apresentam apenas a proposta arquitetural. Assim, uma das limitações do presente trabalho é a falta de comparação técnica com sistemas já existentes;

- b) O fato da implementação das funcionalidades da PoC serem restrinvidas pelo escopo do trabalho, pode ter limitado novos achados e *insights* a respeito de outras particularidades de sistemas de saúde. Além disso, a implementação se deu apenas com a utilização da *blockchain Ethereum*;
- c) Em relação às métricas utilizadas, observou-se que outras também poderiam ser aplicadas para verificação do desempenho mais específico da *blockchain* quanto aos experimentos computacionais. Por outro lado, outros aspectos colaborativos poderiam ter sido explorados para um maior entendimento sobre a usabilidade do sistema por parte dos participantes;
- d) A integração com padrões de interoperabilidade de fato não foi possível implementar no presente trabalho dado o escopo planejado. Mas o presente trabalho utilizou conceitos importantes do FHIR para modelagem dos ativos.

### 9.3 Trabalhos Futuros

A fim de promover novos avanços e achados no presente estudo, pretende-se conduzir as seguintes melhorias como parte dos trabalhos futuros:

- a) Introdução de novas blockchains, tanto públicas como permissionadas a fim de possibilitar a construção de *consortium* das redes e novas funcionalidades quanto ao armazenamento dos registros e controle de acesso;
- b) Com a implementação do item anterior, por ser possível utilizar novos algoritmos de consenso através das novas blockchains adicionadas. Tal possibilidade por proporcionar um aumento na velocidade de latências e transações por segundo;
- c) A utilização de novas métricas para o experimento computacional para verificar o desempenho de forma mais específica das redes, como número de transações por bloco, por exemplo. Já em relação ao experimento social, incluir avaliações relacionadas à novos constructos colaborativos, como *Technology Acceptance Model* (DAVIS, 1989), especificamente visando entender a utilidade percebida e facilidade de uso identificados pelo paciente;
- d) Integração da solução com APIs de padrões de interoperabilidade, como FHIR. Possivelmente com melhorias no modelo arquitetural, criando camadas mais

dedicadas à esta integração;

- e) Apesar de que os temas nos GFs acabaram convergindo, com a implementação de novas funcionalidades, pode ser possível a utilização de novos cenários com um número maior de participantes a fim de gerar novos achados;
- f) Pretende-se incluir novos tipos de papéis de usuários. Por exemplo, entidades que representam Farmácias podem ser adicionadas. Além disso, os pesquisadores também podem fazer parte da rede, visto que o volume de informações adicionadas podem contribuir para estudos.

## REFERÊNCIAS

- ACHARYA, V.; YERRAPATI, A. E.; PRAKASH, N. **Oracle Blockchain Quick Start Guide**: a practical approach to implementing blockchain in your enterprise. Birmingham: Packt Publishing Ltd, 2019. 350 p.
- AGBO, C. C.; MAHMOUD, Q. H.; EKLUND, J. M. Blockchain technology in healthcare: a systematic review. **Healthcare**, Multidisciplinary Digital Publishing Institute, v. 7, n. 2, p. 56, abr. 2019. Disponível em: <<https://www.mdpi.com/2227-9032/7/2/56>>. Acesso em: 27 jan. 2020.
- AGOSTINHO, B.; SCHREINER, G.; GOMES, F.; PINTO, A. S. R.; DANTAS, M. Unificação de dados de saúde através do uso de blockchain e smart contracts. In: XV ESCOLA REGIONAL DE BANCO DE DADOS, 15., 2019, Santa Catarina. **Anais...** Santa Catarina, Brasil: SBC, 2019. p. 31–40.
- AGUIAR, E. J. D.; FAIÇAL, B. S.; KRISHNAMACHARI, B.; UYEYAMA, J. A survey of blockchain-based strategies for healthcare. **ACM Computing Surveys (CSUR)**, New York, USA, v. 53, n. 2, p. 1–27, 2020. Disponível em: <<https://doi.org/10.1145/3376915>>. Acesso em: 27 abr. 2020.
- ANTONOPoulos, A. M. **Mastering Bitcoin**: unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly Media, 2014. 298 p.
- ANTONOPoulos, A. M.; WOOD, G. **Mastering Ethereum**: building smart contracts and dapps. Sebastopol, CA: O'Reilly Media, 2018. 424 p.
- ARAUJO, R. J. V. **Aula II - Educação Interprofissional e Suas Bases Teórico Conceptuais E Metodológicas**, Brasil, 29 abr. 2021. Disponível em: <[https://www.docscopy.com/pt/pratica-em-saude-integrativa-4/7395914](https://www.docscopy.com/pt/pratica-em-saude-integrativa-4/7395914/)>. Acesso em: 20 jun. 2021.
- BACELAR, G.; CORREIA, R. **As bases do openEHR**. Porto, Portugal: Virtual Care, 2015. 43 p.
- BACH, L.; MIHALJEVIC, B.; ZAGAR, M. Comparative analysis of blockchain consensus algorithms. In: INTERNATIONAL CONVENTION ON INFORMATION AND COMMUNICATION TECHNOLOGY, ELECTRONICS AND MICROELECTRONICS (MIPRO), 41., 2018, Opatija. **Anais...** Opatija: IEEE, 2018. p. 1545–1550.
- BARCELOS, N. **Os pilares da Segurança da Informação – Quais são e qual sua importância para uma segurança efetiva**, Belo Horizonte, 16 jul. 2019. Tripla IT. Disponível em: <[https://triplait.com/os-pilares-da-seguranca-da-informacao](https://triplait.com/os-pilares-da-seguranca-da-informacao/)>. Acesso em: 12 mar. 2021.
- BASHIR, I. **Mastering blockchain**. Birmingham, United Kingdom: Packt Publishing Ltd, 2017. 540 p.
- BAYAZIT, N. Investigating design: A review of forty years of design research. **Design issues**, Massachusetts, v. 20, n. 1, p. 16–29, jan. 2004. Disponível em: <<https://ieeexplore.ieee.org/document/6789750>>. Acesso em: 27 abr. 2020.
- BECK, R.; AVITAL, M.; ROSSI, M.; THATCHER, J. B. Blockchain technology in business and information systems research. **Business Information Systems Engineering**,

Springer, Alemanha, v. 59, n. 10, p. 381–384, nov. 2017. Disponível em: <<https://doi.org/10.1007/s12599-017-0505-1>>. Acesso em: 27 abr. 2020.

BECK, R.; WEBER, S.; GREGORY, R. W. Theory-generating design science research. **Information Systems Frontiers**, Springer, Netherlands, v. 15, n. 4, p. 637–651, fev. 2013. Disponível em: <<https://doi.org/10.1007/s10796-012-9342-4>>. Acesso em: 27 abr. 2020.

BENSON, T.; GRIEVE, G. **Principles of health interoperability: SNOMED CT, HL7 and FHIR**. Londres, Inglaterra: Springer, 2021. 79–102 p.

BENTOV, I.; LEE, C.; MIZRAHI, A.; ROSENFELD, M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]. **ACM SIGMETRICS Performance Evaluation Review**, ACM New York, NY, USA, v. 42, n. 3, p. 34–37, 2014. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/2695533.2695545>>. Acesso em: 10 ago. 2020.

