UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS DA EDUCAÇÃO
PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Patryck Ramos Martins

Um Modelo de Blockchain para Privacidade dos Dados na Saúde 4.0

Florianópolis
2023

Patryck Ramos Martins

Um Modelo de Blockchain para Privacidade dos Dados na Saúde 4.0

Dissertação submetida ao Programa de Pós Graduação em Ciência da Informação da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Ciência da Informação.

Orientador: Prof. Douglas Dyllon Jeronimo de Macedo, Dr.

Florianópolis
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Martins, Patryck Ramos
Um Modelo de Blockchain para Privacidade dos Dados na Saúde 4.0 / Patryck Ramos Martins ; orientador, Douglas Dyllon Jeronimo de Macedo, 2023.
182 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós Graduação em Ciência da Informação, Florianópolis, 2023.

Inclui referências.

1. Ciência da Informação. 2. Blockchain. 3. Privacidade. 4. Saúde 4.0. 5. BIMHE. I. Macedo, Douglas Dyllon Jeronimo de. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. III. Título.

Patryck Ramos Martins

Um Modelo de Blockchain para Privacidade dos Dados na Saúde 4.0

O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 14 de junho de 2023 por banca examinadora composta pelos seguintes membros:

Prof. Mario Antonio Ribeiro Dantas, Dr.
Universidade Federal de Juiz de Fora

Prof. Moisés Lima Dutra, Dr.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Ciência da Informação.

Documento assinado digitalmente
Edgar Bisset Alvarez
Data: 05/09/2023 06:49:30-0300
CPF: ***.516.228-**
Verifique as assinaturas em https://v.ufsc.br

_____
Prof. Edgar Bisset Alvarez, Dr.
Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Douglas Dyllon Jeronimo de Macedo
Data: 04/09/2023 10:18:01-0300
CPF: ***.987.372-**
Verifique as assinaturas em https://v.ufsc.br

_____
Prof. Douglas Dyllon Jeronimo de Macedo, Dr.
Orientador

Florianópolis, 14 de junho de 2023.

A Deus.
A minha família.

AGRADECIMENTOS

Ao meu orientador, em especial, Professor Dr. Douglas Dyllon Jeronimo de Macedo por acreditar no trabalho, pela confiança, por seu profissionalismo e por toda paciência durante o processo de orientação. Obrigado por compartilhar seus conhecimentos e me acompanhar nesta jornada, aprendi muito. Vamos em frente!

Ao Professor Dr. Moisés Lima Dutra que conheci no PGCIN e desde então admiro por sua generosidade com os alunos e observações sempre pertinentes em todos os trabalhos que juntos realizamos. Obrigado por participar diretamente em minha formação e pela parceria nas correções.

Ao Professor Dr. Mario Antonio Ribeiro Dantas, por seus apontamentos, pelas trocas e exemplos técnicos que muito enobreceram o trabalho.

A todos os Professores do PGCIN, em especial aos Professores: Dr. Edgar Bisset Alvarez, Dr. Adilson Luiz Pinto, Dra. Eliana Maria dos Santos Bahia Jacintho, Dra. Renata Cardozo Padilha, Dr. Gustavo Medeiros de Araújo e Dr. Márcio Matias, pelos ensinamentos, parcerias e conversas.

Aos colegas de classe que partilharam do caminho, em especial ao Edgar, Iuri, Mateus, Luana e Fabiane.

A minha esposa Leila, meus filhos Arthur e Davi, por entenderem a importância desta etapa e perceberem que também era por eles todo este foco e força voltado a mais um projeto acadêmico.

Aos meus pais Carlos e Ivalda, por me incentivarem sempre e por todo o suporte que sempre me proporcionaram. Agradeço também ao meu irmão George pelo apreço de sempre.

Ao Jorge W. Petry Neto pela amizade, por crer e apoiar meus projetos de todas as formas. Muito Obrigado mesmo!

Ao Hallan Medeiros pela ajuda técnica, discussões criteriosas sobre o projeto independente do momento, tudo com muita qualidade. Valeu Amigo.

A Gislaine Parra Freund por me apresentar a possibilidade de um sonho, pelos conselhos, palavras e narrativas de apoio.

Aos Professores do IESGF que ajudaram no processo e suportaram minhas ausências acadêmicas em especial ao Robson Cavalcante, Jorge Sandoval, Charles Alandt, André Leite, Douglas Hiura, Ana Paula, Daniel Krause e Ricardo Espíndola.

“Estamos vivendo mais um dos intervalos da história, onde a característica principal é a transformação da nossa cultura material pelos mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação.”

(Manuel Castells, 2019)

RESUMO

Espaços em saúde buscam na tecnologia apoio estratégico para gestão, assistência ao paciente e tratamento de doenças. O progresso tecnológico é apto para transformar processos operacionais, podendo promover vantagens pontuais e tornar-se decisivo em questões críticas. Cumpre, também, função de integrar serviços desobstruindo adversidades recorrentes nos cenários médicos para prover melhor técnica aos profissionais de saúde no auxílio aos pacientes. Seu caráter indispensável nos ambientes em saúde indicam às organizações encontrar oportunidades em investimento, mantendo e entendendo as tendências em tecnologias para saúde com intuito em servir profissionais e usuários de saúde. Todavia, junto às vantagens tecnológicas existem desafios, quanto aos dados que circulam nos cenários de saúde devido à criticidade. Tais ambientes produzem muitas informações e o compartilhamento e transações entre sistemas computacionais profissionais de saúde e usuários aumentam gradativamente para melhorar a integração e serviços oferecidos. Surgem então propostas com novos métodos que auxiliam organizações a gerir dados sensíveis minimizando problemas com a privacidade. Este trabalho propõe um modelo para compartilhar registros dos pacientes em cenários de saúde a partir da tecnologia Blockchain. Como forma de suportar o desenvolvimento do modelo foi elaborada uma fundamentação teórica sobre os conceitos elementares do Blockchain e conteúdos relacionados, e também uma revisão sistemática de literatura com período de abordagem entre os anos de 2018 a 2023. O modelo, denominado BIMHE, foi criado a partir dos métodos e técnicas existentes para compartilhamento de dados em ambientes de saúde. Ele está proposto, inicialmente, a partir de três visões (Camadas do Modelo, Mapa Estrutural e Barramento de Dados), os quais condicionam a transação dos dados autorizados por pacientes a partir da origem solicitante (profissionais de saúde). Um estudo de caso em um ambiente simulado e controlado foi implementado a partir da plataforma descentralizada Ethereum Ganache, com cenário para validar o modelo. Os resultados experimentais indicaram a possibilidade da troca de informação entre paciente e médico a partir do conceito de troca de chaves e armazenamento no ambiente Blockchain, com dados sendo entregues somente ao solicitante a partir do consentimento do usuário paciente e assim demonstrando a viabilidade da abordagem proposta.

Palavras-chave: Blockchain; Saúde 4.0; Privacidade; BIMHE.

ABSTRACT

Healthcare spaces look to technology for strategic support in management, patient care, and disease treatment. Technological progress is able to transform operational processes, and can promote specific advantages and become decisive in critical issues. It also fulfills the function of integrating services, clearing recurring adversities in medical scenarios to provide better techniques to health professionals in helping patients. Its indispensable character in healthcare environments indicates to organizations to find opportunities in investing, maintaining, and understanding the trends in healthcare technologies in order to serve healthcare professionals and users. However, along with the technological advantages come challenges, as data circulates in healthcare settings due to criticality. Such environments produce a lot of information and the sharing of information and transactions between computer systems, healthcare professionals, and users is gradually increasing in order to improve the integration and services offered. Proposals are then emerging with new methods that help organizations manage sensitive data while minimizing privacy issues. This paper proposes a model for sharing patient records in healthcare settings from Blockchain technology. As a way to support the development of the model, a theoretical foundation on the elementary concepts of Blockchain and related content was elaborated, and also a systematic literature review with an approach period between the years 2018 to 2023. The model, called BIMHE, was created based on existing methods and techniques for sharing data in healthcare environments. It is initially proposed from three views (Model Layers, Structure Map, and Data Bus), which condition the transaction of patient-authorized data from the requesting source (healthcare professionals). A case study in a simulated and controlled environment was implemented from the decentralized Ethereum Ganache platform, with a scenario to validate the model. The experimental results indicated the possibility of information exchange between patient and physician from the concept of key exchange and storage in the Blockchain environment, with data being delivered only to the requester from the consent of the patient user and thus demonstrating the viability of the proposed approach.

Keywords: Blockchain; Health 4.0; Privacy; BIMHE.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

3DES	Triple Data Encryption Standard
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
ABCI	Application Blockchain Interface
ABI	Application Binary Interface
ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AGV	Automated Guided Vehicle
AIDS	Acquired Immunodeficiency Syndrome
AMQP	Advanced Message Queuing Protocol
APPs	Australian Privacy Principles
APPI	Act on the Protection of Personal Information
ASTM-CCR	American Society for Testing and Materials-Continuity of Care Record
AWS	Amazon Web Services
BSL	Blockchain Service Layer
BSSP	Blockchain-Based Secure and Privacy-Preserving
CAST	Carlisle Adams and Stafford Tavares
CB-EHRs	Credible Blockchain-based E-health Record
CI	Ciência da Informação
CLI	Command Line Interface
CorDapps	Corda Distributed Applications
COVID-19	Coronavirus Disease 2019
CPF	Cadastro de Pessoa Física
CPR	Computer-based Patient Record
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
CSV	Comma Separated Values
DApps	Decentralized Applications
dBFT	Delegated Byzantine Fault Tolerance
DC	Data Center
DDoS	Distributed Denial of Service

DES Data Encryption Standard

DID Decentralized Identifier

DLT Distributed Ledger Technology

DIDDO Decentralized Identifier Descriptor Object

DPKI Decentralized Public Key Infrastructure

DPOS Delegated Proof of Stake

EC2 Elastic Compute Cloud

EDI Electronic Data Interchange

EEA Enterprise Ethereum Alliance

EHR Electronic Health Records

EMR Electronic Medical Record

ENANCIB Encontro Nacional de Pesquisa em Ciência da Informação

EPR Electronic Patient Records

ERP Enterprise Resource Planning

EVM Ethereum Virtual Machine

FHIRChain Fast Healthcare Interoperability Resources Chain

GB Gigabyte

GDPR General Data Protection Regulation

GHz Gigahertz

GNU GNU's Not Unix!

GPS Global Positioning System

GT Grupos de Trabalho

GW Gateway

HDD Hard Disk Drive

HIE Health Information Exchange

HIPAA Health Insurance Portability and Accountability Act

HL7 Health Level Seven International

HL7-CDA Health Level Seven International-Clinical Document Architecture

HL7-EHR Health Level Seven International-Electronic Health Records

HSM Hardware Security Module

HTML HyperText Markup Language

HTTP Hypertext Transfer Protocol Secure

IA Inteligência Artificial

IBFT Istanbul Byzantine Fault Tolerant

ID	Identity
IDE	Integrated Development Environment
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronic Engineers
IHR	Individual Health Records
IPFS	Interplanetary File System
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoS	Internet of Service
IoT	Internet of Things
IP	Internet Protocol
iPHR	Intelligent Personal Health Record
JDBC	Java Database Connectivity
JS	JavaScript
JSON	JavaScript Object Notation
LCP	Ledger Consensus Protocol
LGPD	Lei Geral de Proteção de Dados
LIMS	Laboratory Information Management System
MEC	Mobile Edge Computing
MS	Microsoft
MSP	Membership Service Provider
ONC	Office of the National Coordinator
P2P	Peer-to-Peer
PBFTP	Plenum Byzantine Fault Tolerant Protocol
PDA	Personal Digital Assistants
PEP	Prontuário Eletrônico do Paciente
PIPEDA	Personal Information Protection and Electronic Documents Act
PHA	Patient Health Application
PHI	Private Health Information
PHIS	Personal Health Information System
PHM	Private Health Management
PHR	Personal Health Record
PKI	Public Key Infrastructure
PMR	Patient Medical Records

PoA	Proof of Authority
PoC	Proof of Conformance
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
PRMS	Patient's E-Healthcare Records Management System
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RC2	Rivest Cipher
RES	Registro Eletrônico em Saúde
RFID	Radio Frequency Identification
RME	Registro Médico Eletrônico
RPC	Remote Procedure Call
RPCA	Ripple Protocol Consensus Algorithm
RPM	Remote Patient Monitoring
RSA	Rivest-Shamir-Adleman
RSL	Revisão Sistemática da Literatura
SMS	Short Message Service
SO	Sistema Operacional
SOM	Service Oriented Middleware
SPV	Simplified Payment Verification
SSD	Solid State Drive
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLS	Transport Layer Security
TM	Trademark
UHR	Universal Health Record
UNL	Unique Node List
XML	eXtensible Markup Language
W3C	World Wide Web Consortium
YAC	Yet Another Consensus

SUMÁRIO

1 INTRODUÇÃO

Ações hostis em ambientes computacionais sempre são uma preocupação para quem é o alvo ou usufrui dos serviços providos que necessitam de aspectos mínimos de segurança implementados. Agentes ameaçadores estão em constante desenvolvimento colocando em risco os ativos de informação das organizações. Diante dos diversos cenários críticos impostos, tecnologias, produtos ou serviços que provocam uma ruptura nos padrões existentes, promovem possibilidades antes pouco exploradas viabilizando novas formas de entender os ambientes computacionais e os negócios por estes suportados.

A temática deste trabalho é promover o uso da tecnologia Blockchain aplicado a cenários do ramo da saúde, com a preocupação em garantir a privacidade nas transações das informações dos pacientes. A Blockchain pode ser definida como uma estrutura de dados distribuída, sem uma entidade central reguladora e constituído por registros de informações formatados em um encadeamento de blocos conectados uns aos outros utilizando mecanismos criptográficos, que são empregues para certificar a sequência dos blocos e prevenir manipulações (Chervinski; Kreutz, 2019; Lauslahti; Mattila; Seppala, 2017; Crosby *et al*., 2016; Government Office for Science, 2016). A descentralização da tecnologia Blockchain minimiza ações hostis contra modificações dos blocos sequenciais armazenados, pois alterações indevidas deveriam ser realizadas em todas as cópias distribuídas (Chervinski; Kreutz, 2019). Esta tecnologia pode ser empregada em cenários distintos, além do ramo da saúde especificado neste trabalho, tais como para suportar ambientes de eleições, gestão de documentos e cadeia de suprimentos (Crosby *et al*., 2016).

A Blockchain, é indicada para cenários com sistemas interoperáveis, auditáveis e seguros (Crosby *et al*., 2016; Swan, 2015). Comparando com sistemas tradicionais de armazenamento de dados, a tecnologia Blockchain institui um conjunto de benefícios para minimizar riscos na gestão de informações sensíveis na área de saúde. A Blockchain faz parte de uma nova gama de tecnologias, Efanov e Roschin (2018) e Crosby *et al*. (2016), explicam que o modelo tecnológico distribuído existente na tecnologia Blockchain é baseado na capacidade dos recursos em comunidades compartilhadas. Os atuais avanços tecnológicos se estendem aos cuidados de saúde, o que conduz a chamada revolução da Saúde 4.0 (*Health* 4.0). Bause *et al.* (2019) explica a existência de um novo paradigma para beneficiar pacientes e médicos, que melhora o acolhimento e vínculo e qualidade da informação. Em ambientes de saúde, tecnologias capacitam e proporcionam valor ao paciente e orientam os profissionais de saúde e organizações. Os benefícios com a aplicação dos conceitos da Saúde 4.0 são inúmeros

e habilitam, por exemplo, o paciente a acessar os registros pessoais de saúde, possibilitando gerenciar a informação e liberar o que considera ideal em cada situação. Logo, disponibilizar o dado se torna uma atividade atrelada ao paciente e com os conceitos existentes na Saúde 4.0, a estratégia é melhorar os serviços de saúde, e a conectividade entre as partes interessadas nos cuidados de saúde usando a tecnologia (Bause *et al.*, 2019).

No estudo de Zhang *et al*. (2018b) são expostas algumas fragilidades dos sistemas de saúde, como a problemática da gerência e manutenção dos dados. Estes dados por muitas vezes são tratados como registros isolados e fragmentados, as comunicações entre os sistemas são atrasadas para dispor as informações e as ferramentas de fluxo de trabalho se caracterizam por falta de interoperabilidade. Neste contexto, o Blockchain oferece a oportunidade de permitir o acesso a registros médicos, com o adicional da detecção de adulteração, como uma das possibilidades de contribuições do Blockchain na temática saúde, chamando atenção, para este projeto de pesquisa o compartilhamento seguro de dados detalhado por (Zhang *et al*., 2018a).

Para prover informações é preciso respeitar o detentor dos dados em um processo burocrático de abordagens tecnológica e jurídica. Conforme Ribeiro e Canedo (2020) a proteção de dados pessoais é um problema tratado por diversos países com criação de leis e regulamentos para proteger os direitos fundamentais e a privacidade. As leis mais rígidas existentes para este propósito, são da União Europeia, a *General Data Protection Regulation* (GDPR), a lei sobre Proteção de Informações Pessoais (APPI) do Japão, *Australian Privacy Principles* (APPs), Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) e leis dos Estados Unidos, incluindo a Privacidade do Consumidor da Califórnia Lei de 2018 (CCPA). No Brasil existe a Lei Geral de Proteção de Dados (LGPD), baseada na GDPR (Ribeiro; Canedo, 2020).

Todas estas leis possuem num dos fundamentos o respeito à privacidade e determina o dado pessoal como toda informação associada à pessoa natural identificada ou identificável, ou seja, elementos possíveis para identificar um indivíduo, tal qual o nome, número do Cadastro de Pessoa Física (CPF), número do telefone ou endereço (Doneda; Mendes, 2013). Além do dado pessoal, uma tipificação especial chamada dados pessoais sensíveis são também críticas e protegidas por lei, pois podem lesar o proprietário da informação, tais quais dados sobre saúde.