BOWEN, G. A. et al. Document analysis as a qualitative research method. **Qualitative research journal**, United Kingdom, v. 9, n. 2, p. 27–40, ago. 2009. Disponível em: <<https://www.emerald.com/insight/content/doi/10.3316/QRJ0902027/full/html>>. Acesso em: 2 fev. 2021.

BRASIL. Conselho Federal de Enfermagem. Resolução COFEN nº 564/2017, de 6 de novembro de 2017. Aprova o novo Código de Ética dos Profissionais de Enfermagem. **Diário Oficial da União**. Brasília, DF, 2002. Disponível em: <<http://www.cofen.gov.br/resolucao-cofen-no-5642017\59145.html>>. Acesso em: 18 set. 2020.

BRASIL. Conselho Federal de Medicina. Resolução CFM nº 1.638/2002, de 9 de agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. **Diário Oficial da União**. Brasília, DF, 2002. Disponível em: <<https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638>>. Acesso em: 18 set. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF, 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)>. Acesso em: 28 jul. 2020.

BROGNOLI, T. da S.; FERENHOF, H. A. Transformação digital no governo brasileiro: desafios, ações e perspectivas. **Navus: Revista de Gestão e Tecnologia**, Serviço Nacional de Aprendizagem Comercial (Senac), Brasil, v. 10, n. 1, p. 41–50, 2020. Disponível em: <<https://dialnet.unirioja.es/servlet/articulo?codigo=7774794>>. Acesso em: 5 jun. 2021.

BUTERIN, V. et al. **Ethereum White Paper**. Londres, Inglaterra: GitHub repository, 2013. v. 1. 32 p. Disponível em: <<https://ethereum.org/en/whitepaper/>>. Acesso em: 09 set. 2020.

CASTRO, M.; LISKOV, B. et al. Practical byzantine fault tolerance. In: **THIRD SYMPOSIUM ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION**, 3., 1999, New Orleans. **Anais...** Califórnia, USA: USENIX Association, 1999. p. 173–186.

CHEHAB, G. C. O direito ao esquecimento na sociedade da informação. **Revista dos Tribunais [recurso eletrônico]**, São Paulo, v. 104, n. 952, fev. 2015. Disponível em: <<https://dspace.almg.gov.br/xmlui/handle/11037/17254>>. Acesso em: 20 mar. 2021.

CHRISTIDIS, K.; DEVETSIKOTIS, M. Blockchains and smart contracts for the internet of things. **IEEE Access**, Austrália, v. 4, p. 2292–2303, mai. 2016. Disponível em: <<https://ieeexplore.ieee.org/document/7467408>>. Acesso em: 02 abr. 2021.

CONCEIÇÃO, A. F. da; SILVA, F. S. C. da; ROCHA, V.; LOCORO, A.; BARGUIL, J. M. Eletronic health records using blockchain technology. **ArXiv**, v. 1804.10078, p. 1–15, abr. 2018. Disponível em: <<https://arxiv.org/pdf/1804.10078.pdf>>. Acesso em: 25 set. 2020.

CONSULTING, C. **Consequences of Poorly Performing Software Systems**. 2014. 7 p. Disponível em: <<https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/COLLABUS/C140206C.pdf>>. Acesso em: 28 jul. 2021.

COOPER, J.; LEWIS, R.; URQUHART, C. et al. Using participant or non-participant observation to explain information behaviour. **Information Research**, Suécia, v. 9, n. 4, p. 16, jul. 2004. Disponível em: <<http://informationr.net/ir/9-4/paper184.html>>. Acesso em: 1 mar. 2021.

CORPORATION, I. **PoET 1.0 Specification**. 2017. Disponível em: <<https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html>>. Acesso em: 20 mar. 2020.

COSTA, A. M. Nicolaci da; PIMENTEL, M. Sistemas colaborativos para uma nova sociedade e um novo ser humano. In: PIMENTEL, M.; FUKS, H. (orgs.). **Sistemas Colaborativos**. Rio de Janeiro: Elsevier, 2011. p. 1–13.

COSTA, A. P.; LOUREIRO, M. J.; REIS, L. P. Do modelo 3c de colaboração ao modelo 4c: Modelo de análise de processos de desenvolvimento de software educativo. **Revista Lusófona de Educação**, Portugal, v. 27, n. 27, p. 181–200, set. 2014. Disponível em: <<https://repository.sdum.uminho.pt/bitstream/1822/64052/1/n27a12.pdf>>. Acesso em: 8 mar. 2021.

CUKIERMAN, H. L.; TEIXEIRA, C.; PRIKLADNICKI, R. Um olhar sociotécnico sobre a engenharia de software. **Revista de Informática Teórica e Aplicada**, Brasil, v. 14, n. 2, p. 199–219, dez. 2007. Disponível em: <<https://is.cos.ufrj.br/wp-content/uploads/2019/05/Um-Olhar-Sociotecnico-sobre-a-Engenharia-de-Software.pdf>>. Acesso em: 7 jan. 2021.

DAVIS, F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. **MIS quarterly**, USA, v. 13, n. 3, p. 319–340, set. 1989. Disponível em: <<https://www.jstor.org/stable/249008>>. Acesso em: 28 out. 2020.

DEBUS, M. **Manual para excelencia en la investigación mediante grupos focales**. Washington, D.C.: Academy for Educational Development, 1994. 97 p.

DHAGARRA, D.; GOSWAMI, M.; SARMA, P.; CHOUDHURY, A. Big data and blockchain supported conceptual model for enhanced healthcare coverage. **Business Process Management Journal**, United Kingdom, v. 25, n. 7, p. 1612–1632, mar. 2019. Disponível em: <<https://www.emerald.com/insight/content/doi/10.1108/BPMJ-06-2018-0164/full/html>>. Acesso em: 28 jul. 2021.

EBERHARDT, J.; TAI, S. On or off the blockchain? insights on off-chaining computation and data. In: EUROPEAN CONFERENCE ON SERVICE-ORIENTED AND CLOUD COMPUTING, 6., 2017, Oslo. **Anais...** Oslo, Noruega: Springer, 2017. p. 3–15.

FAN, K.; WANG, S.; REN, Y.; LI, H.; YANG, Y. Medblock: efficient and secure medical data sharing via blockchain. **Journal of Medical Systems**, USA, v. 42, n. 8, p. 136, jun. 2018. Disponível em: <<https://link.springer.com/article/10.1007/s10916-018-0993-7>>. Acesso em: 23 jan. 2020.

FHIR. **FHIR Specification - Resources List**. 2019. Disponível em: <<https://www.hl7.org/fhir/resourcelist.html>>. Acesso em: 19 mar. 2021.

FUENTES, L. Clinicappchain: a low-cost blockchain hyperledger solution for healthcare. In: INTERNATIONAL CONGRESS ON BLOCKCHAIN AND APPLICATIONS, 1., 2019, Ávila. **Anais...** Ávila, Espanha: Springer, 2019. p. 36.

FURKS, H.; PIMENTEL, M. **Sistemas Colaborativos**. Rio de Janeiro: Elsevier, 2011. 416 p.