Nos Estados Unidos, por exemplo, a Lei de Responsabilidade e Portabilidade de Seguro Saúde (HIPAA - *Health Insurance Portability and Accountability Act*), que possui a base para regulamentações federais discorre sobre dados sensíveis em saúde, abordando informações relacionadas a condições físicas ou mentais passadas, presentes ou futuras de um

indivíduo considerando estas informações de saúde, protegidas (Drolet *et al.*, 2017; Doneda; Mendes, 2013).

Esforços medidos para comportar a melhor maneira em dispor dados remetem ao conceito da Saúde 4.0. Conforme Al-jaroodi, Mohamed e Abukhousa (2020), estes novos conceitos tecnológicos na área de saúde ajudam a coletar e gerir dados, melhorando o detalhamento de informações, aprimorando compartilhamento e colaboração dos diferentes serviços de saúde, com relação a recursos e dados de pacientes. Outra condição alcançada é a possibilidade de limitar e ter controle na proteção dos dados do paciente, entre entidades na troca de informações sigilosas. Centrar os serviços com a preocupação na privacidade do paciente é afirmado por Ćwiklicki, Klich e Chen (2020) como emergente e que retém atenção de diversas autoridades de saúde. A fusão de vários elementos tecnológicos é propícia para administrar a quantidade de dados gerada diariamente e este trabalho irá abordar uma destas tecnologias, a Blockchain, na área da saúde com intenção de garantir a privacidade dos dados.

1.1 PROBLEMA DE PESQUISA

O problema que este trabalho busca auxiliar na resolução são as hostilidades e vulnerabilidades quanto aos dados pessoais sensíveis quando compartilhados em sistemas e ambientes na saúde. Esta adversidade é contemplada por autores, (Ćwiklicki; Klich; Chen, 2020; Coutinho *et al.*, 2020; Yassein *et al.*, 2019; Chanchaichujit *et al.*, 2019; Qadri *et al.*, 2020; Kordestani; Barkaoui; Al-Zahran, 2020; World Health Organization, 2011; Agência Nacional de Saúde Suplementar, 2019; Istepanian; Woodward, 2003). A preocupação quanto ao dado do paciente é refletida em exemplos, que indicam a utilização de tecnologias para prover e disseminar informações, mas ao mesmo tempo existe uma temeridade quanto a interconexão de ambientes e falta de capacidade dos usuários em saber como compartilhar dados com menos ameaças atreladas.

A utilização de tecnologias junto ao setor da saúde é crescente, porém, também são colocadas questões importantes quanto à garantia da transmissão e armazenamento dos dados (Jalali; Landman; Gordon, 2020). Considera-se que ambientes de saúde possuem a incumbência em suportar dados pessoais, considerados sensíveis, neste sentido, garantir a melhor ação no acesso a tais informações é uma das preferências nestes cenários (Hathaliya; Tanwar, 2020). Barrows e Clayton (1996), atentam sobre a obrigatoriedade em garantir o acesso aos dados pessoais obtidos no decorre de processos médicos, isto deve ser possível somente a quem tem

permissão de acesso e necessidade de visualização das informações, considerando danos financeiros, sociais e psicológicos que a exteriorização dos dados deve causar aos pacientes.

Existem exemplos que ilustram as preocupações dos autores, como as receitas médicas, pertencentes ao prontuário do paciente e elaboradas com dados sensíveis, estas detêm referências à saúde do paciente, possibilidades de tratamento e prescrição médica, além dos dados pessoais, como nome, números de documentos, endereço e histórico do paciente. De forma complementar a Agência Nacional de Saúde Suplementar (2020) atenta para preocupações maiores no acesso incorreto aos dados, como no caso de medicamentos prescritos para auxiliar no tratamento de doenças estigmatizantes (AIDS, tuberculose, hanseníase) que colocam os enfermos como abomináveis na sociedade.

É importante abordar que as organizações detentoras de dados sensíveis devem se preocupar com a privacidade do paciente, por também estarem sujeitas a perdas monetárias já que mantém a posse das informações. Isto é colocado no Art. 52 da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados), onde preconiza penas administrativas quando acontecer infração as regras mencionadas, como o impedimento de uso dos dados e até remoção destes da base de informações, com interrupção das atividades de tratamento desses dados ou multa limitada a R$ 50 milhões, por transgressão realizada (Brasil, 2018).

Com a pandemia da COVID-19 muitos processos de informatização nos ambientes de saúde foram antecipados, tais como a Telemedicina, em especial devido a incapacidade de acessar os serviços de saúde tradicionais sob ameaça de contaminação, além disso o incremento de transações pessoais em ambientes de saúde acelaram as preocupações com a privacidade dos dados (Jalali; Landman; Gordon, 2020).

Como condição determinante para conter o problema exposto, as tecnologias caracterizadas na qualidade de Saúde 4.0 possuem papel fundamental. Ao mesmo tempo que geram dados a partir dos inúmeros sistemas de monitoramento e coleta (IoT, dispositivos vestíveis) no auxílio a interação com os pacientes, também precisam ser empregadas para aproveitar de uma maneira adequada as informações geradas. Neste sentido foi empregado o uso da Blockchain para minimizar erros de gestão nos dados sensíveis dos pacientes, junto a conceitos criptográficos para compartilhamento de informação.

1.1.1 Pergunta de Pesquisa

Sob a composição dos cenários atuais de saúde e compartilhamento de dados dos usuários com o interesse em segurança destas informações, este trabalho busca responder a seguinte questão de pesquisa:

- Como a partir da tecnologia Blockchain é possível auxiliar na privacidade dos dados em sistemas de Saúde 4.0?

1.2 OBJETIVOS

Nas seções que seguem estão descritos o objetivo geral e os objetivos específicos deste trabalho.

1.2.1 Objetivo Geral

Propor um modelo utilizando Blockchain que possibilite o aumento na privacidade dos dados no escopo da Saúde 4.0.

1.2.2 Objetivos Específicos

Na intenção de atingir o objetivo geral foram estabelecidos os seguintes objetivos específicos:

- Identificar os métodos de Blockchain em sistemas de Saúde 4.0;
- Elaborar um modelo conceitual com a inclusão do conceito de privacidade para que o paciente estabeleça permissões de acesso sobre o seu próprio dado sensível;
- Desenvolver um estudo de caso prático, com um protótipo usando ambiente Blockchain e métodos criptográficos, aplicado ao modelo;
- Avaliar o modelo proposto em um ambiente simulado e controlado.

1.3 MOTIVAÇÃO E JUSTIFICATIVA

O compartilhamento de dados tornou-se importante para quase todos os campos da vida (Al-Zahrani, 2020). Nunca se trocou tanta informação nesta nossa sociedade que vive em

rede (Giardelli, 2012). Ainda há muitos desafios a serem enfrentados para responder adequadamente aos riscos decorrentes do processamento de dados em uma sociedade em rede (Doneda; Mendes, 2013). Pesquisas indicam preocupações com o compartilhamento de dados, e as possíveis informações sensíveis dos proprietários destes dados que podem ser consumidas de maneira indevida e sem autorização, sendo tratadas muitas vezes como mercadoria (Liu *et al.*, 2015; Lu *et al*, 2020; Bernabe *et al.*, 2019; Chang *et al.*, 2018). As tecnologias ao colocarem benefícios para os usuários, também podem implicar em uma série de violações, que conduz a prejuízos financeiros e moral, por exemplo.

Em especial, dados em saúde, temática deste trabalho, são informações que precisam de atenção com relação ao quesito privacidade, devido ao volume excessivo de transações existentes, ao sigilo que por muitas vezes é necessário ter e as dificuldades em encontrar mecanismos de segurança no compartilhamento de informações em saúde (Akbar; Bhawiyuga; Siregar, 2021; Huang; Kandula; Wang, 2021; Silva; Aquino Junior; Melo, 2019). É bom ressaltar que as informações em saúde são confidenciais e protegidas por lei, portanto, deve-se tomar cuidado sempre que tais informações forem comunicadas ou transmitidas, devido ao conjunto de informações inesgotáveis e as interações entre provedores de serviço em saúde e paciente (Drolet *et al*., 2017). Ao encontro disso, no Brasil em 2020 de maneira explicita, a partir do Decreto n.º 10.332 ficou instituída pelo governo federal a chamada Estratégia de Governo Digital, no qual tem por objetivo, disponibilizar ambientes interoperáveis a partir de soluções tecnológicas na administração pública federal direta, autárquica e fundacional, até 2022 (Brasil, 2020). Nesta lei existe a consideração sobre tecnologias para oferecer, por exemplo, conjuntos de dados por meio de soluções de Blockchain, assim como, preocupações na identificação confiável do dado e uso de algoritmos seguros.

O setor de saúde possui prognósticos animadores com relação a investimento e atenção da sociedade em geral. Por Mohamed e Abdellatif (2019) até 2021 o mercado de saúde alcançaria $136,8 bilhões de investimento em todo o mundo, outra informação relevante oriunda dos Estados Unidos é o gasto de $300 bilhões anualmente em inovação médica. Em Epiphaniou, Daly e Al-Khateeb (2019) fica claro que as iniciativas sempre existiram e se tornam mais específicas com o avanço da tecnologia. Várias iniciativas anteriores impulsionaram o investimento em tecnologia de saúde e somente nos Estados Unidos, as estimativas da economia resultante de uma melhor gestão de dados de saúde chegam a $81 bilhões anualmente e mais de $19 bilhões alocados para a modernização dos sistemas de saúde.

O investimento anterior em sistemas de dados de saúde pode ser um facilitador ou um obstáculo para a adoção de avanços na área de saúde. O investimento em tecnologia só terá sucesso se existir um alinhamento com os processos clínicos e existir aceitação dos usuários finais (Chanchaichujit *et al.*, 2019). Surgem apreensões com a utilização de tecnologia e apesar do investimento em saúde, novas preocupações são relatadas por Lee, Kim e Kim (2019), Bhuiyan *et al.* (2018), no qual indicam também avanços das tecnologias, mas atrelado a explosão de dados em saúde.

Conforme Lee, Kim e Kim (2019) junto ao aumento de informações dispostas existe o problema de compartilhamento de dados que apresenta desafios principalmente pela falta de confiabilidade no sistema de compartilhamento e também a variedade dos formatos de dados, ou seja, os dados não são interoperáveis entre as instituições de saúde. O relato sobre problemas ratifica as preocupações e a constatação por números, endossa o momento de atenção. Como exemplo, em 2015 nos Estados Unidos, mais de 112 milhões de registros médicos vazaram gerando $6,2 bilhões em prejuízo. Na Coreia do Sul também houve incidente em 2018, ocasionando $720.000 em fraude de seguro com a falsificação de documentos médicos. Segundo Bhuiyan *et al*. (2018) tanto o setor privado quanto o público estão lidando com os desafios da segurança de dados e muitas empresas relatam hostilidades contra dados de pacientes.

Hostilidades que buscam se beneficiar financeiramente com a posse de registros médicos de forma ilegal estão crescendo, tais registros médicos podem ser vendidos a fornecedores terceirizados que têm interesse em identificar as condições dos indivíduos ou o potencial de desenvolvê-los no futuro (Epiphaniou; Daly; Al-Khateeb, 2019). As diversas problemáticas dos ambientes de saúde e propostas para solucioná-los sempre existiram e neste trabalho será explorado o conceito da privacidade junto aos dados sensíveis dos pacientes. Para isso, é respeitado o surgimento da temática Saúde 4.0, observando as questões tecnológicas conduzidas deste propósito e as tendências de implantação.

Chanchaichujit *et al.* (2019) comenta que está ocorrendo nos ambientes de saúde o surgimento da Saúde 4.0, ou seja, alguns dos princípios da Indústria 4.0 como a integração de tecnologias com o IoT para coleta de dados, o uso de IA para análise e a Blockchain ao tratar registros médicos de pacientes. A intenção com a Saúde 4.0 é proporcionar ações para que as pessoas tomem decisões mais informadas e incentivar a prevenção proativa. O novo momento tecnológico traz questões específicas antes não geridas, como afirma Epiphaniou, Daly e Al-khateeb (2019) sobre a privacidade, no qual os sistemas existentes devem reconhecer que nem

todos os ambientes de saúde e profissionais de saúde devem ter acesso a todo o conjunto de dados dos pacientes.

Este trabalho irá utilizar a Blockchain como tecnologia proposta para melhor governar os dados sensíveis dos pacientes e regular as transações efetuadas com estes a partir do consentimento dos proprietários das informações. A tecnologia Blockchain a partir da estrutura padrão de funcionamento, vem sendo implantada em áreas preocupadas com o sigilo das informações, Lee, Kim e Kim (2019) percebem a tecnologia Blockchain como usada para melhorar a confiabilidade dos dados compartilhados. Desde a sua proposição a tecnologia Blockhain mostrou perspectivas de aplicações promissoras e atraiu atenções em diversos setores da sociedade sendo aplicado em muitos campos, incluindo a área médica (Hongwei; Xinhui; Sanyang, 2004; Yue *et al.*, 2016; Azaria *et al.*, 2016; Li *et al.*, 2020).

Loizou, Karastoyanova e Schizas (2019) reportam com base em desenvolvimentos recentes, várias aplicações construídas em torno da Blockchain na saúde para estabelecer o uso seguro dos dados do paciente. Os vários aplicativos que são usados atualmente no gerenciamento de dados de pacientes estão agora sendo reestruturados para implementar o compartilhamento e armazenamento de dados usando a tecnologia Blockchain. Da mesma forma, novas iniciativas de pesquisa são necessárias com o objetivo de melhorar a usabilidade da privacidade e o controle de privacidade, tornando as implantações de blockchains totalmente em conformidade com os regulamentos de privacidade (Bernabe *et al*., 2019).

A Blockchain está trazendo várias oportunidades para novos aplicativos relacionados à saúde. Vários domínios, como compartilhamento de dados de pacientes e segurança de dados, têm prioridade na prevenção do uso ilegal de informações por várias partes (Loizou; Karastoyanova; Schizas, 2019). Por Bhuiyan *et al.* (2018) o trunfo da tecnologia Blockchain é organizar os dados de forma que as transações possam ser verificadas e registradas enquanto se obtém o consenso de todas as partes envolvidas, cada participante é conhecido com antecedência e já foi pré-aprovado, controlando assim quem pode acessar e modificar os dados sensíveis.

1.4 DELIMITAÇÃO DO ESCOPO

O enquadramento deste trabalho o delimita na linha de pesquisa: Dados, Inteligência e Tecnologia, na área da Ciência da Informação. O trabalho traça uma abordagem direcionada à privacidade de dados em ambientes de saúde que possuem tecnologias provenientes do

contexto 4.0, por meio de um modelo para entendimento do fluxo dos processos relativos à interação entre profissional da saúde, estabelecimento de saúde e paciente.

Esta pesquisa não explora aspectos sobre a disponibilidade de infraestrutura e integridade de sistemas computacionais existentes em ambientes de saúde. O modelo criado não é preparado para ser utilizado de forma genérica como base por sistemas informatizados ou sistemas *web* que queriam integrar suas transações com ambientes Blockchain.

Desta maneira o escopo é definido em explicar a proposta do modelo, aplicando este em um ambiente controlado, se limitando as características e recursos do ambiente. É válido ressaltar que como produto deste trabalho se espera o modelo concebido e um cenário estabelecido com os propósitos dispostos no modelo e apontados neste trabalho. Portanto é esperado uma contribuição à área da saúde ofertando um modelo que respeite o proprietário da informação, não inviabilize o compartilhamento dos dados e automatize a interação entre médico e paciente.

1.5 CONTRIBUIÇÕES

As deliberações e resultados deste trabalho colaboram para a base de experimentos com a tecnologia Blockchain frente aos desafios de novas pesquisas e implantações em Saúde 4.0 preocupadas com a privacidade dos pacientes. Deste modo vale ressaltar as oportunidades que surgem a partir das contribuições deste trabalho. A principal contribuição científica é a elaboração do modelo. O modelo define visões (serviço, conceitual, lógica) que propõe de uma forma geral o dado compartilhado com o objetivo de oferecer este apenas para quem tem o direito de acessá-lo.

A 1ª visão (camadas do modelo – visão de serviços) contribui para expor os princípios e serviços que caracterizam as abstrações das dependências entre as entidades e a forma como o dado é produzido até ser consumido. A 2ª visão (mapa estrutural – visão conceitual) é válida para direcionar as entidades (paciente, médico e organização) e os possíveis acessos que estas têm, colaborando com a identificação mais abrangente dos papéis de cada usuário. Já a 3ª visão (Barramento de Dados – visão lógica) apresenta as interações sequencialmente corretas entre solicitantes e proprietários dos dados no compartilhamento de informações. Estas visões contempladas no modelo mostram uma alternativa para pesquisadores utilizarem como comparação em estudos com a tecnologia Blockchain em referência ao conceito de privacidade perante cenários em saúde. Além disso, uma Revisão Sistemática da Literatura foi realizada e

como resultante foram identificados, interpretados e avaliados documentos relevantes ao problema a ser trabalhado nesta pesquisa, correlacionando Blockchain, Saúde 4.0 e Privacidade.

Como contribuição social este trabalho tem o potencial em agregar aos indivíduos que utilizam serviços em saúde um método para implementar o conceito de privacidade a partir do compartilhamento de informações no setor da saúde. A avaliação por meio de um estudo de caso em um ambiente simulado e controlado que foi realizado neste trabalho possibilitou analogias em cenários reais e entende-se que operacionalizado em um ambiente com recursos humanos capacitados pode servir de base para efetuar análises para melhor aplicar o conceito de privacidade no compartilhamento de informações. Com isso como premissa da Saúde 4.0, com a aplicação do modelo, seria possível fornecer mais um serviço ao paciente facilitando o entendimento do que é compartilhado e melhorando a transparência das transações no sentido de estabelecer um melhor controle dos dados acessados.

Quanto às contribuições tecnológicas deste trabalho é válido citar mais uma proposta na utilização da tecnologia Blockchain em ambientes de saúde, voltado especificamente ao acesso controlado a dados e considerar o cenário que será estabelecido para avaliar o modelo criado, colocando ferramentas computacionais como elementares no processo dos testes com o modelo. Os experimentos no estudo de caso envolvendo tecnologias para construção de ambientes Blockchain, monitorando e coletando registros das interações mostram um bom início de testes para o entendimento de realmente buscar, se estas são as tecnologias ideais no processo. Todos as etapas práticas realizadas para criação do estudo de caso, como os mecanismos para realização das interações entre as entidades paciente, médico e organização, as configurações realizadas na arquitetura de rede e de *hosts*, assim bem como as trocas na rede Blockchain, até a captura dos registros solicitados são elucidativas para compreender a maturidade das tecnologias perante o problema enfrentado. Outro processo que contribui é o formato da rede Blockchain, este foi utilizado inicialmente de maneira padrão (rede pública) para avaliação das interações e das posições ideais para aplicar o conceito de privacidade.

1.6 ALINHAMENTO DO TEMA A ÁREA DE CIÊNCIA DA INFORMAÇÃO

A Ciência da Informação (CI) por Borko (1968) é a disciplina que investiga as propriedades e o comportamento informacional, além disso, determina as forças que governam os fluxos de informação visando a acessibilidade e a usabilidade ótima, também se preocupando com as técnicas aplicadas aos computadores e sistemas de programação.

Como afirma Mikhailov, Chernyi e Gilyarevsky (1969) com a crise da informação no final da década de 1950 foi mandatório perceber o momento e ter o armazenamento, organização e recuperação de dados amparando o pesquisador. Na crise da informação houve a atenção em descobrir a origem da explosão informacional e como se comportar a partir deste aspecto. Com as evoluções tecnológicas, existiu desarmonia na evolução, atrapalhando o elo da informação e suportes para registro e consumo com base nas tecnologias (Souza; Almeida; Baracho, 2013).

Por Taylor (1966) a CI analisa os atributos e o comportamento da informação, desde os fluxos informacionais, gestão e tratamento da informação, melhorando o acesso e benefício. Em Souza, Almeida e Baracho (2013) é alertado sobre a necessidade da CI diante de imensas massas de dados, buscando novas e inovadoras soluções. Verifica-se então a preocupação dos autores em como melhor utilizar os dados produzidos e aproveitar estes, a partir de inúmeras proposições.

A tecnologia da informação é aliada da CI, como explanado por Saracevic (1996, p. 42), "(...) a CI está inexoravelmente ligada à tecnologia da informação.". Por Saracevic (1996), a Ciência da Informação possui fundamentalmente valores atrelados com a Ciência da Computação em vários aspectos. Seja no desenvolvimento de algoritmos, transferência de informação, produtos, serviços, transformações da informação, entre várias vertentes que estabelecem parâmetros complementares, mas não competitivos. As relações cada vez mais evoluem adaptabilidade dos processos em comum, sendo que uma Ciência projeta a outra resolvendo problemas e ajudando mutuamente. A Ciência da Informação trata das tecnologias e serviços relacionados que facilitam seu gerenciamento e uso (Saracevic, 2009).

Entendendo a privacidade como um dos campos de estudo da Ciência da Informação, conforme Lévy (1996, 1999); Mcgarry (1999); Grisoto, Sant’ana e Santarem Segundo (2015), considerando a Blockchain como uma tecnologia para suportar dados e complementarmente se apoiando no alinhamento dos autores supracitados, este trabalho possui aderência ao Programa de Pós-Graduação em Ciência da Informação. Estabelece também relação com o Encontro Nacional de Pesquisa em Ciência da Informação (ENANCIB), a partir de dois grupos de trabalhos, sendo o GT (Grupos de Trabalho) 08 referenciado como “Informação e Tecnologia” e o GT 11 “Informação & Saúde”.

1.7 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em 6 capítulos, sendo este a Introdução. O próximo capítulo é indicada a revisão bibliográfica necessária para a base teórica da pesquisa, apresentando conceitos fundamentais para este trabalho como Saúde 4.0 e o escopo sobre a tecnologia Blockchain. No terceiro capítulo os aspectos metodológicos são postos, caracterizando o trabalho e detalhando as fases de planejamento, além disso, é apresentada a Revisão Sistemática da Literatura contemplando a fase de entendimento dos métodos encontrados a partir da tecnologia Blockchain.

Na sequência é proposto o modelo, denominado BIMHE, para gerenciar a privacidade em ambientes de saúde, com as interações previstas. No capítulo 5 foi apresentado o estudo de caso para esta pesquisa, com a arquitetura do projeto, tecnologias utilizadas, os documentos necessários para entender as interações do projeto e a aplicação do modelo criado. O capítulo 6 descreve as considerações finais do projeto e as experiências adquiridas com a execução e análises do modelo proposto.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo é apresentada a fundamentação teórica sobre os assuntos relacionados a esta pesquisa. A primeira seção contextualiza a temática Saúde especificando os principais conceitos para guiar os propósitos de análise, especificações e desenvolvimento proposto. Após isso foram abordados os aspectos computacionais do projeto, apresentando os conceitos elementares para o emprego do compartilhamento de dados. Seguindo foi descrito a tecnologia Blockchain, contextualizando e indicando as principais abordagens que estão sendo utilizadas.

2.1 TECNOLOGIAS PARA SAÚDE

No sentido de trazer clareza, são abordados como que estudos denominam os termos elementares que surgem a partir da união entre saúde e tecnologia. Istepanian e Woodward (2017) discorre que é imperativo esclarecer algumas diferentes terminologias usadas para o domínio de saúde, quando se refere à tecnologia. Nesta perspectiva Istepanian e Woodward (2017), demonstram a importância de definir, teleconsulta, telemedicina, telessaúde, *e-healt* e *m-health*.

Teleconsulta é um segmento da Telemedicina que provê comunicação eletrônica entre os profissionais médicos a operadora de saúde (centros de saúde) e o paciente em áreas remotas, no qual não estão em condições de fazer viagem até o local de tratamento (Perez-Noboa *et al*., 2021; Ramli; Ali, 2018; Saechow *et al*., 2014). Kordestani, Barkaoui e Zahran (2020) complementam que o tratamento remoto traz custos reduzidos e se torna mais saudável em comparação com as consultas presenciais, devido à existência de possíveis contaminações em ambientes públicos. Saechow *et al*. (2014) explica a Teleconsulta tipificada em: síncrona, ou seja, atendimento em tempo real e assíncrona, acompanhamento dos dados de exames e monitoramento. Ramli e Ali (2018) completa que o propósito é entregar especialidades médicas em locais longínquos e aperfeiçoar o conhecimento em saúde das operadoras de saúde e profissionais. Este conhecimento produzido é gerado na busca, troca, construção e armazenamento de perícia médica, os aconselhamentos, ou segundas opiniões são outras possibilidades ao utilizar Teleconsulta (Ramli; Ali, 2018). Perez-Noboa *et al*. (2021) coloca que a Teleconsulta é muito eficaz em posicionamentos sobre, quando se precisa de um maior números de especialistas e filtragem e análise de sintomas de quais pacientes precisam se deslocar a um centro de saúde.

Telemedicina é, conforme Mohamed e Abdellatif (2019); Istepanian e Woodward (2017); Chandwani e Kumar (2018) um conceito para definir serviços médicos prestados por meio de Tecnologia da Informação e Telecomunicações. Chandwani e Kumar (2018) completam que a Telemedicina traz a entrega remota de serviços relacionados à saúde por meio da transferência de áudio, vídeo e informações gráficas por meio das TICs (Tecnologia da Informação e Comunicação), com diagnóstico e consultas. Por Mohamed e Abdellatif (2019) a Telemedicina pode ter tipificações no uso, tal como: para receber apontamentos médicos por intermédio das plataformas de mensagens, marcação de consultas e detecção por sensores especiais de anomalias no corpo do paciente. Istepanian e Woodward (2017) destacam que Telemedicina é um termo guarda-chuva, designando uma vasta gama de objetos e com diferentes significados, como, por exemplo, a utilização de tecnologia da informação moderna, especialmente comunicações audiovisuais interativas para relacionamento entre médico e paciente em locais distintos, o diagnóstico médico e atendimento ao paciente, prestação de serviços a locais distantes da origem, serviços de largura de banda e telefonia.

A Telessaúde amplia o escopo de atuação da Telemedicina incluindo áreas de atuação para saúde pública, educação em saúde, serviços de saúde, saúde ambiental, saúde industrial, entre outros (Istepanian; Woodward, 2017; Narva *et al*., 2017). Ishani *et al*. (2016) considera a Telessaúde uma estratégia para melhorar e gerenciar o atendimento aos pacientes com doenças crônicas (doenças pulmonares, doenças cardíacas, obesidade, depressão e diabetes são exemplos), independente de localização, com benefícios em áreas remotas que são escassas em cuidados de subespecialidade. Kordestani, Barkaoui e Zahran (2020); Yassein *et al*. (2019), Narva *et al*. (2017); Istepanian e Woodward (2017); Ishani *et al*. (2016) referem que um dos principais benefícios que a Telessaúde oferece é minimizar o custo das consultas de rotina ao médico, com monitoramento remoto por profissionais de saúde dos dados fisiológicos de um paciente para diagnóstico e gerenciamento de doenças. Yassein *et al*. (2019) coloca que a Telessaúde lida com todos os casos e problemas de saúde por meio de diferentes tipos de tecnologias e a principal interação é entre o paciente e o médico.

O termo *e-health* é definido por Coutinho *et al*. (2020); Mukhiya *et al*. (2019); Lai (2016); Kirtava *et al*. (2016); Matsumoto, Ogawa e Tsuji (2016) como o uso de tecnologias de informação e comunicação para a área da saúde, abrangendo uma gama de serviços, incluindo, sistemas de informação de gestão de saúde, prontuários médicos e de saúde eletrônicos (*e-registries*), Telemedicina, *e-learning*, gestão de conhecimento em saúde e também *m-health*. Coutinho *et al*. (2020) resumem que o *e-health* é um conjunto de soluções tecnológicas em

saúde apoiada na Internet para prover serviços. Lai (2016) completa que *e-health* significa usar o poder da tecnologia da informação para melhorar os serviços de saúde pública, podendo acontecer por meio da capacitação e treinamento dos profissionais de saúde. Mukhiya *et al*. (2019); Liu *et al*. (2015) abordam um requisito muito comum para aplicativos de *e-health*, a troca de informações entre os sistemas de saúde e o suporte aos pacientes enquanto estes ficam em casa. Liu *et al*. (2015) colocam a universalização dos dados como importante fator ao ser utilizado o *e-health*.

O conceito de *m-health* surge em 2003 e tem como aliado a evolução do *smartphone*, disseminando assim o conceito de onipresença no mundo digital, situação explorada atualmente nos aplicativos de saúde, que atuam em conjunto com sensores médicos sem fio, comunicações móveis, conectividade de rede e a Internet (Istepanian; Woodward, 2017). Por Lai (2016); Istepanian e Woodward (2017); World Health Organization (2011) *m-health* deve ser relacionado com a prática da medicina e da saúde apoiada por dispositivos móveis, *smartphones*, *tablets* e PDAs (Personal Digital Assistants), para serviços de saúde e informações clínicas. Kirtava *et al*. (2016) adendam que o *m-health* usufrui de tecnologias 3G (Third Generation) ou 4G (Fourth Generation) como meio para transmitir dados entre profissionais médicos e pacientes e World Health Organization (2011) completa que além dos *smartphones*, a tecnologia SMS (Short Message Service) também está presente no *m-health*, assim como GPS (Global Positioning System) e *bluetooth*, suportando aplicações básicas e complexas. Lai (2016) elucida um importante detalhe informando que o *m-health* surge a partir do *e-health* como um subsegmento da *e-health* e os *smartphones* contribuem para a proliferação do uso de conceitos *m-health*, beneficiando o telemonitoramento de agravos crônicos nas áreas de cardiologia, endocrinologia, pneumologia e dermatologia (Kirtava *et al*., 2016). Istepanian e Woodward (2017) chamam a atenção para a mudança de paradigma que o *m-health* traz, revertendo o modelo tradicional baseado em eventos, com o paciente consultando o médico apenas quanto está doente. Com o *m-health* existe o monitoramento contínuo do paciente.

2.2 REGISTROS EM SAÚDE

Da mesma forma que a seção anterior, esta foi construída para esclarecimentos de termos utilizados em tecnologias de saúde. O propósito é como melhor se posicionar ao referir os registros de pacientes em ambientes de saúde, neste trabalho. Antes da definição Smolij e

Dun (2006) colocam em pauta moldes relativos ao armazenamento de informações de saúde do paciente e gestão, a saber:

- American Society for Testing and Materials Continuity of Care Record (ASTM-CCR): padrão de conteúdo das informações de saúde, de código aberto, para dados de saúde e troca de informações, compatível com W3C (World Wide Web Consortium) com esquema no formato XML (eXtensible Markup Language);
- Health Level Seven International-Clinical Document Architecture (HL7-CDA): norma de marcação que traz o formato das informações de saúde do paciente, baseada em XML onde se especifica a codificação, estrutura e semântica de documentos clínicos;
- Health Level Seven International-Electronic Health Records (HL7-EHR System Functional Model): fornece uma lista de referência de funções que podem estar presentes em um Sistema de Registro Eletrônico em Saúde, com o objetivo de definir um padrão para exteriorizar as funcionalidades de um sistema.

Estas formas de interoperabilizar registros de pacientes em saúde são importantes para os desafios encontrados de transitar e armazenar as informações em diferentes tipos e modelos de sistemas nas mais diversas unidades organizacionais em saúde sendo privada ou pública. A capacidade de diversos sistemas computacionais e organizações cooperarem, trabalhando no intuito da troca de informações representa ganho na experiência do paciente. Mas apesar dos padrões, normas e referência existem conflitos na terminologia para representar os registros nos ambientes de saúde. No Quadro 1 são dispostas siglas utilizadas por autores e instituições, que de alguma forma representam registros de pacientes.

Quadro 1 – Resumo das siglas utilizadas em registros em saúde.

SIGLA	NOME	QUALIFICAÇÃO
CPR	Computer-based Patient Record	Registro com o estado de saúde do paciente e informações demográficas e financeiras, posteriormente absorvido pelo EHR/RES.
EHR	Electronic Health Records	Versão digital do prontuário em papel de um paciente, com históricos médicos.
EMR	Electronic Medical Record	Registro eletrônico de informações relacionadas à saúde de um indivíduo que pode ser criado, coletado, gerenciado e consultado por médicos e funcionários autorizados.
EPR	Electronic Patient Records	Versão atualizada do conceito EMR.
HIE	Health Information Exchange	Troca de informações sobre cuidados de saúde em redes de saúde.
IHR	Individual Health Records	Sigla para representar o mesmo conceito de PHR.

Continua...

SIGLA	NOME	QUALIFICAÇÃO
iPHR	Intelligent Personal Health Record	Registro PHR inteligente para sistemas especialistas.
PEP	Prontuário Eletrônico do Paciente	Formato do EMR para o Brasil.
PHA	Patient Health Application	Sigla para representar o mesmo conceito de PHR, utilizado para aplicações específicas.
PHI	Private Health Information	Sigla para representar o mesmo conceito de PHR.
PHIS	Personal Health Information System	Sistema em saúde sob controle dos pacientes com informações pessoais em saúde e integração para diagnóstico, tratamento e prevenção de doenças.
PHM	Private Health Management	Sigla para representar o mesmo conceito de PHR.
PHR	Personal Health Record	Coleta de documentação médica de um indivíduo mantida pelo próprio indivíduo ou cuidador, que contém dados como: histórico, medicamentos e intervenções.
RES	Registro Eletrônico em Saúde	Versão do EHR para o Brasil.
RME	Registro Médico Eletrônico	Versão do EMR para o Brasil.
UHR	Universal Health Record	Sigla para representar o mesmo conceito de PHR.

Fonte: Elaborado pelo autor.

As siglas dispostas no Quadro 1 podem representar a informação de um paciente com capacidade de identificá-lo em um cenário de saúde por vários ambientes e sistemas distintos. Todavia, buscar esclarecimentos sobre possíveis confusões no tema é uma boa prática. O início do problema ocorre ao usar de forma alternada e fora de contexto as siglas: EHR (Electronic Health Records) e EMR (Electronic Medical Record). Há um nível geral de confusão sobre a diferença no setor da saúde na maioria dos países devido à falta geral de clareza por parte dos formuladores de políticas, profissionais de saúde e consultores (World Health Organization, 2011).

O EHR ou Registro Eletrônico em Saúde (RES) pode ser definido como uma coleção longitudinal de informações pessoais de saúde relativas a um único indivíduo gerado por uma ou mais interações em qualquer ambiente de prestação de cuidados de saúde e armazenado eletronicamente (Himss Health Information Standards Work Group, 2013; ISO, 2005; World Health Organization, 2011). Esse agrega informações como dados demográficos do paciente, anotações de progresso, problemas, medicamentos, sinais vitais, histórico médico anterior, imunizações e dados laboratoriais (World Health Organization, 2011). Então o EHR possui todo o ciclo e roteiro do paciente com o conceito inicial de ser interoperável e oferecer ações conjuntas de profissionais e ambientes distintos.

Já o EMR ou Registro Médico Eletrônico (RME), também conhecido por PEP (Prontuário Eletrônico do Paciente) no Brasil, compreende outro escopo conceitual. Habitualmente possui um vocabulário médico controlado, com informações gerais sobre o

paciente, anotações de possíveis enfermidades e agravos, com característica de coleta e registros destes dados realizados por um único médico. Apesar de menos completo, o EMR pode colaborar além do atendimento clínico, como no faturamento, gerenciamento de qualidade, relatórios e vigilância em saúde pública. Podem ser interoperáveis dependendo dos formatos de transmissão (Dubovitskaya *et al.*, 2017; World Health Organization, 2011). Kimble (2014) complementa informando que o EMR aparece a partir dos anos 1990 sendo depois tais registros denominados EPR (Electronic Patient Records - Registro Eletrônico dos Pacientes).