GARCIA, L. R. et al. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. São Paulo, Brasil: Editora Blucher, 2020. 128 p.

GODOY, A. S. Uma revisão histórica dos principais autores e obras que refletem esta metodologia de pesquisa em ciências sociais. **Revista de Administração de Empresas**, São Paulo, Brasil, v. 23, n. 2, p. 57–63, 1995. Disponível em: <<https://www.scielo.br/j/rae/a/wf9CgwXVjpLFVgpwNkCgnC/?format=pdf&lang=pt>>. Acesso em: 02 set. 2020.

GOMEZ. **Why Web Performance Matters: Is Your Site Driving Customers Away?** 2011. 8 p. Disponível em: <[http://www.mcrinc.com/Documents/Newsletters/201110\\_why\\_web\\_performance\\_matters.pdf](http://www.mcrinc.com/Documents/Newsletters/201110_why_web_performance_matters.pdf)>. Acesso em: 28 jul. 2021.

GONÇALVES, M. I.; ROCHA, P. K.; ANDERS, J. C.; KUSAHARA, D. M.; TOMAZONI, A. Comunicação e segurança do paciente na passagem de plantão em unidades de cuidados intensivos neonatais. **Texto & Contexto-Enfermagem**, Santa Catarina, Brasil, v. 25, n. 1, 2016. Disponível em: <<https://www.scielo.br/j/tce/a/4pFXWwtDd4j4qGd8pkshVys/?format=pdf&lang=pt>>. Acesso em: 1 ago. 2021.

GREVE, F. G. et al. Blockchain e a revolução do consenso sob demanda. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 36., 2018, São Paulo. **Anais...** São Paulo, Brasil: SBC, 2018. p. 1–52. Disponível em: <<http://143.54.25.88/index.php/sbrcminicursos/article/view/1770>>. Acesso em: 03 ago. 2020.

GROENEVELD, W. et al. Exploring the role of creativity in software engineering. In: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING: SOFTWARE ENGINEERING IN SOCIETY (ICSE-SEIS), 43., 2021, Madrid. **Anais...** New York, NY, USA: IEEE, 2021. p. 1–9.

GUPTA, S.; SADOGHI, M. Blockchain transaction processing. **Encyclopedia of Big Data Technologies**, 2019. Disponível em: <[https://www.researchgate.net/publication/325116198\\_Blockchain\\_Transaction\\_Processing](https://www.researchgate.net/publication/325116198_Blockchain_Transaction_Processing)>. Acesso em: 02 ago. 2020.

HAQUE, R. et al. Blockchain-based information security of electronic medical records (EMR) in a healthcare communication system. In: PENG, S.; SON, L. H.; SUSEENDRAN, G.; BALAGANESH, D. (eds.). **Intelligent Computing and Innovation on Data Science**. Singapore: Springer, 2020. p. 641–650.

HASSELGREN, A.; WAN, P. K.; HORN, M.; KRALEVSKA, K.; GLIGOROSKI, D.; FAXVAAG, A. GDPR compliance for blockchain applications in healthcare. **ArXiv**, v. 2009.12913, p. 1–8, set. 2020. Disponível em: <<https://arxiv.org/pdf/2009.12913.pdf>>. Acesso em: 25 nov. 2020.

IBARRA, J.; JAHANKHANI, H.; KENDZIERSKYJ, S. Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime. In: JAHANKHANI, H.; KENDZIERSKYJ, S.; JAMAL, A.; EPIPHANIOU, G.; AL-KHATEEB, H. (eds.). **Blockchain and Clinical Trial**. [S.I.]: Springer, 2019. p. 115–137.

JAHAN, F.; MOSTAFA, M.; CHOWDHURY, S. Sha-256 in parallel blockchain technology: Storing land related documents. **International Journal of Computer Applications**, United States, v. 175, n. 35, p. 8887, 2020. Disponível em: <[https://www.researchgate.net/profile/Fariha-Jahan-3/publication/347738608\\_SHA-256\\_in\\_Parallel\\_Blockchain\\_Technology\\_Storing\\_Land\\_Related\\_Documents/links/5feb9eb045851553a004e504/SHA-256-in-Parallel-Blockchain-Technology-Storing-Land-Related-Documents.pdf](https://www.researchgate.net/profile/Fariha-Jahan-3/publication/347738608_SHA-256_in_Parallel_Blockchain_Technology_Storing_Land_Related_Documents/links/5feb9eb045851553a004e504/SHA-256-in-Parallel-Blockchain-Technology-Storing-Land-Related-Documents.pdf)>. Acesso em: 02 mar. 2021.

JANSSEN, M.; WEERAKKODY, V.; ISMAGILOVA, E.; SIVARAJAH, U.; IRANI, Z. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. **International Journal of Information Management**, United Kingdom, v. 50, n. 1, p. 302–309, 2020. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0268401219305067>>. Acesso em: 25 jul. 2021.

JENAL, S.; ÉVORA, Y. D. M. Desafio da implantação do prontuário eletrônico do paciente. **Journal of Health Informatics**, São Paulo, v. 4, n. 1, p. 216–219, 2012. Disponível em: <<http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/view/253>>. Acesso em: 04 jun. 2021.

KARANTIAS, K.; KIAYIAS, A.; ZINDROS, D. Proof-of-burn. In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 24., 2020, Kota Kinabalu, Malaysia. **Anais...** [S.I.]: Springer, 2020. p. 523–540.

KING, S.; NADAL, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. **Self-published Paper**, v. 19, p. 1, 2012. Disponível em: <<https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf>>. Acesso em: 10 ago. 2020.

KLEIN, L. What do we actually mean by 'sociotechnical'? on values, boundaries and the problems of language. **Applied ergonomics**, United States, v. 45, n. 2, p. 137–142, 2014. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0003687013000690>>. Acesso em: 24 ago. 2021.

KOTESKA, B.; KARAFILOSKI, E.; MISHEV, A. Blockchain implementation quality challenges: a literature. In: WORKSHOP OF SOFTWARE QUALITY, ANALYSIS, MONITORING, IMPROVEMENT, AND APPLICATIONS (SQAMIA), 6., 2017, Belgrade, Serbia. **Anais...** Belgrade, Serbia: CEUR, 2017. p. 11–13.

KUJAWSKI, G. Tropeços colaborativos. **GV EXECUTIVO**, [S.I.], v. 2, n. 1, p. 61–65, 2003. Disponível em: <<https://rae.fgv.br/sites/rae.fgv.br/files/artigos/1770.pdf>>. Acesso em: 27 ago. 2021.

LAHM, J. V.; CARVALHO, D. R. Prontuário eletrônico do paciente: avaliação de usabilidade pela equipe de enfermagem. **Cogitare Enfermagem**, Curitiba, PR, v. 20, n. 1, p. 38–44, 2015. Disponível em: <<https://revistas.ufpr.br/cogitare/article/view/36485>>. Acesso em: 02 jul. 2020.

LAKSHMAN, A.; MALIK, P. Cassandra: a decentralized structured storage system. **ACM SIGOPS Operating Systems Review**, v. 44, n. 2, p. 35–40, 2010. Disponível em: <<https://dl.acm.org/doi/10.1145/1773912.1773922>>. Acesso em: 11 jun. 2021.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. **The Byzantine generals problem**. [S.l.: s.n.], 2019. 203–226 p.

LARRY, S.; IAKOVOU, L.; IACOPELLA, M. V. **Transforming Trade and Ensuring Global Supply Chain Security with Blockchain and Smart Contracts**. 2021. Disponível em: <<https://uh.edu/bti/research/shi-iakovou-blockchain/bti-writtendeliverables-blockchainshi-final-reduced1.pdf>>. Acesso em: 21 jun. 2021.

LIN, I.-C.; LIAO, T.-C. A survey of blockchain security issues and challenges. **IJ Network Security**, v. 19, n. 5, p. 653–659, 2017. Disponível em: <<http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf>>. Acesso em: 07 ago. 2020.

LIU, W.; YU, Q.; LI, Z.; LI, Z.; SU, Y.; ZHOU, J. A blockchain-based system for anti-fraud of healthcare insurance. In: **International Conference on Computer and Communications (ICCC)**, 5. Chengdu, China: IEEE, 2019. p. 1264–1268.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39–52, 2021.

LUCENA, A. U. de; HENRIQUES, M. A. A. Estudo de arquiteturas dos blockchains de bitcoin e ethereum. In: IX ENCONTRO DE ALUNOS E DOCENTES DO DCA/FEEC/UNICAMP (EADCA), 9., Campinas. **Anais...** Campinas, 2016. p. 4.

LUU, L.; NARAYANAN, V.; ZHENG, C.; BAWEJA, K.; GILBERT, S.; SAXENA, P. A secure sharding protocol for open blockchains. In: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 23., 2016, Vienna, Austria. **Anais...** New York, United States: Association for Computing Machinery, 2016. p. 17–30.

MARTINS, L.; SARTOR, G. D.; SILVA, M. P. da. Prontuário eletrônico do paciente: Adoção de novas tecnologias de acesso. **Journal of Health Informatics**, v. 11, n. 3, p. 67–73, 2019. Disponível em: <<http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/viewFile/608/361>>. Acesso em: 29 mai. 2021.

MASSAD, E.; MARIN, H. d. F.; NETO, R. S. d. A. O prontuário eletrônico do paciente na assistência, informação e conhecimento médico. In: **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico**. [S.l.: s.n.], 2003. p. iii–202.

MAZLAN, A. A.; DAUD, S. M.; SAM, S. M.; ABAS, H.; RASID, S. Z. A.; YUSOF, M. F. Scalability challenges in healthcare blockchain system—a systematic review. **IEEE Access**, v. 8, p. 23663–23673, 2020. Disponível em: <<https://ieeexplore.ieee.org/document/8968381>>. Acesso em: 10 jan. 2021.

MCCAMBRIDGE, J.; WITTON, J.; ELBOURNE, D. R. Systematic review of the hawthorne effect: new concepts are needed to study research participation effects. **Journal of clinical epidemiology**, Elsevier, v. 67, n. 3, p. 267–277, 2014. Disponível em: <<https://pubmed.ncbi.nlm.nih.gov/24275499/>>. Acesso em: 25 jul. 2020.

MCFARLANE, C.; BEER, M.; BROWN, J.; PRENDERGAST, N. Patientory: a healthcare peer-to-peer emr storage nntwork v1. **Entrust Inc.: Addison**, p. 1–19, 2017. Disponível em: <<https://www.patientory.com/wp-content/uploads/2017/04/>>. Acesso em: 19 jan. 2020.

METCALFE, W. Ethereum, smart contracts, dapps. In: **Blockchain and Crypt Currency**. [S.I.]: Springer, Singapore, 2020. p. 77–93.

MINGXIAO, D.; XIAOFENG, M.; ZHE, Z.; XIANGWEI, W.; QIJUN, C. A review on consensus algorithm of blockchain. In: IEEE INTERNATIONAL CONFERENCE ON SYSTEMS, MAN, AND CYBERNETICS (SMC), 1., 2017 Banff. Banff: IEEE, 2017. p. 2567–2572.

MIRANDA, C. F. et al. **Manual de Certificação para Sistemas de Registro Eletrônico em Saúde**. 4.3. ed., [S.I.:S.n.]. 2019. 167 p. Disponível em: <[http://www.sbis.org.br/certificacao/Manual\\_Certificacao\\_SBIS-CFM\\_2019\\_v4-3.pdf](http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2019_v4-3.pdf)>. Acesso em: 03 abr. 2020.

MÖLKEN, R. V. **Blockchain across Oracle**: understand the details and implications of the Blockchain for Oracle developers and customers. [S.I.]: Packt Publishing Ltd, 2018. 532 p.

MORAES, C. R. Bassan de; VALENTIM, M. L.; SOUZA, L. P. Pinheiro de. Recursos informacionais para a construção do conhecimento em empresas de software: Abordagem sistêmica. **Brazilian Journal of Information Science**, Marília, São Paulo, v. 13, n. 3, 2019. Disponível em: <<https://revistas.marilia.unesp.br/index.php/bjis/article/view/8933>>. Acesso em: 03 mai. 2020.

MORGAN, D. L. Focus groups. **Annual review of sociology**, v. 22, n. 1, p. 129–152, 1996. Disponível em: <[https://www.researchgate.net/profile/David-Morgan-43/publication/305389505\\_Focus\\_Groups/links/5bcaa150299bf17a1c61a4fe/Focus-Groups.pdf](https://www.researchgate.net/profile/David-Morgan-43/publication/305389505_Focus_Groups/links/5bcaa150299bf17a1c61a4fe/Focus-Groups.pdf)>. Acesso em: 2 ago. 2021.

MOURÃO, A. D.; NEVES, J. d. R. Impactos da implantação do prontuário eletrônico do paciente sobre o trabalho dos profissionais de saúde da prefeitura municipal de belo horizonte. In: **Anais do Simpósio de Excelência em Gestão e Tecnologia**, 4. Rio de Janeiro: AEDB, 2007. p. 22–24.

MUYLDER, C. F. D.; OLIVEIRA, J. G. de; BATISTA, C. L.; MARQUES, R. M. Segurança da informação ea área da saúde: a convergência dos temas ea intensidade das publicações científicas. **Revista de Gestão em Sistemas de Saúde**, v. 8, n. 2, 2019. Disponível em: <<https://periodicos.uninove.br/revistargss/article/view/14139>>. Acesso em: 01 abr. 2019.

NABBEN, K. Blockchain security as “people security”: Applying sociotechnical security to blockchain technology. **Frontiers in Computer Science**, Frontiers, v. 2, p. 62, 2021. Disponível em: <<https://www.frontiersin.org/articles/10.3389/fcomp.2020.599406/full>>. Acesso em: 14 abr. 2021.

- NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 02 mar. 2020.
- NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. New Jersey: Princeton University Press, 2016. 328 p.
- NASCIMENTO, J. d. S. G.; RODRIGUES, R. R.; PIRES, F. C.; GOMES, B. F. Passagem de plantão como ferramenta de gestão parasegurança do paciente. **Rev. enferm. UFSM**, v. 8, n. 3, p. 1–16, 2018. Disponível em: <<https://periodicos.ufsm.br/reufsm/article/view/29412>>. Acesso em: 18 mai. 2021.
- NGUYEN, G.-T.; KIM, K. A survey about consensus algorithms used in blockchain. **Journal of Information processing systems**, v. 14, n. 1, p. 101–128, 2018. Disponível em: <[https://volunteerscience.com/media/research\\_teams/Luke's\%20Sandbox/consent\\_forms/revised\\_proposal.2.pdf](https://volunteerscience.com/media/research_teams/Luke's\%20Sandbox/consent_forms/revised_proposal.2.pdf)>. Acesso em: 11 ago. 2020.
- NIELSEN, J. **Usability engineering**. California, USA: Morgan Kaufmann, 1994.
- OLIVEIRA, N. M.; VITERBO, J.; BOSCAROLI, C. Disrupção e apropriação tecnológica: Uma experiência com airbnb em um destino turístico não indutor. In: **Proceedings of Information Systems in Latin America Conference (ISLA)**, 4. UT, United States: [s.n.], 2020. p. 11.
- ONIK, M. M. H.; AICH, S.; YANG, J.; KIM, C.-S.; KIM, H.-C. Blockchain in health-care: Challenges and solutions. In: **Big data analytics for intelligent healthcare management**. London, UK: Elsevier, 2019. p. 197–226.
- ONWUEGBUIZE, A. J.; DICKINSON, W. B.; LEECH, N. L.; ZORAN, A. G. A qualitative framework for collecting and analyzing data in focus group research. **International journal of qualitative methods**, v. 8, n. 3, p. 1–21, 2009. Disponível em: <<https://journals.sagepub.com/doi/full/10.1177/160940690900800301>>. Acesso em: 10 jun. 2021.
- OPENEHR. **What is openEHR?** 2021. Disponível em: <[https://www.openehr.org/about/what\\_is\\_openehr](https://www.openehr.org/about/what_is_openehr)>. Acesso em: 18 mar. 2021.
- PARK, S.; PIETRZAK, K.; ALWEN, J.; FUCHSBAUER, G.; GAZI, P. **Spacecoin: a cryptocurrency based on proofs of space**. IACR Cryptology ePrint Archive, 2015. v. 528. 29 p. Disponível em: <<https://eprint.iacr.org/2015/528.pdf>>.
- PASSOS, C. N. Transformação digital na saúde: Desafios e perspectivas. **Revista Científica Hospital Santa Izabel**, v. 3, n. 3, p. 178–184, 2019. Disponível em: <<https://revistacientifica.hospitalsantaizabel.org.br/index.php/RCHSI/article/view/53/34>>. Acesso em: 5 jun. 2021.
- PETRONI, B. C. A.; FRANCO, G. R. Smart contracts baseados em blockchain na cadeia de custódia digital: uma proposta de arquitetura. In: **Proceedings of International Conference on Forensic Computer Science and Cyber Law (ICOFCS)**. São Paulo, Brazil: [s.n.], 2018. p. 23–30.
- PIMENTEL, M.; GEROSA, M. A.; FILIPPO, D.; RAPOSO, A.; FUKS, H.; LUCENA, C. J. P. d. Modelo 3c de colaboração para o desenvolvimento de sistemas colaborativos.

In: III SIMPÓSIO BRASILEIRO DE SISTEMAS COLABORATIVOS, 3., 2006, Vienna. **Anais...** [S.I.], 2006. p. 58–67.

PIOVESAN, A.; TEMPORINI, E. R. Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública. **Revista de Saúde Pública**, v. 29, n. 4, p. 318–325, 1995. Disponível em: <<https://www.scielo.br/j/rsp/a/fF44L9rmXt8PVYLNvphJgTd/?lang=pt>>. Acesso em: 02 set. 2020.

PIZZOL, S. J. S. d. Combinação de grupos focais e análise discriminante: um método para tipificação de sistemas de produção agropecuária. **Revista de Economia e Socio-Logia Rural**, SciELO Brasil, v. 42, n. 3, p. 451–468, 2004. Disponível em: <<https://www.scielo.br/j/resr/a/r5ffkfdPkVWJhrjFJTStDzf/abstract/?lang=pt&format=html>>. Acesso em: 21 jun. 2020.

POSSARI, J. F. **Prontuário do paciente e os registros de enfermagem**. 2. ed. [S.I.]: Editora Érica, 2005. 248 p.

PRINZ, W. Blockchain and cscw—shall we care? In: PROCEEDINGS OF 16TH EUROPEAN CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK-EXPLORATORY PAPERS, 16., 2017 Bonn, Germany. **Anais...** Bonn, Germany: European Society for Socially Embedded Technologies (EUSSET), 2018.

QUEIROZ, V. F. de; BURGER, I. J. D.; GONÇALVES, M.; AGUIAR, L. F. de S.; PRESTES, J. My health data conectando pessoas, gerando saúde. In: SIMPÓSIO INTERNACIONAL NETWORK SCIENCE, 2., 2018, Rio de Janeiro. **Anais...** Rio de Janeiro, 2018.

RAIKWAR, M.; GLIGOROSKI, D.; VELINOV, G. Trends in development of databases and blockchain. In: INTERNATIONAL CONFERENCE ON SOFTWARE DEFINED SYSTEMS (SDS), 7., Paris, France. **Anais...** New York, NY, USA: IEEE, 2020. p. 177–182.

RAMACHANDRAN, S. et al. A review on blockchain-based strategies for management of electronic health records (ehrs). In: INTERNATIONAL CONFERENCE ON SMART ELECTRONICS AND COMMUNICATION (ICOSEC), 2020, Trichy. **Anais...** Trichy, India: IEEE, 2020. p. 341–346.

RAVAL, S. **Decentralized applications: harnessing Bitcoin's blockchain technology**. [S.I.]: "O'Reilly Media, Inc.", 2016.

REIS, I. M. d. O. **O direito ao esquecimento e a proteção dos dados pessoais: uma perspectiva analisada num confronto com a proposta adotada pela legislação da união europeia e o ordenamento jurídico brasileiro**. Trabalho de Conclusão de Curso (Graduação em Direito) – Curso de Direito, Fortaleza, 2018. Disponível em: <[http://www.repositorio.ufc.br/bitstream/riufc/41249/1/2018\\_tcc\\_imoreis.pdf](http://www.repositorio.ufc.br/bitstream/riufc/41249/1/2018_tcc_imoreis.pdf)>. Acesso em: 20 out. 2018.

RICARTE, I. L. Sistemas nacionais de prontuários eletrônicos frente à privacidade de dados. 2019. Disponível em: <<http://eprints.rclis.org/33929/>>. Acesso em: 30 mai. 2021.

ROCHA, C. P. da; CARNEIRO, A. V. S.; MEDEIROS, M. V. B.; MELO, A. Segurança da informação: A iso 27.001 como ferramenta de controle para lgpd. **Revista de**

**Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78–97, 2019. Disponível em: <<http://www.revistasfap.com/ojs3/index.php/tic/article/view/285/246>>. Acesso em: 5 abr. 2021.