Outro tipo de registro existente é o PHR (Personal Health Record – Registro de Saúde Pessoal), que contém dados de saúde e demais informações sobre o paciente com a tutela do provimento de dados atrelado ao paciente. As informações então são controladas e gerenciadas por meio do paciente ou por um procurador legal. É comum ser associado a compreensão fácil ao paciente, com informações de saúde relevantes, e indicado para auxiliar no gerenciamento de doenças. O PHR vincula o conceito de privacidade e confidencialidade das informações de saúde nele contidas, por não depender de terceiros para ser gerido e acessado. Muitos ambientes de saúde não o consideram um registro legal estando sujeito a várias limitações legais e o usuário fica dependente dos serviços disponíveis na Internet para estabelecer uma visão integrada (World Health Organization, 2011).

As siglas supracitadas são as mais comumente encontradas em ambientes de saúde, pesquisas sobre registros em saúde e sistemas informatizados. Apesar disto, existem outros tipos de siglas presentes que denominam, de certa forma, os registros existentes dos pacientes em ambientes de saúde, ou conforme (Smolij; Dun, 2006) os termos relativos ao gerenciamento de informações de saúde do paciente. Assim sendo foram encontradas siglas para representar o conceito similar ao PHR, como: IHR (Individual Health Records), PHA (Patient Health Application), PHM (Private Health Management), PHI (Private Health Information), UHR (Universal Health Record), iPHR (Intelligent Personal Health Record - Registo Pessoal de Saúde Inteligente), PHIS (Personal Health Information System) (World Health Organization, 2011; Smolij; Dun, 2006).

Muitos destes termos são utilizados indistintamente, para descrever os mesmos conceitos ou semelhantes. Por isso, tem por finalidade promover o debate e ao mesmo tempo definir qual a melhor estratégia de utilização para este trabalho. Outros dois termos para abordar que trouxeram expectativas para o trabalho foram HIE (Health Information Exchange - Intercâmbio de Informações em Saúde) e CPR (Computer-based Patient Record - Registro do Paciente Baseado em Computador).

CPR é a sigla que representa o início do Registro Eletrônico de Saúde, mas com implementação incompleta, em razão da concepção utópica apresentada para utilização. O propósito era ter um registro do paciente perpétuo, internacional e com informações sobre todas as especialidades possíveis em todos os ambientes de saúde que o paciente tivesse acesso. Devido à época que foi lançado e por todas dificuldades até hoje existentes na integração de ambientes distintos na área da saúde a ideia foi absorvida por outros conceitos como o RES. Outro conceito também oriundo destas movimentações de pacientes é o HIE (Health Information Exchange - Troca de Informações de Saúde) onde a finalidade é compartilhar informações de um grupo específico de ambientes e negócios em saúde, com interesse em promover o alcance e a busca de informações clínicas para viabilizar melhor conduta aos profissionais de saúde na prestação de serviços ao paciente (World Health Organization, 2011; Smolij; Dun, 2006).

Independente do propósito, os conceitos nesta seção apresentados possuem a característica de proporcionar ganhos aos pacientes que necessitam documentar particularidades pertencentes à área médica. A preocupação neste trabalho é inserir no contexto saúde uma alternativa para ao mesmo tempo popular informações e tornar compartilhável, mas ao mesmo tempo confidencial respeitando os interesses do paciente.

2.3 PRIVACIDADE

Consoante a Priberam (2011), privacidade é a condição do que é privado, pessoal ou íntimo, ou seja, relacionado à vida privada. O limite da privacidade de um indivíduo engloba informações que apenas ele possui, mas que os outros não conhecem e isto, deve ocorrer até quando o proprietário da informação permita existir o compartilhamento (Chang *et al*., 2018). O conceito de privacidade surge em 1970, conforme Lee (2020) gradualmente começa apresentar vínculos a partir de 1980 com sistemas de informação. Segundo Chang *et al.* (2018) a privacidade informacional tem sido ativamente discutida no campo dos sistemas de informação no que diz respeito à violação de informações pessoais, cujo aumento de acontecimentos relacionados ocorre na era da informação.

Um dos efeitos colaterais do rápido avanço tecnológico tem sido a crescente ameaça à privacidade das pessoas, impulsionada pela extrema facilidade com que as informações privadas são atualmente capturadas, trocadas, usadas e mantidas (Nsengimana, 2017). Conforme Chen *et al.* (2020) novos estudos devem dar mais atenção ao conceito de privacidade.

No entanto, ainda existem defeitos no gerenciamento atual de privacidade e segurança, como por exemplo, garantir que o número de pacientes não seja usado por terceiros ou por outros pacientes, para atos hostis. As empresas com plataformas na Internet violam a privacidade dos indivíduos por meio das práticas de gerenciamento de informações pessoais inadequadas e as preocupações de privacidade com tais dados causam vários efeitos colaterais sociais (Lee, 2020).

Nsengimana (2017) alerta que um maior grau de consciência pessoal relacionado aos riscos à privacidade, o exercício de zelo pessoal deliberado e a autocrítica são necessários para entregar benefícios junto ao uso da tecnologia. Com muitas informações críticas, os dados sensíveis são ameaçados constantemente. Pesquisas, como Natsiavas *et al.* (2018), são realizadas para entender como estão pacientes e os cuidados com a privacidade dos dados sigilosos e indicam um maior percentual de pacientes preocupados a respeito do compartilhamento de informações pessoais.

Compartilhamento de dados de saúde com segurança e preservação da privacidade: tem o potencial de envolver milhões de indivíduos, provedores de saúde, entidades de saúde e pesquisadores médicos para compartilhar grandes quantidades de dados (Kuo; Kim; Ohno-Machado, 2017). A tecnologia é capaz de suprir funções notórias para a sociedade, com alta disponibilidade, com resposta às solicitações dos cidadãos em tempo real a partir de uma variedade de dispositivos inteligentes conectados, mas é preciso respeitar os limites de segurança e responsabilidade. Nesse contexto, a confiança entre as pessoas e os governos que detêm essas informações vitais sobre respectivos cidadãos deve ser irrepreensível (Nsengimana, 2017).

A privacidade melhora tecnologias que já se apresentam costumeiramente falhas, mas, isso não é fundamentalmente verdade. Além disso, é incorreto afirmar que a segurança não pode ser garantida sem sacrificar a privacidade das pessoas (Nsengimana, 2017). As preocupações com a privacidade das informações dos pacientes na área da saúde operadas por computação em nuvem afetam não apenas a confiança ou a crença dos pacientes no risco de privacidade, mas também a intenção de adotar soluções de *e-health* (Xu, 2019).

2.4 CRIPTOGRAFIA

Conforme Dooley (2018), a criptografia consiste em um conjunto de técnicas para criar sistemas de escrita secreta. Stinson e Paterson (2019) colaboram definindo que a criptografia

tem por objetivo permitir a existência de uma comunicação em um canal inseguro entre emissor e receptor sem que algum tipo de ato mal intencionado consiga entender o conteúdo das mensagens trafegadas. A razão central em utilizar o conceito de criptografia é para manter a informação sigilosa, no qual muitas empresas empregam quando dados confidenciais estão envolvidos (Hintzbergen *et al.,* 2018).

A criptografia tem sido usada para ajudar a fornecer comunicações confidenciais entre partes mutuamente confiáveis, onde em sua forma mais básica, emissor e receptor, concordam com uma determinada chave secreta antes da mensagem transmitida A chave é usada para transformar a mensagem original (normalmente chamada de texto simples) em uma forma embaralhada que é ininteligível para quem não possui a chave, sendo esse processo chamado então de criptografia e a mensagem embaralhada denominada de texto cifrado. Para leitura da mensagem é necessário o processo reverso, ou seja, receber o texto cifrado, e usar a chave para transformar o texto cifrado de volta no texto simples original, este é o processo de descriptografia (Stinson; Paterson, 2019).

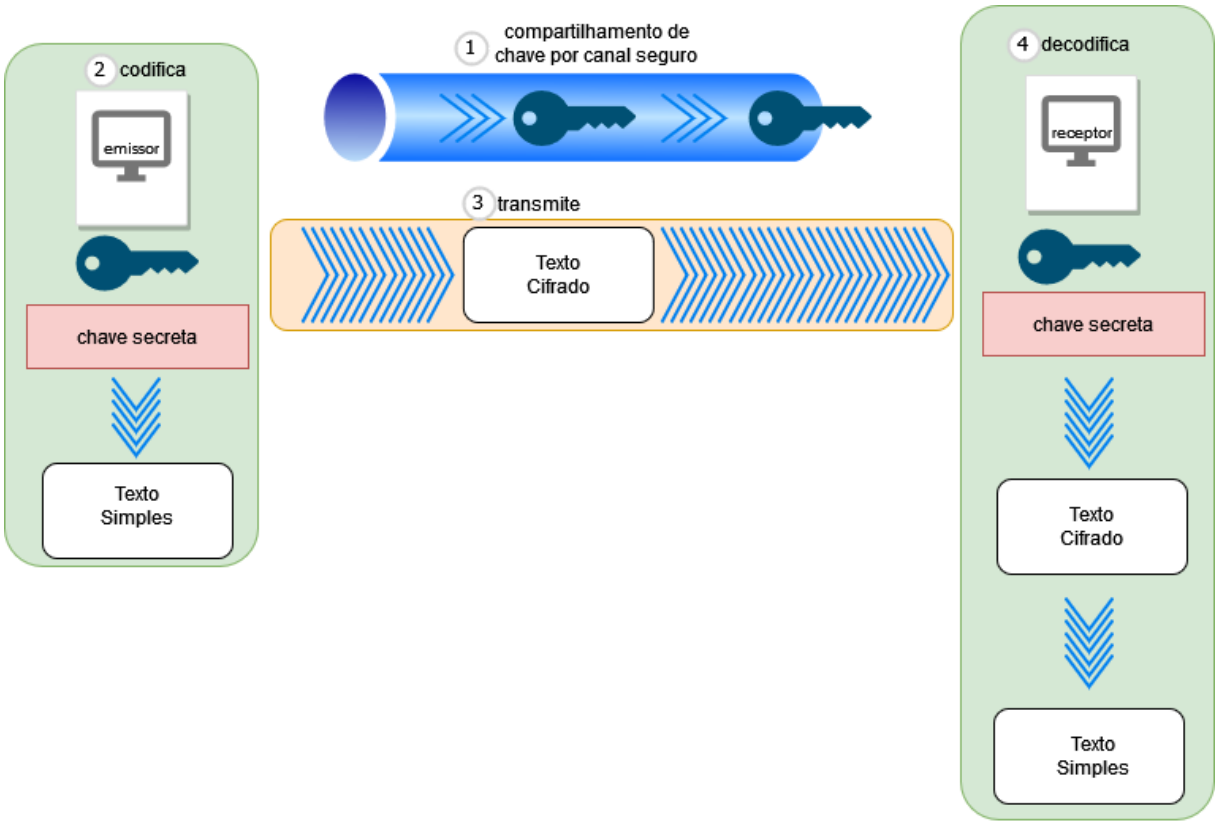
Soluções que utilizam o conceito de criptografia precisam se preocupar com o gerenciamento das chaves compartilhadas, estas são críticas e requerem de rigoroso controle no armazenamento e processos de distribuição. As chaves criptográficas precisam ser resguardadas para não terem adulterações ou qualquer tipo de avaria, pois é possível a inviabilidade de acesso ao dado por problemas advindos de chaves perdidas, comprometidas, com acessos vencidos ou roubadas (Dooley, 2018; Hintzbergen *et al.,* 2018).

São opções de algoritmos baseados em chaves, os simétricos e os assimétricos e estes têm o emprego do conceito de chaves, mas de maneira diferente, enquanto a característica da criptografia simétrica é a existência de uma chave secreta que o emissor e o receptor compartilham para cifrar e decifrar os dados, a criptografia assimétrica funciona a partir de um par de chaves, onde a chave pública é responsável pela criptografia dos dados que só podem serem descriptografados a partir da chave privada deste mesmo par de chaves (Hintzbergen *et al*., 2018).

A criptografia simétrica, ilustrada na Figura 1, converte um texto simples em uma mensagem cifrada, por intermédio de uma chave secreta, utilizada também subsequentemente para decriptar a mensagem, revertendo em texto simples, porém, a criptografia simétrica precisa de um canal seguro antes que qualquer texto cifrado seja transmitido, pois esta chave secreta precisa ser compartilhada entre emissor e receptor antes da ação criptográfica (Stinson;

Paterson, 2019; Hintzbergen *et al*., 2018). Portanto a exposição da chave, é necessária para criptografar os dados, mas é uma questão crítica a ser resolvida em cada transação.

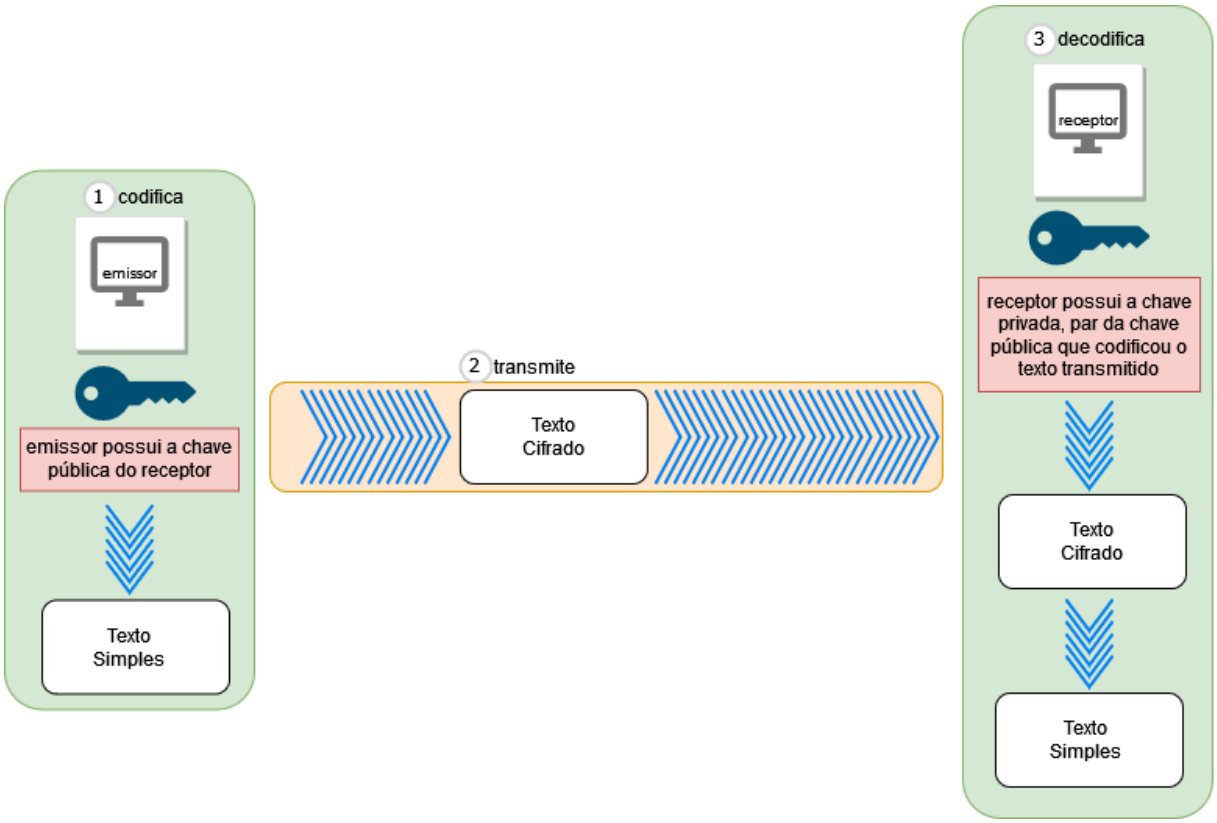
Figura 1 – Esquema de funcionamento da criptografia simétrica



Fonte: Elaborada pelo autor.

Já na criptografia assimétrica, demonstrada na Figura 2, existe o conceito do par de chaves, com a chave pública deste par de chaves sendo compartilhada para criptografar o dado e somente a chave privada do mesmo par de chaves utilizado para descriptografar, nesse caso então não é mais necessário que o emissor e receptor tenham a mesma chave. A vantagem é que mesmo com a chave pública conhecida por terceiros não se tem a descriptografia da informação, pois o dono do par de chaves é o único detentor da chave privada para decifrar o dado, ou seja, a descriptografia usa a chave privada secreta, no qual nunca é transmitida a ninguém em nenhum lugar (Stinson; Paterson, 2019; Dooley, 2018; Hintzbergen *et al*., 2018).

Figura 2 – Esquema de funcionamento da criptografia assimétrica.



Fonte: Elaborada pelo autor.

São exemplos de algoritmos simétricos, com chave única, o AES, DES, 3DES, IDEA, Blowfish, Twofish, RC2 e CAST e assimétricos com par de chaves, o RSA, ElGamal, Diffie-Hellman e Curvas Elípticas. O propósito deste trabalho não é esgotar o assunto e conceitos sobre criptografia, mas explorar algumas possibilidades de implementação para desenvolver soluções junto a tecnologia Blockchain.

2.5 SAÚDE 4.0

O termo Saúde 4.0 tem por objetivo o investimento em tecnologia nos ambientes de saúde e Al-Jaroodi, Mohamed e Abukhousa (2020) explicam que pode ser definida como a implementação de plataformas integradas de saúde, virtualizadas, na nuvem, entre outros tipos, de forma distribuída e em tempo real se oferecendo como serviço para pacientes, profissionais, responsáveis, hospitais, clínicas, fornecedores. Este conceito é associado a integração de tecnologias com os vários ramos da saúde a partir de automatizações e inovações, fornecendo modelos melhores e interações mais eficazes em toda a cadeia da saúde.

A origem de como os serviços de saúde foram modificados ao longo dos anos é retratada por Thuemmler e Bai (2017) que colocam uma grande transformação na década de 1970, onde os ambientes eram centrados no hospital e focado no profissional de saúde, migrando agora para um modelo de atendimento distribuído e orientado ao paciente, onde muitos elementos de atendimento são fornecidos virtualmente e por cuidadores informais, normalmente os responsáveis dos pacientes. Thuemmler e Bai (2017) ainda descrevem que leitos hospitalares e hospitais na Europa diminuíram em decorrência do avanço da saúde e do monitoramento tecnológico, indicando uma tendência para o futuro dos hospitais, se tornando o último recurso para condições onde as tecnologias modernas não podem ajudar de modo efetivo.

A Saúde 4.0 permite que dados valiosos sejam usados de forma mais consistente e eficaz. É possível a partir dos conceitos da Saúde 4.0 identificar áreas de melhoria e permitir que as pessoas tomem decisões mais informadas, ajudando a mover todo o setor de saúde de um sistema que é reativo e focado na taxa por serviço para um sistema que é baseado em valor, que mede resultados e incentiva a prevenção proativa (Chanchaichujit *et al*., 2019).

É bom salientar que embora todo aparato tecnológico existente, ocorre uma demora dos ambientes de saúde em se qualificar com adoções tecnológicas de uma forma geral, no qual a circunstância mais preponderante é a insuficiência tecnológica do local com os processos de trabalho (Yusof; Stergioulas; Zugic, 2007). As tecnologias existentes no conceito da Saúde 4.0 tem o caráter disruptivo e podem, se bem aplicadas melhorar o atendimento médico e organizar os cenários de saúde. Há vários fatores que influenciam o impulso para a melhoria da assistência à saúde, Chanchaichujit *et al*. (2019) colocam o interesse governamental de cada nação, o aumento de uma população com conhecimento de tecnologia e o envolvimento e capacitação dos prestadores de serviços em saúde. Em Al-Jaroodi, Mohamed e Abukhousa (2020) e Chanchaichujit *et al*. (2019) existe um estudo sobre Saúde 4.0, as tecnologias possíveis, tipos de implementação e aplicações existentes, no entanto anterior a estas características é relevante traçar o processo histórico até o atual momento das especificidades de cada época, principais características, inovações e dificuldades.

2.5.1 Histórico Tecnológico

Chanchaichujit *et al*. (2019) afirmam que apesar da prestação de serviços em saúde ter muito a ganhar com a implementação de tecnologias da informação, o processo têm sido o mais

lento de todos, comparado a outros setores na adoção de tecnologia. Para Morrow *et al*. (2012) o regime de alinhamento entre tecnologias, processos clínicos e usuários demorou para ocorrer, sendo desprezado por muito tempo nos ambientes de saúde, não se estreitou o relacionamento das tecnologias, trazendo rejeições por muito tempo. Chanchaichujit *et al*. (2019) comentam sobre a curta história da TI na saúde, e vislumbra o surgimento de novas tecnologias disruptivas, com papel crucial no fechamento da lacuna de capacidade e na conquista de mais aceitação dos principais usuários. Nos estudos de Kirtava *et al*. (2016), por exemplo, é notável que os diagnósticos e monitoramento de doenças com a introdução do *e-health* aumentou a confiança dos pacientes nos tratamentos

Mas este avanço e o aparecimento do termo Saúde 4.0 possui uma linha histórica e antecedida pelas evoluções das relações existentes entre saúde e tecnologia. Antes do século XIX não existia uma nomenclatura característica para apresentar os diferentes estágios de desenvolvimento da saúde a partir da tecnologia. Todavia, é possível reconhecer progressos expressivos na cronologia da medicina e da tecnologia médica, no qual inspiraram gradualmente o modo de entender a evolução da área da saúde onde são exemplos de marcos (Venkatapuram, 2011; Kessler, 2007; Sackett *et al.*, 2000):

- No século XV, a prensa móvel, desenvolvida para imprimir textos, oportunizou a manufatura em grande quantidade de livros e a transmissão do conhecimento médico, proporcionando o ensino e esclarecimentos da população sobre saúde e enfermidades;
- No século XIX, o descobrimento do procedimento de anestesia que trouxe cirurgias de menos riscos aos pacientes, e o desenvolvimento do microscópio, o qual permitiu melhores análises, exames e pesquisas;

Além das descobertas existia um grande número de sistemas de cura e práticas médicas em distintas culturas, tais como: a medicina tradicional chinesa com a prática da acupuntura; na Índia com a denominada Ayurveda (prática médica passada que focalizava a conexão entre o corpo, a mente e o espírito); e na Grécia antiga, a partir da observação clínica e do tratamento holístico do paciente (Venkatapuram, 2011; Kessler, 2007; Sackett *et al*., 2000). Surgiram nomenclaturas para retratar distintas épocas de desenvolvimento da tecnologia na área da saúde, estas foram evidenciadas para mostrar que existiu um curso progressivo dos sistemas de saúde com maior complexidade, interoperabilidade, propriedade de compartilhar informações e sustentar a tomada de decisões dos estabelecimentos de saúde

Existem, nos autores, divergências em indicar as décadas e marcos das épocas em Saúde. As discordâncias ocorrem com a vigência da era de cada período, com relação à surgimento, intervalo de tempo e término. Ahmad *et al.* (2022) comentam as várias classificações existentes sobre as fases da Saúde, indicando que a distribuição por estágios de evolução acontece de acordo com diferentes critérios, como estrutura social, desenvolvimento técnico científico, desenvolvimento de serviços e o uso de tecnologias de comunicação. No Quadro 2 são expostos autores e os quatro (4) estágios, Saúde 1.0, Saúde 2.0, Saúde 3.0 e Saúde 4.0, separados pela classificação dos estágios a partir dos critérios estabelecidos em (Ahmad *et al*., 2022).

Quadro 2 – Estágios em Saúde.

Desenvolvimento de serviços / tecnologias de comunicação				
Autor	**Saúde 1.0**	**Saúde 2.0**	**Saúde 3.0**	**Saúde 4.0**
Ahmad *et al*. (2022)	séc. XVIII a 1920	entre 1920 e 2010	entre 1990 e 2020	a partir de 2015
Chanchaichujit *et al*. (2019)	entre 1970 e 1990	entre 1990 e 2005	a partir de 2000	a partir de 2018
Shaikh e Ali (2020)	a partir de 1970	até 2005	entre 2006 e 2015	a partir de 2016
Nair e Tanwar (2020)	entre 1970 e 1990	entre 1990 e 2006	entre 2006 e 2015	a partir de 2015
Kumari et al. (2018)	entre 1970 e 1990	entre 1991 e 2005	entre 2006 e 2015	a partir de 2016
Sharma, Aujla e Bajaj (2019)	entre 1990 e 2009	entre 2007 e 2017	a partir de 2017	futuro
Desenvolvimento técnico-científico				
Autor	**Saúde 1.0**	**Saúde 2.0**	**Saúde 3.0**	**Saúde 4.0**
Chen *et al*. (2019)	a partir de 1830	a partir de 1890	a partir de 1980	a partir de 2020
Pang *et al*. (2018)	entre 1840 e 1890	entre 1890 e 1960	entre 1960 e 2010	a partir de 2018
Estrutura Social				
Autor	**Saúde 1.0**	**Saúde 2.0**	**Saúde 3.0**	**Saúde 4.0**
Jain *et al*. (2021)	entre 1970 e 1990	entre 1980 e 2005	a partir de 2005	a partir de 2020

Fonte: Elaborado pelo autor.

O Quadro 2 foi construído para demonstrar algumas possíveis classificações entre autores e os critérios supracitados. Vale ressaltar que alguns autores não listados apenas seguem as épocas existentes na Revolução Industrial não esclarecendo os motivos pertinentes a cada fase ter associação em determinado período. Outra constatação é observada nos autores que trazem tecnologias provenientes do conceito Saúde 4.0, estes se apoiam em tecnologias e na Internet como característica norteadora do processo da divisão de épocas.

Apesar de existirem autores que trazem a evolução respeitando outros fatores históricos e de processos que combinam razões não tecnológicas e nem de serviços, ou devido a evoluções de cura, doenças, vacinas, este trabalho se baseou no critério definido por Ahmad *et al.* (2022) denominado como desenvolvimento de serviços e o uso de tecnologias de comunicação, visto o projeto e temática serem de caráter tecnológico, concentrando tecnologias

do conceito de Saúde 4.0. Sendo assim, as épocas são classificadas neste trabalho acompanhando (Shaikh; Ali, 2020; Nair; Tanwar, 2020; Chanchaichujit *et al*., 2019; Kumari *et al*., 2018).

Num primeiro momento, entre 1970 e 1990, existe o aparecimento dos sistemas modulares de TI (Tecnologia da Informação), sendo este período chamado de Saúde 1.0. Não há uma data precisa para o início da Saúde 1.0, pois ela é uma referência conceitual que abrange um período histórico extenso. Depois do ano de 1990, durante uma década e meia, a maioria dos sistemas de TI iniciaram o funcionamento em rede, e os EHRs que estavam sendo gerados começaram a se integrar com imagens clínicas, conferindo aos médicos uma perspectiva melhor, sendo este momento conhecido como Saúde 2.0. A partir do ano 2000, ocorre o desenvolvimento das informações genômicas, simultaneamente com a criação dos dispositivos vestíveis e dispositivos implantáveis. A integração de todos os dados resultantes, em conjunto com os registros eletrônicos do paciente já em rede, chancela o início da Saúde 3.0. Todavia, devido à incompatibilidade de dados e resistência dos provedores de saúde, a adoção de TI na Saúde 4.0 não produziu melhorias significativas para a coletividade. Após estas fases de evoluções o conceito de Saúde 4.0 compõe principalmente as tecnologias, IoT para integração de tecnologias e coleta de dados, Inteligência Artificial (IA) para análises e Blockchain para registros médicos de pacientes.

Este processo evolutivo das diferentes condutas existentes nos ambientes de Saúde durante os anos e seus principais marcos são apresentados no Quadro 3.

Quadro 3 – Evolução das tecnologias junto à saúde no conceito Saúde 4.0.

	Saúde 1.0	**Saúde 2.0**	**Saúde 3.0**	**Saúde 4.0**
Principal objetivo	Melhorar a eficiência e reduzir papéis	Melhoria dos dados compartilhados e produtividade	Fornecer soluções centradas no paciente	Fornecer rastreamento em tempo real e soluções como resposta
Foco	Automação simples	Conectividade com outras organizações	Interatividade com Pacientes	Monitoramento integrado em tempo real, diagnósticos com suporte a IA
Compartilhamento de informações	Dentro de uma organização	Dentro de um grupo de provedores de saúde	Dentro de um país	Cadeia global de suprimentos de saúde

Continua...

	Saúde 1.0	Saúde 2.0	Saúde 3.0	Saúde 4.0
Principais tecnologias usadas	Sistema de Gerenciamento de Informações Laboratoriais e Sistemas Administrativos	EDI e computação em nuvem com mensagens HL7 para intercâmbio de dados	Registros Eletrônicos Médicos, Big Data, Dispositivos Vestíveis e Sistemas de Otimização.	IoT, Blockchain, Inteligência Artificial, Data Analytics
Limitações	Sistemas autônomos com funcionalidade limitada	Compartilhamento de informações críticas sem interação com pacientes	Diferentes padrões utilizados dentro da comunidade com interoperabilidade limitada	Tecnologias novas e não testadas com preocupações sobre privacidade de dados

Fonte: Adaptado de Chanchaichujit *et al*. (2019).

Posterior a apresentação do Quadro 3, referente ao progresso que a área da saúde transportou até atingir o conceito Saúde 4.0 é propício compreender quais são os componentes principais que devem ser respeitados e incorporados. Com base em Al-Jaroodi, Mohamed e Abukhousa (2020); Chanchaichujit *et al.* (2019) um conjunto de tecnologias é proposto.

2.5.2 Tecnologias 4.0

As tecnologias aqui descritas são oriundas possuem as definições baseadas em Langley *et al.* (2021); Al-Jaroodi, Mohamed e Abukhousa (2020); Chanchaichujit *et al.* (2019) trazem as tecnologias consideradas integrantes do propósito da Saúde 4.0:

- **Internet das Coisas (IoT)**: Aqui a intenção é capacitar os pacientes a realizarem o auto-gerenciamento das necessidades médicas e fornecer canais para comunicação mais interativa com os profissionais de saúde. Os dispositivos inteligentes capturam com precisão os dados em tempo real e se comunicam para possíveis decisões. É possível conectar dispositivos médicos em uma rede, com sensores para medir, a frequência cardíaca, temperatura corporal, comportamento do sono, pressão arterial, atuadores como bomba de infusão, alarmes, ventiladores, e sistemas médicos, como máquinas de diálise, máquinas de raio-x e outros dispositivos de diagnóstico e tratamento;
- **Internet de Todas as Coisas (IoE)**: Concepção da interconexão de pessoas, processos, dados e coisas (dispositivos inteligentes). Possui abordagem mais holística, trabalhando a preferência do usuário, onde todos os objetos físicos poderão fazer parte desta rede com intuito de facilitar ao usuáro praticidade e

conhecimento. Pode ser vista em exemplos como na área da saúde em que dispositivos vestíveis, aplicativos de saúde, registros médicos eletrônicos e outras fontes de dados integrados para melhorar a eficiência e a qualidade do atendimento médico, podendo realizar diagnósticos preventivos, monitorando sinais vitais de um paciente afim de tomar ações antes de um adoecimento;

- **Internet dos Serviços (IoS)**: Este conceito é atrelado aos serviços, com ofertas e utilização por meio da Internet, a demanda pode ser propiciada produto ou processo, ou seja, sem intermediários, como por exemplo, uma ação a partir de uma configuração ou um registro crítico. O conceito de IoS remete a um ambiente que provê serviços, dispostos internamente ou externamente. Pode acontecer a comunicação online entre máquinas ou do homem com a máquina, Exemplos de utilização podem acontecer com o monitoramento de sensores para umidade, temperatura e iluminação, onde geralmente os conceitos de IoT e IoS atuam concomitantemente;
- **Sistemas Ciber-Físicos Médicos (Medical Cyber-Physical Systems – CPS)**: O CPS médico é usado para facilitar interações úteis entre o mundo cibernético (por exemplo, *software* e sinais de controle) e o mundo físico (por exemplo, equipamentos e pacientes) fornecendo serviços contínuos de monitoramento e tratamento de saúde. Os CPS médicos usam controles de retorno incorporados para monitorar e reagir a condições específicas corretamente. Um exemplo de CPS médico são os dispositivos médicos implantáveis como os simuladores cerebrais profundos usados para tratar epilepsia, marcapassos cardíacos usados para regular a frequência cardíaca e bio-instrumentos usados para lidar com bio-sinais;
- **Nuvem de Saúde (Health Cloud)**: A infraestrutura em larga escala fornece computação escalável e sob demanda, armazenamento de dados e recursos e serviços avançados de *software* para aplicativos de saúde. Exemplos incluem armazenar os EHRs, analisar imagens médicas e monitorar riscos e tendências específico para a saúde pública, tais aplicativos exigem computação intensiva e enormes recursos de armazenamento que a nuvem pode oferecer facilmente;
- **Névoa da Saúde (Health Fog)**: A *fog computing*, representa a atribuição da capacidade de processamento mais perto do raio de ação da rede. Geralmente são usados para suavizar e melhorar a comunicação e integração entre dispositivos, sistemas médicos e nuvens de saúde. A névoa da saúde pode fornecer mini-

serviços sob demanda para suporte interativo de baixa latência, reconhecimento de localização e suporte à mobilidade. Como conceito aplicado a saúde a *fog computing* é importante para a carência existente entre a nuvem de saúde e dispositivos de IoT em saúde que precisam de integração constante. É possível ampliar a capacidade computacional a borda da rede tratando os dados produzidos por dispositivos IoTs e gerando informações mais cabíveis a nuvem;

- **Big Data**: As distintas fontes de dados e diferentes tipos e padrões de informações, podem ser computados e sumarizados para potencializar prevenções e predições capacitando serviços de saúde a identificar as melhores tomadas de decisão, quanto á várias frentes de desenvolvimento aplicada a gestão de saúde. O conceito de Big Data para os sistemas em saúde, para as diversas integrações pode ser um aliado devido ao acúmulo agregado ao longo do tempo. A partir da Análise de Big Data é possível oferecer mecanismos avançados para descobrir tendências, correlações e percepções dos dados. As vantagens são grande, desde a redução de custos, melhora dos serviços de saúde e personificação do atendimento ao público de maior qualidade diante das ferramentas de análise;
- **Rede de Comunicação Móvel 5G**: A principal virtude de aplicação da tecnologia de rede 5G (Fifth Generation) é fornecer recursos avançados, como comunicação rápida e de baixa latência, gerenciamento inteligente e recursos de dados. Todos os benefícios das redes móveis em larga escala, definido para os escopos de saúde com *m-health*, são aplicados também para os ambientes e sistemas de saúde. Características como pronta resposta rápida, alcance e serviços acoplados são atrativos para a utilização das redes sem fio que ajudam no monitoramento e prevenção dos pacientes;
- **Inteligência Artificial**: Os conceitos existentes na Inteligência Artificial ajudam vários ambientes em várias proporções no escopo saúde. Alguns são os exemplos, como o fornecimento de modelos preditivos mais precisos da condição de um paciente, otimização dos serviços de um hospital, fluxos de trabalhos ou reconhecimento de padrões. As aplicações existem e a cada dia surgem novas, melhorando algoritmos, entendendo processos recorrentes, personalizando escopos de atendimento, catalogando e aprendendo novas doenças.