ROCHA, F. H.; ARAÚJO, A. A.; SOARES, P.; SARAIVA, R. L.; SOUZA, J. T. de. Uma avaliação de desempenho de soluções off-chain baseadas em sistemas de armazenamento distribuído. **iSys-Brazilian Journal of Information Systems**, Porto Alegre, RS, v. 14, n. 1, p. 04–23, 2021. Disponível em: <<https://sol.sbc.org.br/journals/index.php/isys/article/view/808/1752>>. Acesso em: 12 ago. 2021.

ROY, B. Advances in cryptology. In: INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOLOGY AND INFORMATION SECURITY, 11., 2005, Chennai, India. **Anais...** [S.I.]: Springer Science & Business Media, 2005.

RUARO, R. L.; GLITZ, G. P. C. Panorama geral da lei geral de proteção de dados pessoais no brasil e a inspiração no regulamento geral de proteção de dados pessoais europeu. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor**, Brasília, Brasil, v. 6, n. 2, p. 340–356, set. 2020. Disponível em: <<https://portalrevistas.ucb.br/index.php/REPATS/article/view/11545>>. Acesso em: 15 jun. 2021.

RUBIN, J.; CHISNELL, D. **Handbook of usability testing: how to plan, design and conduct effective tests**. [S.I.]: John Wiley & Sons, 2008. 384 p.

SBIS. **Cartilha sobre prontuário eletrônico: a certificação de sistemas de registro eletrônico de Saúde**. 2012. Disponível em: <[https://portal.cfm.org.br/crmdigital/Cartilha\\_SBIS\\_CFM\\_Prontuario\\_Eletronico\\_fev\\_2012.pdf](https://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf)>. Acesso em: 18 set. 2020.

SCHORR, V.; SEBOLD, L. F.; SANTOS, J. L. G. d.; NASCIMENTO, K. C. d.; MATOS, T. A. Passagem de plantão em um serviço hospitalar de emergência: perspectivas de uma equipe multiprofissional. **Interface-Comunicação, Saúde, Educação**, v. 24, p. e190119, 2020. Disponível em: <<https://www.scielo.br/j/icse/a/kjQFKPxCMzDqrsmGpqHw8Zm/abstract/?lang=pt>>. Acesso em: 2 ago. 2021.

SHAHNAZ, A.; QAMAR, U.; KHALID, A. Using blockchain for electronic health records. **IEEE Access**, IEEE, v. 7, p. 147782–147795, 2019. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8863359>>. Acesso em: 15 jan. 2020.

SHIN, D.; IBAHRINE, M. The socio-technical assemblages of blockchain system: How blockchains are framed and how the framing reflects societal contexts. **Digital Policy, Regulation and Governance**, Emerald Publishing Limited, v. 22, n. 3, p. 245–263, 2020. Disponível em: <<https://www.emerald.com/insight/content/doi/10.1108/DPRG-11-2019-0095/full/html>>. Acesso em: 18 abr. 2021.

SHUKLA, P. A.; SAMET, S. Systematization of knowledge on scalability aspect of blockchain systems. In: FUTURE OF INFORMATION AND COMMUNICATION CONFERENCE, 2020, San Francisco, United States. **Anais...** [S.I.]: Springer, 2020. p. 130–138.

SOARES, P.; ARAÚJO, A. A.; SARAIVA, R.; SANTOS, R.; SOUZA, J. Prontuário eletrônico do paciente baseado em blockchain: Um desenho de pesquisa sociotécnico. In: XVII SIMPÓSIO BRASILEIRO DE SISTEMAS COLABORATIVOS, 12., Rio de Janeiro. **Anais...** Porto Alegre, RS: SBC Openlib, 2021. p. 13–18.

- SWAN, M. **Blockchain: Blueprint for a new economy**. [S.I.]: "O'Reilly Media, Inc.", 2015.
- TUCKMAN, B. W. Developmental sequence in small groups. **Psychological bulletin**, American Psychological Association, v. 63, n. 6, p. 384, 1965. Disponível em: <<https://psycnet.apa.org/record/1965-12187-001>>. Acesso em: 27 abr. 2020.
- VAISHNAVI, V.; KUECHLER, B. **Design Research in Information Systems**. Heidelberg: Springer, 2004. 524 p.
- VIANA, C.; BRANDÃO, A.; DIAS, D.; CASTELLANO, G. Blockchain para gerenciamento de prontuários. **Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)**, n. e28, p. 177–187, 2020. Disponível em: <<http://repositorio.unicamp.br/handle/REPOSIP/363161>>. Acesso em: 20 set. 2020.
- VREEDE, G.-J. D.; KOLFSCHOTEN, G. L.; BRIGGS, R. O. Thinklets: a collaboration engineering pattern language. **International Journal of Computer Applications in Technology**, Inderscience Publishers, v. 25, n. 2-3, p. 140–154, 2006. Disponível em: <<https://www.inderscienceonline.com/doi/abs/10.1504/IJCAT.2006.009064>>. Acesso em: 27 abr. 2020.
- WOHLIN, C.; RUNESON, P.; HÖST, M.; OHLSSON, M. C.; REGNELL, B.; WESSLÉN, A. **Experimentation in software engineering**. Boston: Springer Science & Business Media, 2012.
- WONG, M. C.; YEE, K. C.; NØHR, C. Socio-technical considerations for the use of blockchain technology in healthcare. IOS Press, v. 247, p. 636–640, 2018. Disponível em: <<https://pubmed.ncbi.nlm.nih.gov/29678038/>>. Acesso em: 10 maio 2021.
- WÜST, K.; GERVAIS, A. Do you need a blockchain? In: CRYPTO VALLEY CONFERENCE ON BLOCKCHAIN TECHNOLOGY (CVCBT), 2018, Zug, Switzerland. **Anais...** Zug, Switzerland: IEEE, 2018. p. 45–54.
- XIE, J.; YU, F. R.; HUANG, T.; XIE, R.; LIU, J.; LIU, Y. A survey on the scalability of blockchain systems. **IEEE Network**, v. 33, n. 5, p. 166–173, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8823874>>. Acesso em: 29 mai. 2021.
- XIONG, Y.; DU, J. Electronic evidence preservation model based on blockchain. In: **Proceedings of the 3rd International Conference on Cryptography, Security and Privacy**, 3. NY, United States: Association for Computing Machinery, 2019. p. 1–5.
- XU, X.; WEBER, I.; STAPLES, M. Blockchain patterns. In: **Architecture for Blockchain Applications**. [S.I.]: Springer, 2019. p. 113–148.
- YUAN, Y.; WANG, F.-Y. Blockchain and cryptocurrencies: Model, techniques, and applications. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, IEEE, v. 48, n. 9, p. 1421–1428, 2018. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8419306>>. Acesso em: 05 mar. 2021.
- ZHANG, P.; WHITE, J.; SCHMIDT, D. C.; LENZ, G.; ROSENBLoom, S. T. Fhirchain: applying blockchain to securely and scalably share clinical data. **Computational and Structural Biotechnology Journal**, Elsevier, v. 16, p. 267–278, 2018. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S2001037018300370>>. Acesso em: 18 jan. 2020.