As técnicas que fazem parte do propósito geral da Saúde 4.0 não são entendidas apenas como desenvolvimento tecnológico. Al-Jaroodi, Mohamed e Abukhousa (2020);

Chanchaichujit *et al.* (2019) especificam que existem 5 (cinco) Princípios Fundamentais da Saúde 4.0, que são:

- **Interoperabilidade**: Capacidade de conectar distintos dispositivos e sistemas médicos. A interoperabilidade é o princípio primário e a chave inicial para a Indústria 4.0. A habilidade do sistema de se comunicar com vários outros sistemas para coordenar funções distintas e trocar dados é chamada de interoperabilidade. A interoperabilidade fornece ao homem e à máquina a capacidade de obter dados em tempo real, o que permite uma tomada de decisões mais rápida e eficaz. Sem a interoperabilidade, imensas quantidades de dados coletados e armazenados todos os dias ficam sem uso ou não são trocados com outros sistemas para processamento. Para desenvolver oportunidades e aumentar a presença de integração entre homem e máquina, as instalações devem ser vinculadas à IoT. A interoperabilidade permite a integração de *softwares* como sistemas Enterprise Resource Planning (ERP), EMRs, Laboratory Information Management System (LIMS) e outros tipos de *softwares*, minimizando assim o custo de transação entre os sistemas de *softwares* na análise e consolidação dos dados. Os dados coletados em distintos sistemas e dispositivos são processados e consolidados em conhecimentos que podem auxiliar e melhorar a tomada de decisão para as organizações. Os autores colocam que existem alguns procedimentos que aumentam a capacidade de interoperabilidade, como protocolos padrões que não exigem muitos esforços de codificação extra;
- **Virtualização**: Capacidade de criar cópias virtuais (digitais) de diferentes dispositivos, sistemas e processos de saúde. Algumas funções que não podem ser executadas no mundo físico podem ser formadas no mundo digital. Os dados obtidos a partir de instalações, juntamente com seus equipamentos e processos, são simulados com modelos de simulação virtual para desenvolver uma visão digital das operações. Essa visão digital é denominada Virtualização e fornece a competência de minimizar o tempo de inatividade dos equipamentos, melhorar processos e lidar com situações complexas. A visão virtualizada é útil na coordenação e monitoramento do mundo físico e digital. Prestar serviços remotos e monitorar a condição e a localização do produto são apenas alguns dos benefícios tangíveis da Virtualização. Muitas organizações enfrentam desafios para entender os benefícios e o impacto da incorporação de novas tecnologias em seus processos. A virtualização proporciona uma visão exata das atividades realizadas por "humano

e máquina", juntamente com a capacidade de otimizar processos e utilizar medidas preventivas para mitigar riscos. Os benefícios combinados de robôs móveis, realidade virtual e equipamentos de Realidade Aumentada são exemplos que proporcionam grandes oportunidades;

- **Descentralização**: Capacidade dos sistemas de saúde de se controlarem com decisões adequadas. No processo de fabricação tradicional, vários subsistemas em cada etapa do processo são apoiados por um sistema centralizado. Em uma estrutura centralizada, um computador central incorporado à lógica empresarial é usado para fornecer soluções para outros subsistemas. Com a Indústria 4.0, há certas restrições em torno de ter uma estrutura centralizada. Uma estrutura centralizada limita a escalabilidade. Também é difícil adaptar-se aos próximos avanços ou responder às flutuações, pois a estrutura não pode ser alterada quando atinge sua capacidade máxima. Em uma estrutura distribuída, os nós (*hosts*) lógicos podem ser usados para ajudar ou lidar com os subsistemas ou componentes remotos. Para melhorar a inteligência e funcionalidade em uma estrutura distribuída, os dados coletados são compartilhados com cada nó (*hosts*) e as capacidades de cada nó são combinadas. Componentes ou subsistemas são programados com lógica de negócios em uma estrutura completamente descentralizada. Esse recurso aumenta a inteligência necessária para executar as funções necessárias e permite a coordenação com outros subsistemas para gerenciar tarefas mais complicadas. Do ponto de vista da Indústria 4.0 de descentralização, mais robôs e AGVs (Veículos Auto Guiados) podem ser adicionados para melhorar a facilidade de operação e a tomada de decisões descentralizada e com isso melhorar a execução mais rápida das operações. Os subsistemas e os trabalhadores são coordenados com a ajuda dos CPSs;
- **Capacidade em Tempo Real**: Capacidade de reunir e analisar ativamente os dados de saúde para tomar as medidas corretas. Obter informações em curso ou em tempo real sobre equipamentos e seus processos é o objetivo final deste princípio fundamental. Este princípio é complementar aos princípios de Virtualização e Interoperabilidade que promovem recursos em tempo real. Os CPSs médicos também são usados para coletar dados em tempo real em toda uma cadeia de suprimentos. Robôs, AGVs e equipamentos que interagem com dispositivos computadorizados, como scanners, sensores e etiquetas RFID (Radio Frequency Identification) e se conectam com IoT fornecem também este de dados em tempo

real. Nesses casos, homem e máquina podem tomar decisões em tempo real com a ajuda de dados em tempo real;

- **Orientado a Serviços**: Capacidade de criar serviços de *software* para interagir com dispositivos e sistemas médicos. As atividades ou serviços realizados por máquinas e seres humanos são otimizados por meio da conexão com a internet. O IoS é usado para otimizar o serviço e isso é realizado para melhorar a orientação do serviço. Desde o estágio inicial de movimentação de mercadorias até a fase final de análise de dados, todos os serviços envolvidos são supervisionados via internet para mitigar questões específicas de negócios. Para ilustrar o ponto anterior, se uma estação de montagem modular equipada com AGVs for submetida a uma abordagem orientada ao serviço, o IoS serve como uma plataforma para os AGVs e estações modulares realizarem os serviços necessários. As etiquetas RFID sobre mercadorias contêm procedimentos de projeto, e os serviços necessários em relação ao projeto são decididos de forma autônoma pelas máquinas. Nesse ponto, a máquina formula o procedimento necessário e orienta os serviços a serem realizados por meio de IoS. Apesar de coletar e armazenar grandes quantidades de dados, a troca de informações entre vários sistemas torna-se muito complexa. No entanto, a orientação de serviços capacita fluxos de dados mais liberados entre e dentro dos sistemas. O *software* utilizado por uma empresa serve como uma ferramenta para gerenciar serviços internos, o que, por sua vez, maximiza os benefícios da funcionalidade externa. O *software* de suporte serve como uma plataforma bem fundamentada para otimizar e executar processos de negócios. Um outro aspecto trabalhado neste princípio é uma maior capacidade de alterar processos e ofertar maior escalabilidade;
- **Modularidade**: Capacidade de melhorar os módulos individuais para atender a novos requisitos e reutilizar os módulos disponíveis para construir novos sistemas de saúde. Este conceito preconiza a construção entendendo que precisa existir um planejamento para se adaptar ao novo. Uma solução que se molda intrinsecamente às mudanças e novos avanços é denominada como modular. Estas soluções modulares permitem que uma empresa responda rapidamente à flutuação da demanda e garanta a segurança dos investimentos iniciais durante as específicas adaptabilidades. Estes ajustes rápidos para suprirem demandas emergenciais, são

fundamentais ao escopo da saúde que eventualmente trabalha com situações novas, tais como surtos de doenças que precisam ser entendidas e documentadas.

Em Al-Jaroodi, Mohamed e Abukhousa (2020); Chanchaichujit *et al.* (2019); Grigoriadis *et al.* (2016); Yusof, Stergioulas e Zugic (2007), são indicadas aplicações que se tornam cada dia mais rotineiras e utilizam conceitos de Saúde 4.0, como por exemplo, a informação da administração das doses de medicamentos, dispositivos eletrônicos de auto-injeção com transmissão via rádio, aplicativos com foco no controle de dispositivos implantados em pacientes, aplicativos de suporte a profissionais de saúde com os mais diversos focos, aplicativos para gerenciamento automatizados de recursos hospitalares, aplicativos para gestão geral de sistemas integrados de saúde, serviços de apoio à coleta de transferência de dados, segurança e privacidade.

O momento atual da Saúde 4.0 indicado por Thuemmler e Bai (2017) traz a virtualização no domínio da saúde e o surgimento da próxima geração de novas tecnologias sem fio, mais especificamente o 5G, fornecendo os predicados necessários que faltam para cada vez mais conectar dispositivos, reduzindo tempos de latência abaixo de 5 ms, melhoria da cobertura, melhoria da vida útil da bateria nos dispositivos, melhoria da segurança, qualidade de serviço (QoS - Quality of Service) e qualidade da experiência (QoE - Quality of Experience), largura de banda aprimorada e melhor suporte aos dispositivos IoTs. Estas são algumas das soluções que podem surgir com o emprego da Saúde 4.0, a partir dos princípios e tecnologias.

Tais adventos surgem como facilitadores a médicos e pacientes e provedores de saúde, mas precisam ser gerenciados e trabalhados com escopo definido para não se tornarem barreiras burocráticas na utilização dos serviços de saúde. Thuemmler e Bai (2017) citam que novas tecnologias de rede, como a rede de 5ª geração (5G) irão permitir acesso onipresente, melhorar a conectividade e permitir a orquestração *ad-hoc* de serviços, integrando pacientes, cuidadores formais e informais, assistentes sociais e médicos praticantes. É bom entender que em estudos por Liu *et al*. (2015); Moreira Neto *et al*. (2018); Mukhiya *et al*. (2019); Coutinho *et al*. (2020), as tecnologias neste documento tratadas como conceito de Saúde 4.0 são também atreladas ao termo *e-health*, em uma coleção de soluções computacionais alusivas a área da saúde, utilizando a Internet para dispor serviços.

Conforme Coutinho *et al*. (2020) o *e-health* projeta diversos enfoques, que são iguais ao conceito de Saúde 4.0, como o monitoramento remoto de pacientes, acesso local e remoto à informações de saúde, possibilidade da integração de processo de de negócios condizentes ao

setor de saúde, boa comunicação entre provedores e pacientes, fornecimento de serviços para a entrega de informações e acesso a informação essenciais aos pares.

Estas são algumas das soluções que podem surgir com o emprego da Saúde 4.0, a partir dos princípios e tecnologias. Tais adventos surgem como facilitadores a médicos e pacientes e provedores de saúde, mas precisam ser gerenciados e trabalhados com escopo definido para não se tornarem barreiras burocráticas na utilização dos serviços de saúde.

2.5.3 Perspectivas da Saúde 4.0

Autores possuem visões e opiniões distintas, mas complementares, do que está porvir junto a temática Saúde 4.0. Em Matsumoto, Ogawa e Tsuji (2016), já chamava atenção que o *e-health*, vem sendo implementado em muitos países e para que o sistema seja mais difundido, há muitos obstáculos, como *frameworks*, bases econômicas da implementação e outras regulações. Matsumoto, Ogawa e Tsuji (2016) se preocupavam com os sistemas médicos legados estabelecidos na era anterior ao surgimento do *e-health*, se importando por comprovar o custo por efetividade, comparando os benefícios e investimentos.

Essa mesma expectativa em existir obstáculos é disposta em Ćwiklicki, Klich e Chen (2020); Bause *et al*. (2019); Chanchaichujit *et al*. (2019), quanto à Saúde 4.0, no qual reforçam uma necessária mudança de cultura, alfabetização aos ambientes, com ajustes aos novos ambientes, tecnologias e regulamentações, provas de conceitos, aceitação clínica, onde é preciso atrair o médico as novas tecnologias e estes encorajarem os pacientes para utilização cada vez mais das propriedades tecnológicas.

Chanchaichujit *et al*. (2019) explicam que regulamentos rígidos têm demonstrado retardar a inovação e o desenvolvimento de tecnologias. Bause *et al*. (2019) temem a diminuição da produtividade e uma consequente redução da qualidade de serviço com a adoção da Saúde 4.0 até profissionais estiverem capacitados e pacientes familiarizados com os conceitos disruptivos. Bause *et al*. (2019) salientam que pacientes diante de informações pessoais e críticas de forma instantânea podem entrar em conflitos constantes com profissionais médicos gerando atritos e exposições desnecessárias, a chamada soberania do paciente, sobre os dados é um fator preponderante que evolui a discussão junto a prática de tecnologias inerentes à Saúde 4.0. Bause *et al*. (2019) colocam que a personalização a serviços é um fator crescente também junto à Saúde 4.0 e a melhor experiência ao usuário final vai ser colocada como prioridade, onde conforme Chanchaichujit *et al*. (2019) afirmam ser o paciente agora o

principal elemento e não mais a doença. Em um ponto os autores Ćwiklicki, Klich e Chen (2020); Bause *et al*. (2019); Chanchaichujit *et al*. (2019) indicam o mesmo, a implantação dos serviços da Saúde 4.0 reduz custos em saúde.

É consenso que as tecnologias junto aos ambientes de saúde estão evoluindo em integrações diversas para promover a saúde e o bem-estar dos pacientes e tudo que o cerca. Neste documento foi relatado as tecnologias e conceitos atuantes na Saúde 4.0 que são disruptivas e adaptadas ao escopo da saúde. A Saúde 4.0, as tecnologias relacionadas e princípios fundamentais quando aplicados de forma correta beneficiam serviços de saúde e impactam positivamente em fluxos de processos, diminuindo gargalos de atuação, integrando soluções centralizadas, melhoram procedimentos assistenciais, gerenciam melhor plataforma de dados brutos, analisam tendência, compartilham recursos oferecendo também de forma geral, redução dos custos de saúde.

A maneira colaborativa das tecnologias atuantes da Saúde 4.0, os modos de predições existentes quanto ao paciente e o montante de informações são estratégicos e se empregados em composição com os profissionais de saúde e responsáveis por ambientes de saúde são decisivos e podem atuar beneficamente em processos críticos. Tentativas de implantação das tecnologias provenientes da Indústria 4.0 na área da saúde, no entanto, precisam de acolhimento por profissionais de saúde, instituições de saúde, hospitais e paciente. Processos de capacitação, quanto a utilização das tecnologias são considerados críticos e prioritários, legislações e regulamentações também precisam ser adaptadas para não inviabilizar, ou burocratizar processos primários.

2.6 BLOCKCHAIN

Esta seção é norteadora para a tecnologia Blockchain, cerne neste trabalho. Considerada uma das tecnologias presentes no conceito da Saúde 4.0 é primordial na concepção do modelo proposto, sendo utilizada para auxiliar no processo de privacidade dos dados sensíveis do paciente.

2.6.1 Contextualização

O uso de informação sensível é praticado a todo o momento na internet e em vários ambientes computacionais. Os cenários possíveis para utilização de tecnologias que minimizam

e apoiam critérios específicos de segurança surgem para validar a transmissão de informação. Os avanços computacionais propõem uma melhora em cada transação envolvida, mas o uso inadequado de tecnologias ainda impede encontrar o melhor caminho em cada dado envolvido nos processos de comunicação. Acessos não autorizados a sistemas são prerrogativas comuns para investimento em ações que simbolizam certificar a transparência na execução de quaisquer trocas de dados.

Considerando Cert.BR (2019), o número de incidentes em segurança relacionando ambientes que usam tecnologia se mantém preocupante. Aliado a isto, a acelerada ascensão da tecnologia da informação conduziu a sociedade e organizações a terem, cada vez mais, processos, novos e já existentes, dependentes em sistemas computacionais e serviços apoiados na internet.

Um dos momentos marcantes para redefinir conceitos e valores tradicionais sobre segurança em transações na internet acontece depois do surgimento das moedas digitais, que precisam encontrar um modo de assegurar partes de uma transação e considerar seguro realizar troca de dados críticos. As moedas digitais se desenvolvem e intensificam o surgimento de diversas tecnologias e várias lacunas ainda precisam ser preenchidas para assegurar e preservar o tráfego destas informações. Para ter consistência em transações as moedas digitais precisam ter uma forma de corroborar sua existência e validade de transações. A ideia do ambiente seguro e da moeda digital, por Chaum (1981), não é relativamente nova, pois já haviam modelos transacionais, com algoritmos para validações e alguns exemplos que se preocupavam em criptografar os negócios digitais entre os sistemas computacionais, todavia apenas recentemente existe êxito no escopo de segurança que se deve cumprir para estas moedas digitais.

Desde o bitcoin[1] em 2008, várias centenas de criptomoedas foram desenvolvidas e aceitas por uma ampla variedade de transações nos principais mercados comerciais *on-line*, conforme cita Campbell-Verduyn (2018). O bitcoin foi à primeira criptomoeda com utilização em larga escala. Mesmo antes da existência do bitcoin já existiam inúmeras tentativas, tais como protocolos de *e-cashes* (dinheiro eletrônico) com uso de criptografia, mas com dependência de intermediadores. Quebra-cabeças computacionais desenvolvido por Wei Dai (criador do *b-money*) em 1998 foi uma tentativa de criar um consenso descentralizado em transações sendo uma proposta que teve como obstáculo as falhas bizantinas, problema no qual o Bitcoin traz como principal virtude a resolução. As falhas bizantinas, por Antonopoulos (2014), remetem a

[1] Neste documento **b**itcoin será referido à moeda e **B**itcoin a rede com infraestrutura completa e tecnologia.

insegurança das tentativas de criação das redes descentralizadas antes do Bitcoin, pois a dinamicidade da população de uma rede traz à tona possíveis falhas devido à ação de um conjunto de *hosts* que precisa ocorrer sobre alguma decisão computacional, sempre levando em consideração atuações maliciosas e uma resposta a isso. O problema de existir um consenso, neste caso, ocorre na busca ter as condições ideais para validar alguma ação sendo que um número representativo dos *hosts* participantes seja confiável e interessado em processar a informação correta.