ZHANG, R.; GEORGE, A.; KIM, J.; JOHNSON, V.; RAMESH, B. Benefits of blockchain initiatives for value-based care: proposed framework. **Journal of medical Internet research**, v. 21, n. 9, p. e13595, 2019. Disponível em: <<https://www.jmir.org/2019/9/e13595/>>. Acesso em: 11 jun. 2021.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE INTERNATIONAL CONGRESS ON BIG DATA (BIGDATA CONGRESS), 1., 2017 Boston. **Anais...** Boston: IEEE, 2017. p. 557–564.

## APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

### Termo de Consentimento Livre e Esclarecido (TCLE)

#### CONSENTIMENTO INFORMADO

##### 1. Sobre o estudo?

O trabalho envolve o desenvolvimento de um Prontuário Eletrônico do Paciente (PEP) baseado em Blockchain. A presente pesquisa utiliza uma abordagem sociotécnica para seu desenvolvimento e avaliação. Nesta etapa, realizaremos o experimento a fim de avaliar o viés social, visando entender aspectos colaborativos entre diferentes participantes ao utilizar o PEP integrado à novas tecnologias, como blockchain.

##### 2. Quem pode participar?

Pessoas com mais de 18 anos, que demonstre alguma articulação ou envolvimento profissional na área da saúde, ou participante que represente o paciente.

##### 3. O que será solicitado?

Após seu consentimento para participar da pesquisa, pretende-se realizar o experimento a partir de um grupo focal buscando entender os processos atuais do uso de PEP, em seguida, ocorrerá uma observação participante por meio do uso da ferramenta e, posteriormente, outro grupo focal discutindo os aspectos e experiência do uso em questão. O grupo focal será guiado por questões baseadas em conceitos colaborativos e de aceitação da tecnologia.

##### 4. Quais são seus direitos e responsabilidades ao participar do estudo?

A participação nesta pesquisa não implica riscos para você. Sua participação é completamente voluntária e anônima, portanto, não solicitaremos dados pessoais e seu endereço IP não será armazenado.

- Você tem o direito de se recusar a participar.

- Você pode parar a qualquer momento, mesmo depois de dar permissão.

- Você não precisa dar um motivo para abandonar a pesquisa e interromper sua participação não trará nenhuma consequência.

- Se você iniciar, mas encerrar sua participação antes de concluir a pesquisa, todos os seus dados serão descartados para análise.

- Você tem o direito de conhecer os resultados gerais da pesquisa, que será divulgada por meio do projeto que será realizado.

As informações obtidas serão armazenadas em formato eletrônico pelos pesquisadores e somente a equipe de pesquisa terá acesso a esses dados. Os dados serão armazenados eletronicamente em um banco de dados, nos computadores da equipe de pesquisa, sendo esses dados obtidos, processados anonimamente, atribuindo um código pessoal que não permite a identificação do participante.

Garantimos que o tratamento dos seus dados será tão cuidadoso quanto na coleta inicial. Os resultados do estudo serão utilizados apenas para fins científicos, divulgação em conferências e criação de publicações científicas.

##### 5. Remuneração

Você não receberá nenhuma remuneração por participar deste estudo. Nem em caso de evento adverso.

##### 6. Riscos

O único risco associado à participação neste estudo é um pequeno grau de envolvimento emocional ao responder às perguntas. Nesse caso, você pode parar de responder e retomar quando julgar apropriado ou, definitivamente, parar de participar.

##### 7. Gravação da imagem e voz

O procedimento de avaliação que será realizado, estará sendo gravado para que seja possível fazer a análise de usabilidade do sistema proposto. Sua utilização será apenas para fins acadêmicos e não será compartilhado com terceiros sob nenhuma hipótese.

##### 8. Detalhes do contato

Este estudo é realizado pela aluna Pamella Soares de Sousa, do Programa de Pós-Graduação em Ciência da Computação da UECE e orientado pelo Prof. Dr. Jerffeson Teixeira de Souza (UECE).

Se você tiver perguntas ou comentários sobre a pesquisa, envie um e-mail para o endereço de correspondência: [pamella.soares@aluno.uece.br](mailto:pamella.soares@aluno.uece.br).

Se durante a pesquisa você tiver quaisquer comentários ou preocupações relacionadas à condução da pesquisa ou perguntas sobre seus direitos ao participar do estudo, poderá entrar em contato com alguns dos avaliadores.

Agradecemos antecipadamente por participar desta pesquisa,

Você concorda com o termo apresentado? \*

Tenho mais de 18 anos e concordo que meus dados sejam utilizados para os fins desta pesquisa.

## APÊNDICE B – FORMULÁRIO DE CARACTERIZAÇÃO DOS PARTICIPANTES

Dados do Participante	
Preencha os espaços com os dados solicitados	
<b>Nome completo:</b> *	
Sua resposta	
<b>Idade:</b> *	
Sua resposta	
<b>Escolaridade:</b> *	
<input type="radio"/> Médio	
<input type="radio"/> Superior (Graduação)	
<input type="radio"/> Pós-graduação	
<input type="radio"/> Mestrado	
<input type="radio"/> Doutorado	
<b>Área de formação:</b> *	
Sua resposta	
<b>Organização em que trabalha:</b> *	
Sua resposta	
<b>Cargo (atuação profissional):</b> *	
Sua resposta	
Há quanto tempo você atua na área da saúde? (Perfil "Paciente" não precisa responder esta questão)	
Sua resposta	

## APÊNDICE C – CENÁRIO 1 DO EXPERIMENTO SOCIAL

### Cenário 1: Atendimento com a Instituição de Saúde (IS)

O Enfermeiro e o Paciente participam do Cenário 1

**PASSO 1**

[ENFERMEIRO (A)] Realize o login no sistema.

email: [enfermeiro2@gmail.com](mailto:enfermeiro2@gmail.com)

senha: 123enferm

[PACIENTE] Realize o login no sistema.

email: [paciente2@gmail.com](mailto:paciente2@gmail.com)

senha: 123pac

**PASSO 2**

[ENFERMEIRO (A)] Em “Registrar Laudo”, selecione o tipo de registro “Observação” para ser cadastrado.

**PASSO 3**

[ENFERMEIRO (A)] Solicite o nº do CPF do paciente e verifique a identificação.

**PASSO 4**

[ENFERMEIRO (A)] Registre “Observação” fornecendo informações sobre os sinais vitais coletados do paciente digitando informações de “Sinal Vital” e “Valor” do teste. Exemplo:

Sinal Vital	Valor
Pressão	120x70mmHg
Temperatura	38,9 C
FC	115 bpm
SatO2	94%

Fonte: <https://www.sanarmed.com/caso-clinico-de-covid-19>

**PASSO 5**

[ENFERMEIRO (A)] Confirme “Registrar Observação” para registro das informações, aguarde o registro finalizar.

**PASSO 6**

[PACIENTE] Verifique a Observação na lista de “Registros” e realize a leitura do registro armazenado pelo Enfermeiro (a).