Por Nakamoto (2008) e Antonopoulos (2014), nas ações de desenvolver criptomoedas anteriores a bitcoin, *b-money* e *bitgold*, por exemplo, os criadores encontravam problemas apesar das tentativas de tornar estas tolerantes a falhas. As falhas bizantinas geravam problemas como o gasto duplo, ou seja, o valor era gasto duas vezes em diferentes transações, neste caso, usariam as mesmas moedas, isso se devia ao fato de as transações serem copiadas e retransmitidas, abrindo possibilidades ilimitadas de transações ilícitas. Satoshi Nakamoto[2] em 2008 desconstrói o paradigma de centralização, controle das transações em uma entidade somente, propondo descentralizar e delegar as validações para todos os nodos de uma rede, onde em cada operação realizada existe a ciência de toda a rede, não existindo dependência de uma unidade reguladora e sendo os registros praticamente imutáveis, devido ao poder computacional difícil de alcançar para alterar um dado já corroborado por toda a rede.

A rede que suporta as transações do bitcoin traz o conceito de P2P (*Peer-to-Peer* – ponto a ponto), não existindo um servidor central, ou uma unidade de controle. Os computadores nesta rede possuem funções que substituem as ações executadas por uma unidade central. Quando existem transações todos na rede ficam cientes sendo criptografados os dados e colocados algoritmos e poder computacional suficiente para minimizar vulnerabilidades. Na prática essa infraestrutura de rede oriunda junto ao Bitcoin é orientada a situações criptográficas protocolares para que negociações sejam reconhecidas e ratificadas como imutáveis, esse suporte que permite estas transações é chamada de Blockchain (Antonopoulos, 2014; Campbell-Verduyn 2018).

Basicamente, Blockchain são sequências digitais de números codificados em *software* de computador, no qual permitem à troca, gravação e transmissão (*broadcasting*[3]) segura de transações entre usuários individuais que operam em qualquer lugar do mundo com acesso à internet (Campbell-Verduyn, 2018). O Blockchain é uma tecnologia que indica caminhos para

[2] Pseudônimo utilizado pelo indivíduo ou grupo de pessoas que criaram o Bitcoin.
[3] Difusão da informação por toda a rede.

realizar configurações por meio de métodos criptográficos e ações descentralizadas, numa espécie de comunidade de sistemas computacionais onde cada um é responsável por armazenar a integridade de cada transação de todas as entidades contidas nesta comunidade.

Em Chervinski e Kreutz (2019, p.13), “um blockchain é uma estrutura de dados distribuída, formada por uma série de blocos de informação encadeados”, ou seja, um bloco é conectado com o anterior gerando assim uma cadeia. Este bloco constitui múltiplas transações, então são denominados como agrupamento de transações chanceladas com identificadores de tempo, uma impressão digital e uma referência para o bloco anterior. Adicionalmente Crosby *et al.*, (2016) colocam o Blockchain como uma rede com registros de informações distribuídas disposto por blocos encadeados, onde estes dados descentralizados são os registros das transações compartilhadas criando um índice de histórico global. Então, o Blockchain é um banco de transações autônomas e progressivas, com registros das atividades realizadas, isto é, as negociações quando ocorrem são armazenadas e não podem ser excluídas, novas informações sobre qualquer alteração podem existir, mas uma transação inserida e ratificada por toda a rede Blockchain não é mais removida. Não existe uma unidade central que consente as transações, portanto. Os blocos por Zheng *et al*. (2018b); Mizrahi (2015), podem ser manuseados por qualquer participante da rede de validação, tendo as cadeias destes blocos replicações no ambiente Blockchain.

Apesar de tantas afirmações sobre a tecnologia é válido citar Allen *et al*. (2020), quando trazem o Blockchain, como em fase experimental de desenvolvimento e diante de incertezas tecnológicas, econômicas e políticas, mas mesmo assim o Blockchain emerge como o componente principal da próxima geração da Internet, na qual está sendo desenvolvida uma infraestrutura econômica digitalmente nativa. A seguir são estruturadas informações sobre os principais conceitos da tecnologia Blockchain, uma história sobre como surgiu, os investimentos atuais e práticas que acontecem.

2.6.2 Falhas Bizantinas

Falhas Bizantinas também conhecidas como Falhas Arbitrárias são estados em sistemas computacionais, especialmente em sistemas distribuídos, ocorridos em situações onde um ou mais elementos apresentam comportamentos faltosos, podem ser produzidas de forma acidental ou propositadamente, tais como: dados corrompidos, comportamento inesperado de programas, ou códigos maliciosos (Pustišek; Živić; Kos, 2022; Koren; Krishna, 2020; Bambara;

Allen, 2018; Tanenbaum; Steen, 2008; Birman, 1996). Neste ponto é bom entender que conforme Tanenbaum e Steen (2008, p.1) “um sistema distribuído é um conjunto de computadores independentes que se apresenta a seus usuários como um sistema único e coerente”, sendo o Blockchain considerado um sistema de banco de dados distribuído.

Em concordância com Coulouris *et al.* (2012) os sistemas distribuídos apresentam o compartilhamento de recursos como um forte motivo para implantação, e os recursos ofertados são diversos aos usuários, mas existem desafios na construção destes sistemas distribuídos, como o tratamento de falhas. Para Tanenbaum e Steen (2008, p. 195) um “sistema apresenta defeito quando não pode cumprir suas promessas.”, tais compromissos são os serviços oferecidos aos usuários. Estes serviços possuem vários estados, e o que ocasiona um erro nestes estados dos serviços é considerado uma falha, onde a construção de sistemas confiáveis está intimamente atrelada ao controle de falhas. O tratamento de falhas é especialmente complexo em sistemas distribuídos (Coulouris *et al*., 2012).

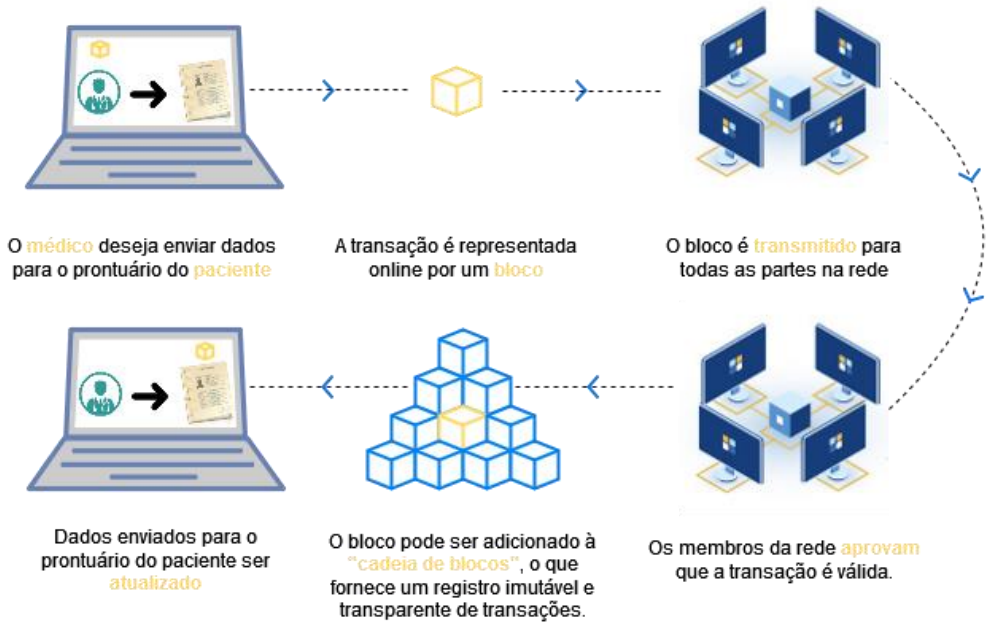
Nos sistemas distribuídos o fator segurança apresenta pontos que podem ser explorados por atos hostis, como a descentralização e a confiança entre os pares. Um componente com falha pode apresentar um tipo de comportamento que é negligenciado e problemático, ou seja, enviar informações conflitantes para diferentes partes do sistema. As falhas que mais comprometem são as falhas bizantinas, também chamadas de falhas arbitrárias. O modelo de falhas bizantinas, abrange estas problemáticas ao ponderar possíveis procedimentos adulteráveis na relação de confiança, pois estes tem potencial para conduzir de modo descabido com intuito de prejudicar o funcionamento de sistemas mesmo em concordância com sua norma (Bambara; Allen, 2018; Tanenbaum; Steen, 2008).

O problema de lidar com esse tipo de falha é expresso abstratamente como o Problema dos Generais Bizantinos e as soluções para a causa são usados no desenvolvimento de implementações de Blockchain. Koren e Krishna (2020) citam, por exemplo, processadores que podem sofrer falhas maliciosas, nas quais produzem saídas arbitrárias e quando os processadores são usados de maneira distribuída, as falhas bizantinas podem causar problemas sutis. Ao tratar sobre o Problema dos Generais Bizantinos no contexto de sistemas distribuídos, são colocados em questão os componentes corrompidos do sistema com sintomas que impedem que outros componentes deste sistema cheguem a um acordo entre eles, ou seja, consenso. Tal acordo é necessário para o correto funcionamento do sistema. A falha bizantina assume qualquer falha que faça com que um componente apresente sintomas diferentes para diferentes partes do sistema (Pustišek; Živić; Kos, 2022).

2.6.3 Funcionamento

O Blockchain é essencialmente um livro público (*ledger*) descentralizado com todos os dados e transações que já foram executados em um sistema. Essas transações são registradas em blocos criados e adicionados à rede Blockchain em uma ordem linear e cronológica (Delgado-Mohatar *et al*., 2020). Estes blocos por Chervinski e Kreutz (2019) na verdade podem ser chamadas de cadeia de blocos de dados que estão ligados uns aos outros por meio de um regramento que utiliza funções *hash* criptográficas. Complementarmente por Lyra (2019) Blockchain é um conjunto de registros transacionais, sincronizados, públicos, distribuídos, de tal forma que o torne independente de um terceiro confiável para validação das operações. O funcionamento da estrutura da corrente de blocos do Blockchain pode ser acompanhado na Figura 3.

Figura 3 – Funcionamento de uma transação com a tecnologia Blockchain.



Fonte: Elaborada pelo autor.

As funções *hash* comentadas são funções matemáticas calculadas a partir de um valor de entrada, onde é inviável computacionalmente encontrar o valor inicial a partir do valor modificado pela função, ou seja, esta função *hash* "mapeia dados de tamanho arbitrário para uma cadeia de bits de tamanho fixo" (Lyra, 2019, p. 23). Na tecnologia Blockchain existem funções *hash* que empregam técnicas criptográficas, no qual possuem importância crítica ao

funcionamento da estrutura de cadeia dos blocos. As funções *hash* criptográficas (resumos criptográficos), por Chervinski e Kreutz (2019), possuem propriedades especiais para garantir a segurança de uma transação na tecnologia Blockchain. Inicialmente ao aplicar uma função para certo dado sempre se deve produzir o mesmo resultado. O resultado chamado de *digest* ou *hash* independente da entrada precisa ser fácil de calcular. Aliado a isto a função *hash* criptográfica deve impedir que a partir do *digest* fosse computacionalmente improvável chegar ao valor de entrada, bem como deve se dificultar gerar o mesmo *digest* a partir de duas entradas distintas (princípio da resistência à colisão). Por fim, deve ser considerado que qualquer alteração na entrada precisa ser condicionada a um novo *digest*, ao tal ponto de não se estabelecer uma relação entre o dado mínimo alterado na entrada com a produção de uma nova saída por este fator alterado, seja somente um caractere (princípio da ocultação).

A partir desta particularidade da função *hash* criptográfica é estabelecido o conceito de imutabilidade, não podem os dados do bloco encadeado serem alterados (Narayanan *et al*., 2016). Uma transação, exibida na Figura 3, contém outras informações inerentes à tecnologia citada, como um carimbo de tempo (comprovação de que os dados existiram naquele momento, assim sendo, inclusos no *hash)* um valor de *hash*, já citado, do bloco anterior e um número aleatório denominado *nonce* de quatro (4) *bytes*, para aferir o valor do *hash*. A partir disto, se alcança a integridade em toda corrente de blocos, pois os números contidos no *hash* são exclusivos e quaisquer alterações nos blocos altera o *hash* (Crosby *et al.*, 2016; Ulrich, 2014).

Como supracitado, um bloco na rede Blockchain para ser construído passa por um algoritmo de consenso que garante a legitimidade das transações deste e sua própria validade. Este mecanismo de consenso em uma rede Blockchain é a PoW (*Proof-of-Work* – Prova de Trabalho). A PoW é utilizada para validar transações e gerar novos blocos para a cadeia. Por meio do emprego da PoW os mineradores (nodos criadores de blocos e validadores de transações), concorrem entre si para completar as transações mais rapidamente e receberem recompensas. A PoW é constituída de enigmas matemáticos e a possibilidade de provar a solução de maneira rápida. Estes problemas matemáticos são custosos computacionalmente e requerem muito do *hardware*. A resposta do problema da PoW a ser resolvida é o *hash* já discutido anteriormente. É importante comentar que a cada 10 minutos, aproximadamente, há um sincronismo e todos os participantes da rede Blockchain concordam com o estado das transações naquele momento, sendo que ninguém na rede se conhece e isso não é necessário, conhecer as partes no qual estão validando as transações, ou seja, isto é a confiança distribuída. Essa confiança faz com que não seja necessário ninguém se conhecer, a própria rede

Blockchain, por meio dos mecanismos de segurança, faz que os participantes atuem de forma correta (Attaran; Gunasekaran, 2019; Pappalardo *et al*., 2018; Milutinovic *et al*., 2016; Crosby *et al.*, 2016; Ulrich, 2014).

A rede Blockchain pode conter qualquer dispositivo eletrônico, incluindo computador, telefone ou até uma impressora, desde que esteja conectado à Internet e possua um endereço IP (*Internet Protocol*). Os dispositivos eletrônicos, na rede Blockchain, são conhecidos como nós ou nodos, e suas principais funções são: i) manter a cópia do Blockchain e ii) validar as transações de retransmissão e copiá-los no Blockchain (Delgado-Mohatar *et al*., 2020). Conforme já citado, quando tais nodos criam novos blocos e consolidam transações já existentes e validadas por meio da rede Blockchain estes são conhecidos como mineradores (Lyra, 2019). O Blockchain então foi projetado com características peculiares, pensando na distribuição do processamento e papel de cada nodo alocado. Para sintetizar o processo histórico, na próxima seção é apresentado o processo de evolução da tecnologia junto às criptomoedas.

2.6.4 Evolução

O Blockchain surge em 2008 como a infraestrutura que suporta o sistema de transações da criptomoeda digital bitcoin (Zhou *et al*., 2018; Crosby *et al*., 2016). A rede Bitcoin então funciona descentralizada, sem autoridade reguladora, permitindo que qualquer um participe da rede e efetue transações. Neste sistema descentralizado, os participantes podem emitir pagamentos uns aos outros sem antes estabelecer confiança entre as partes (Chervinski; Kreutz, 2019). A grande inovação do bitcoin é ser uma moeda digital P2P, mas antes entre os anos de 1980 e 2000 surgiram outras iniciativas: *digicash*, *e-gold*, entretanto todas as iniciativas, além das citadas, possuíam dependência centralizada, ou seja, uma autoridade para validar processos. Então o trunfo revolucionário do modelo de transferência de valor do Bitcoin, desenvolvido e publicado por Satoshi Nakamoto em 2008, é a plataforma que o suporta (Attaran; Gunasekaran, 2019; Lyra, 2019; Ulrich, 2014).

Satoshi Nakamoto estabeleceu a estrutura para a cadeia de blocos e métodos detalhados de uso de uma rede ponto a ponto para gerar um sistema para transações e em janeiro de 2009, foi minerada a primeira transação de bitcoin, o Bloco Genesis, também conhecido como, bloco número 0. Neste mesmo ano o primeiro mercado de troca de bitcoin foi estabelecido em outubro daquele ano, sendo em 2010, a realização da primeira compra de um

produto, com a infraestrutura da rede Blockchain, sendo que a partir de qualquer bloco é possível chegar ao bloco de número 0 (Attaran; Gunasekaran, 2019).

Apesar da técnica implementada é válido ressaltar a intenção de Nakamoto que ressalta a importância do Blockchain sendo livre de uma unidade central, um sistema monetário. Historicamente quando o Bitcoin foi criado, o termo Blockchain não existia. Como os blocos são referenciados uns aos outros por meio da PoW, com tarefas complexas para serem resolvidas que exige poder computacional, antes a tecnologia era chamada por corrente de provas de trabalho e depois veio a se chamar, com a popularização do Bitcoin, em Blockchain (Attaran; Gunasekaran, 2019; Milutinovic *et al*., 2016; Ulrich, 2014).

No surgimento do Blockchain, o intuito era apenas para atender o bitcoin, todavia como a tecnologia se mostrou segura e favorável a outras frentes de desenvolvimento, a aplicação para outros fins que não o bitcoin já vem sendo estudada e praticada. Desde sua aplicação inicial, para o Bitcoin, a ideia original da Blockchain evoluiu bastante em questões de arquitetura (Delgado-Mohatar *et al*., 2020).

Junto à tecnologia Blockchain outros significantes marcos aconteceram aproveitando os conceitos provenientes do estudo de Satoshi Nakamoto em 2008. Swan (2015) expõe que o Blockchain evoluiu se dividindo em gerações distintas. A tecnologia Blockchain 1.0 está atrelada ao conceito de Bitcoin (mineração, *hash* e livro-razão) e diz respeito às criptomoedas e transações financeiras, já a tecnologia Blockchain 2.0 é associada ao Ethereum (*smart contracts*, EVM - Ethereum Virtual Machine e validadores) e oferece uma plataforma para aplicações descentralizadas indo além das transações financeiras simples como pagamentos e transferências, e a tecnologia Blockchain 3.0 se refere a uma vasta gama de aplicativos que não envolvem dinheiro, moeda, comércio, mercados financeiros ou outras atividades econômicas, mas sim, as aplicações incluem arte, saúde, ciência, identidade, governança, educação, bens públicos e vários aspectos da cultura e comunicação, tendo como aplicação mais promissora as cidades inteligentes.