*\*Enfermeiro(a), no Cenário 1 - Passo 4, estão os sinais vitais que você poderá digitar na plataforma. Mas, não está delimitado apenas para esses. Você poderá, incrementar ou mudá-los conforme desejar.*

## APÊNDICE D – CENÁRIO 2 DO EXPERIMENTO SOCIAL

### Cenário 2: Atendimento com Profissional da Saúde (PS)

O **Médico (a)** e o **Paciente** participam do Cenário 2

<b>PASSO 1</b> [MÉDICO] Realize o login no sistema. email: <a href="mailto:medico2@gmail.com">medico2@gmail.com</a> senha: 123med
<b>PASSO 2</b> [MÉDICO] Apresente o CPF de identificação para paciente autorizar acesso ao registro “Observação” registrado pelo Enfermeiro(a).
<b>PASSO 3</b> [PACIENTE] Na listagem de Registros, libere acesso aos registros para o médico(a).
<b>PASSO 4</b> [MÉDICO] Verifique na lista o registro “Observação” que foi compartilhado pelo paciente.
<b>PASSO 5</b> [MÉDICO] Em “Registrar Laudo”, selecione o tipo de registro “Anamnese” para ser cadastrado.
<b>PASSO 6</b> [MÉDICO] Solicite o nº do CPF para identificação do paciente.
<b>PASSO 7</b> [MÉDICO] Registre as respostas de todas as questões respondidas pelo paciente para a Anamnese.
<b>PASSO 8</b> [MÉDICO] Confirme “Registrar Anamnese” para o registro das informações.

**Instruções para o perfil Paciente:** No **Cenário 2 - Passo 7** o **Médico** realizará perguntas para Anamnese que serão respondidas pelo perfil **Paciente**. Devido a um importante assunto que vem sendo bastante debatido nos últimos meses, o caso clínico do paciente apresentará sintomas de Covid-19. A seguir, são listadas as perguntas que o médico irá fazer, e sugerimos a resposta de **História Doença Atual** para o paciente responder, mas não está limitada apenas a elas. *Você, paciente, poderá incrementá-las ou mudá-las conforme desejar. Também poderá responder como preferir nas seguintes perguntas, que não precisam ser verídicas.*

#### **História Doença Atual (HDA)**

Qual a principal queixa? R - Dor de cabeça, falta de ar, febre, dor de garganta.

Início dos sintomas e duração da queixa. R - Há sete dias

Localização da dor. R - Cabeça e garganta.

#### **História Patológica Pregressa**

Está em tratamento médico com algum remédio? Tem alguma alergia? Cirurgia recente? Alterações cardíacas (Cardiopatias)? Hipertensão? Diabetes?

## APÊNDICE E – CENÁRIO 3 DO EXPERIMENTO SOCIAL

### Cenário 3: Realização de exames laboratoriais no Laboratório Médico (LM)

O **Biomédico/Farmacêutico** e o **Paciente** participam do Cenário 3

**PASSO 1**

[BIOMÉDICO] Realize o login no sistema.

email: [lab2@gmail.com](mailto:lab2@gmail.com)

senha: 123lab

**PASSO 2**

[BIOMÉDICO] Em “Registrar Laudo”, selecione o tipo de registro “Exame” para ser cadastrado

**PASSO 3**

[BIOMÉDICO] Solicite nº do CPF para identificação do paciente e verifique a identificação

**PASSO 4**

[BIOMÉDICO] Registre “Exame” fornecendo informações sobre os testes realizados no laboratório digitando informações de “Nome” e “Valor” do teste. Exemplo:

Teste	Valor
Hb	12.1
Leucograma	12.300 sem desvio
Plaquetas	156 mil
PO2	82
HCO3	3

Fonte: <https://www.sanarmed.com/caso-clinico-de-covid-19>

**PASSO 5**

[BIOMÉDICO] Confirme “Registrar Exame” para o registro das informações.

**PASSO 6**

[PACIENTE] Realize a leitura do registro armazenado pelo LM

\*Biomédico(a) ou Farmacêutico(a), no **Cenário 3 - Passo 4**, estão os valores de análises clínicas que você irá digitar na plataforma. Mas, não está delimitado apenas para esses. Você poderá, incrementar ou mudá-los conforme desejar.

## APÊNDICE F – CENÁRIO 4 DO EXPERIMENTO SOCIAL

### Cenário 4: Atendimento com Profissional da Saúde (PS)

O **Médico (a)** e o **Paciente** participam do Cenário 4

<b>PASSO 1</b> [MÉDICO] Apresente o CPF de identificação para o paciente autorizar acesso ao “Exame” registrado pelo Biomédico(a).
<b>PASSO 2</b> [PACIENTE] Na listagem de Registros, libere acesso ao registro “Exame” para o médico(a).
<b>PASSO 3</b> [MÉDICO] Verifique na lista o registro “Exame” que foi compartilhado pelo paciente.
<b>PASSO 4</b> [MÉDICO] Selecione o tipo de registro “Medicação” para ser cadastrado.
<b>PASSO 5</b> [MÉDICO] Solicite o nº do CPF para identificação do paciente.
<b>PASSO 6</b> [MÉDICO] Registre medicação e diagnóstico fornecendo as informações necessárias.
<b>PASSO 7</b> [MÉDICO] Confirme “Registrar Medicação” para o registro das informações.
<b>PASSO 8</b> [PACIENTE] Realize a leitura dos registros feitos pelo médico.

\*Médico (a), no **Cenário 4 - Passo 6**, você poderá simular a prescrição de remédios que geralmente são tratados os sintomas de Covid-19.

## APÊNDICE G – QUESTÕES DO GRUPO FOCAL

**1º MOMENTO - GRUPO FOCAL**  
**PERGUNTAS RELACIONADAS AOS PRONTUÁRIOS ATUAIS**  
 Programa de Pós-Graduação em Ciência da Computação  
 Universidade Estadual do Ceará

---

- 1) Como ocorre o processo de comunicação e colaboração entre uma equipe médica por meio de prontuários atuais, tanto em papel como os eletrônicos?
- 2) Como as informações advindas de diferentes partes e organizações são integradas?
- 3) Atualmente, como o paciente gerencia suas informações de saúde emitidas por diferentes entidades?
- 4) Como ocorre o controle de acesso por parte dos pacientes nos prontuários eletrônicos atuais?

**2º MOMENTO - GRUPO FOCAL**  
**PERGUNTAS RELACIONADAS AOS CONSTRUTOS COLABORATIVOS**  
 Programa de Pós-Graduação em Ciência da Computação  
 Universidade Estadual do Ceará

---

### MODELO 4C DE COLABORAÇÃO

- 1) Como a solução proposta poderia aumentar a qualidade em uma investigação colaborativa no que diz respeito ao diagnóstico de um paciente?
- 2) Quais aspectos críticos em relação à comunicação entre os profissionais seria possível mitigar com o uso da solução proposta?
- 3) Quão importante você considera a possibilidade de controle de acesso no compartilhamento e gerenciamento dos seus registros com outros participantes?

### PEP BASEADO EM BLOCKCHAIN

- 4) Como pode-se perceber a questão da privacidade dos dados e controle de acesso pelo paciente através da solução proposta utilizada?
- 5) O que a imutabilidade dos registros médicos uso da blockchain pode garantir em relação à auditoria dos dados informados pelas entidades de saúde?
- 6) O uso de blockchain possibilita a disponibilidade das informações, ou seja, os registros médicos podem ser acessados a qualquer momento. Qual sua percepção sobre essa característica?