2.6.5 Ethereum

O conceito da Ethereum passa a existir em 2014 por Vitalik Buterin. A Ethereum é uma plataforma descentralizada e arquitetada a partir da Blockchain existente na estrutura do Bitcoin, com o adicional de conceitos como *smart contracts* (contratos inteligentes), aplicativos

descentralizados (DApps - Decentralized Applications) e negócios com a criptomoeda ether e outros *tokens*.

Por Antonopoulos e Wood (2018) cada nodo participante do ambiente Ethereum possui uma máquina virtual, conhecida por EVM, nessa situação tal plataforma concebe uma rede P2P de máquinas virtuais. O Ethereum se diferencia, pois estabelece serviços sobre o conceito Blockchain, como os *smart contracts*, que depois de criados, executam os itens de contrato. Além dos *smart contracts*, por Swan (2018) o Ethereum emprega aspectos diferentes a tecnologia Bitcoin, como diversificação da mineração em um número maior de usuários, transações confirmadas em segundos diferente do Bitcoin que se prolonga por minutos e algoritmo de *hash* próprio chamado *ethash*. Outras considerações igualitárias a plataforma Bitcoin são mantidas, tais como: ser uma rede descentralizada, conceitos de imutabilidade, transparência e privacidade aplicados, inexistência de uma entidade central de validação para os negócios existentes na plataforma, mecanismo de consenso PoW, com possibilidade do PoS (*Proof-of-Stake* – Prova de Participação).

A PoS é um mecanismo de consenso diferente do aplicado no ambiente Bitcoin. A ideia básica, conforme Swan (2018) é que a PoW deixa todos competirem entre si com a mineração concorrente sendo um desperdício. Então a primeira mudança é neste sentido, a PoS usa um processo de eleição no qual um nodo é escolhido aleatoriamente para validar o próximo bloco. Existe uma diferença de nomenclatura, na PoS alterando de mineradores para validadores e isso se reflete no papel desta entidade. Como explica Antonopoulos e Wood (2018), os validadores não são escolhidos por completa aleatoriedade, para se tornar um validador, um nodo necessita depositar certa quantia de moedas na plataforma Ethereum, como se fosse um depósito por segurança, sendo que o tamanho da aposta determina as chances de um validador ser escolhido para gerar o próximo bloco. Este algoritmo de consenso usa uma correlação linear, se dois usuários depositam uma quantidade de moedas na rede Ethereum, mas um destes deposita dez vezes mais, então este tem 10 vezes mais chances de ser escolhido, apesar da aleatoriedade por padrão, sendo mais justo que o PoW, quando comparado ao poder computacional utilizado pelos mineradores no Bitcoin. Quando um nodo for escolhido para validar o próximo bloco, ele verificará se as transações realmente são válidas, para depois adicionar a cadeia de blocos e é notório citar que os nodos validadores perdem uma parte da gratificação da validação se forem aprovadas transações fraudulentas.

O Ethereum está se tornando uma alternativa para aplicações e serviços distintos. Não só os *smart contracts*, mas também as DLTs (Distributed Ledger Technology), e outras formas

de *software* que necessitam de um ambiente escalável, com desempenho ótimo e técnicas de segurança atuais, perante a atualização das hostilidades. Na próxima seção será abordado um conceito complementar aos Blockchains de mercado, as criptomoedas.

2.7 CRIPTOMOEDAS

Conforme Cohen (2004) as moedas digitais são aquelas que dependem da internet para serem transacionadas. Estas são divididas em moedas virtuais e criptomoedas. As moedas virtuais existem em uma comunidade particular, e não precisam ser convertidas em moedas fiduciárias para terem valor, são as conhecidas moedas de jogos de plataforma online, por exemplo, com fins para transações nestes ambientes. Já o termo criptomoeda nasce em 2008, por Satoshi Nakamoto e conforme Hassani, Huang e Silva (2019), está também representa valor e pode ser usada como meio de troca, com a única exceção em ser digital, criptografada e sem formato físico. Criptomoeda, por Hassani, Huang e Silva (2019); Campbell-Verduyn (2018), é uma classificação de moeda digital, descentralizada, no padrão ponto-a-ponto (*peer-to-peer*), sem a presença de intermediadores e empregando criptografia para assegurar as transações, gerir a produção de novas criptomoedas e proteger a identificação dos participantes das transações. É importante perceber que o caráter de segurança é intrínseco as criptomoedas devido ao meio em que estão inseridas. Nas próximas seções são abordadas algumas das criptomoedas existentes considerando CoinMarketCap (2023), importância histórica das criptomoedas e associação com os conceitos originários da tecnologia Blockchain.

2.7.1 bitcoin

A criptomoeda bitcoin surge por meio do artigo de Satoshi Nakamoto e é a primeira a ser utilizada em larga escala e conforme dados da CoinMarketCap (2023) permanecendo mesmo 10 anos depois do surgimento como a mais empregada. A bitcoin utiliza da estrutura original da Blockchain, por Chervinski e Kreutz (2019), e inova trazendo conceitos como a estrutura de validação de novos blocos a partir do esquema de PoW. Aliado a isto existem “[...] esquemas de assinaturas digitais para garantir que os usuários que utilizam moedas realmente as possuem e técnicas de timestamping que marcam a data e a hora da realização das operações” (Chervinski; Kreutz, 2019, p. 19).

Apesar das assinaturas digitais, Nakamoto (2008), indica preocupação com o sistema de segurança ao indicar a necessidade dos nodos serem honestos para que a ação coletiva da rede seja cooperante ao ponto de utilizar o poder computacional para realmente validar as transações. Outro ponto fundamental do ambiente Bitcoin é a descentralização devido ao modelo P2P, aspecto esse citado por Chervinski e Kreutz (2019), como principal contribuição do surgimento desta tecnologia eliminando a obrigação de uma autoridade central para regular, por exemplo, a expedição de novas moedas e a validação de transações.

Um adicional conceito importante, conforme Easley, Ohara e Basu (2019); Chervinski e Kreutz (2019), relacionados à estrutura da rede Bitcoin são os mineradores, pessoas ou organizações com poder computacional, que possuem uma cópia inteira da Blockchain e concorrem entre si para ratificarem transações. Na ocorrência de uma transação os dados dos partícipes são difundidos na rede no intuito em fazer os mineradores validarem. Após a aprovação da transação o minerador introduz um novo bloco na cadeia de dados, tal mineração envolve o uso de *hardware* especializado para encontrar a solução de um complexo problema matemático, com a recompensa pelo sucesso sendo o pagamento, para estes mineradores, com a emissão de novos bitcoins. A quantia de tais pagamentos, e uma variedade de parâmetros, como a dificuldade do problema matemático, até a quantidade total de bitcoins que podem ser extraídos é especificada para cada transação devido a taxas existentes para recompensar mineradores que são variáveis e a importância de cada transação definida por cada usuário.

Além dos mineradores, por Nakamoto (2008) existem os nodos do ambiente e os SPV's (Simplified Payment Verifications - Verificações Simples de Pagamentos). Os nodos também guardam uma cópia inteira da Blockchain e verificam a corretude das transações propagadas, enquanto os SPV´s são participantes da estrutura Bitcoin que não possuem poder computacional para armazenar a cópia inteira da Blockchain, como uma carteira móvel dos *smartphones*, então estes precisam consultar os nodos para trabalhar com as informações existentes na Blockchain.

O bitcoin foi à primeira criptomoeda que gerou confiança para transacionar. A estrutura Blockchain implícita para os participantes fornece um forte controle de propriedade, conforme Nakamoto (2008) entende e propaga que a rede é robusta em sua simplicidade não estruturada. Outras criptomoedas, no entanto surgem para competir com o uso do bitcoin e possuem diferenças de funcionamento.

2.7.2 ether

A criptomoeda junto à plataforma Ethereum, baseada na tecnologia Blockchain, surge em 2015, por Vitalik Buterin. Esta criptomoeda, segundo Buterin (2014) é produzida e utilizada na Ethereum em transações, para pagar os mineradores do ambiente, nos diversos aplicativos existentes da plataforma, nas doações entre usuários e ao trocar por ativos digitais, tais como outras criptomoedas. A ether é considerada por estudiosos como a segunda moeda mais importante na história das criptomoedas.

As transações, por Antonopoulos e Wood (2018) com a ether respeitam as regras da plataforma Ethereum. Para realizar quaisquer negociações os usuários precisam pagar o valor definido com a moeda ether. Apesar de ter um valor econômico, a ether foi desenvolvida para ir além da proposta do bitcoin, sendo então o item no qual habilita o uso da plataforma Ethereum e suas possibilidades de aplicações, como os contratos inteligentes e outros aplicativos baseados na tecnologia Ethereum, não sendo somente uma criptomoeda para enviar e receber valores monetários, mas sim um ativo de recompensa, ou seja, a ether é usada para pagar pelos recursos computacionais (Ethereum Virtual Machine) necessários para executar um aplicativo. Ao usar a EVM, por Antonopoulos e Wood (2018), os usuários necessitam arcar com o custo de uma taxa, denominada Gas, sendo o valor estabelecido na criptomoeda ether. As operações são custosas computacionalmente, por exemplo, para calcular alguma função *hash* o valor estabelecido é em unidade de Gas. Este valor de Gas em ether é mencionado por meio do usuário na transação em si. Dependendo da transação é estabelecido um valor máximo de Gas para a execução da operação.

Os mineradores na plataforma Ethereum, são gratificados em ether. Estes, conforme Antonopoulos e Wood (2018) tem um papel fundamental para o ether, pois conseguem realizar a gestão da moeda consolidando todo ciclo de circulação na transação até a atualização de estado. O minerador é pago com a criptomoeda ether quando o bloco que este é responsável é o primeiro a ser minerado na rede, isto significa que a *Proof-of-Work* foi realizada por ele.

Com relação ao saldo dos participantes das transações, existe a ação condicional no sentido de verificar se o saldo é suficiente para cobrir o custo da transação, neste caso a transação é válida. Por Swan (2018) a conta de origem deduzirá o valor do ether correspondente e a conta do destinatário receberá a quantia. O ether pode ser negociado por contratos inteligentes e a dedução da transação é determinada pelo código escrito com antecedência dentro do contrato inteligente. As transações podem conter dados binários denominados carga

útil (*payload*) e a criptomoeda ether. A carga útil pode não conter informação ou atua como dados de entrada a serem usados na execução do código armazenado na conta do contrato de recebimento. A cada transação no Ethereum existe a assinatura do remetente, o destinatário e o número de criptomoedas do tipo ether enviadas.

Todas as criptomoedas que surgiram após o conceito do bitcoin, como a ether, são chamadas de *altcoins*. Nas duas seções que seguem serão abordadas mais duas destas moedas, respeitando valor de mercado e representação histórica no cenário das criptomoedas.

2.7.3 xrp

A XRP, criada em 2012 é uma criptomoeda que faz parte somente do projeto Ripple, projetado para fornecer meios para troca de moedas, especialmente moedas fiduciárias, sendo útil para transferências com conversões imediatas. Conforme Chowdhury (2019) esta criptomoeda foi concebida inicialmente para as instituições financeiras bancárias melhorarem a eficiência nas próprias transações e com redução de custos operacionais. O projeto desta criptomoeda não foi desenvolvido para servir como moeda independente, mas como parte de uma plataforma que é negociado entre distintas instituições. Em Mauri, Cimato e Damiani (2018) uma das características da criptomoeda e sistema que o cerca é o desempenho perante as outras criptomoedas. Os nodos descentralizados que mantêm o livro-razão do XRP, conhecido como nodos de validação, chegam a um consenso sobre o conjunto de transações a serem incluídas em um novo bloco a ser aprovado em torno de 3 a 4 segundos.

Por Chowdhury (2019) esta criptomoeda não tem a possibilidade de ser minerada, pois isso já aconteceu na implantação da plataforma Ripple criando assim todas as moedas necessárias ao ambiente. A XRP e identificadores de cada usuário são armazenados no livro-razão, além dos saldos, informações sobre ofertas de compra ou venda de moedas e ativos. O processo de consenso, permite usar a XRP para pagamentos, trocas e remessas de forma distribuída. O XRP existe nativamente dentro da plataforma Ripple como moeda livre de contrapartida para as transações possíveis.

Conforme Mauri, Cimato e Damiani (2018) como não existe o conceito de mineradores o XRP é um ativo escasso. No entanto, como a rede Ripple suporta nativamente pagamentos entre moedas, permitindo assim que as partes realizem transações na moeda nativa de cada sistema o intercâmbio entre moedas dentro de rede é facilitado. Em cada transação

enviada à rede é necessária uma taxa de transação especificada na unidade da criptomoeda XRP. Esse custo foi projetado para aumentar com base no volume de transações.

A distribuição do XRP sempre foi um tema de debate. Segundo Chowdhury (2019) o protocolo Ripple cobra um baixo custo de transação. Essa quantia, todavia, não é dada a ninguém, mas é destruída e o protocolo faz isso para impedir a rede de um ataque DDoS (*Distributed Denial of Service*) ou *spam*. Tal prática reduz o número de XRP a cada momento.

2.7.4 Litecoin

A Litecoin (LTC) é uma criptomoeda P2P descentralizada e *opensource*. Perante Gibbs e Yordchim (2014), foi criada por Charlie Lee em 2011 e é baseada na tecnologia Bitcoin, com as mesmas características do conceito Blockchain. A Litecoin também é uma criptomoeda P2P, não utilizando intermediários, descentralizada e sem autoridades centrais. Possui processo de mineração e é a forma de remuneração dos mineradores e unidade básica de valor da rede.

Para Gibbs e Yordchim (2014), o Litecoin apresenta características distintas da plataforma Bitcoin, como a quantidade de criptomoedas disponíveis na plataforma para utilização chegando a ter disponível o quádruplo da quantidade de Bitcoin. Outro aspecto é a velocidade de mineração mais rápida que o bitcoin e o mecanismo de consenso, no qual utiliza a PoW, mas com modificações na função *hash*, sendo denominado esta como *Script*. Conforme Padmavathi e Suresh (2018) a função hash tenta parametrizar os mineradores, nivelando a dificuldade de mineração e permitindo a mineração inclusiva oferecendo oportunidade para *hardwares* com poder computacional não tão grande, tais como utilizados na criptomoeda bitcoin. Este formato de mineração por meio do algoritmo *Script* exige que os processos da PoW sejam feitos sequencialmente e não em paralelo como no Bitcoin, o que permite nodos com poder computacional concorrerem para minerar.

As transações de Litecoin, por Gibbs e Yordchim (2014), são registradas na Blockchain Litecoin, um livro global mantido por a maioria dos clientes, onde são registradas as informações das transações dos pares da internet sem a necessidade de unidade centralizadora. As demais características desta criptomoeda são semelhantes ao bitcoin, como as questões de imutabilidade e demais características da tecnologia Blockchain que armazena as informações do livro-razão da Litecoin.

2.8 TECNOLOGIAS/ABORDAGENS RECENTES

É comum explicar o conceito de Blockchain esclarecendo o funcionamento do Bitcoin, pois estas duas tecnologias estão intrinsecamente atreladas. No entanto, o Blockchain é aplicável a qualquer transação de ativos e trocas *online*. No viés de Zhou *et al*. (2018), o advento das infraestruturas de Blockchain abriram o caminho para um novo domínio de venda de dados, permitindo que proprietários de dados individuais se beneficiem diretamente do compartilhamento de dados proprietários sobre o Blockchain.

Existem estímulos e propostas ao uso da tecnologia *Blockchain* em diversas disciplinas do conhecimento e em localidades distintas, como na Europa, por exemplo, no Reino Unido o governo criou um relatório chamado *Distributed Ledger Technology: beyond blockchain,* propondo melhora de serviços oferecidos pelo governo, indústria, operações financeiras e saúde foram algumas das áreas sugeridas (Government Office for Science, 2016). Um *ledger* é um registro compartilhado de informações, um livro caixa, por exemplo, onde são contidas todas as transações financeiras realizadas. Este conceito junto ao padrão Blockchain permite dissipar todos os *ledgers* distributivamente em uma rede onde a estrutura utiliza os nodos para guardar e replicar os dados. O processo de inovação da tecnologia Blockchain está ocorrendo simultaneamente em muitos setores da economia, finanças, agricultura, comércio e logística, saúde, indústrias e serviços governamentais. Desde o surgimento, houve inovação substancial como os mecanismos de consenso e os contratos inteligentes programáveis em Blockchain (Attaran; Gunasekaran, 2019; Crosby *et al*., 2016; Ulrich, 2014).

2.8.1 Smart contracts

Os *smarts contracts* (contratos inteligentes) surgem como ideia em 1997 por Nick Szabo. Após o advento do *Blockchain* e uma melhora em pesquisas e desenvolvimento o conceito ressurge em 2014 incorporado ao ambiente Blockchain (Lyra, 2019). São basicamente os blocos utilizados para criar aplicações descentralizadas, executado em um ambiente de forma segura, controlando ativos digitais (Delgado-Mohatar *et al*., 2020). Em Lauslahti, Mattila e Seppala (2017), os contratos inteligentes são explicados como protocolos de transação informatizados que executam os termos de um contrato, limitando a quantidade de exceções e demais erros subjetivos, executados automaticamente quando os termos do contrato forem cumpridos e, devido à sua estrutura descentralizada, também são obrigatórios à execução e

invioláveis. Um contrato inteligente reside em um local específico na Blockchain com um endereço exclusivo (Attaran; Gunasekaran, 2019).

Lyra (2019) traz a importância de *smart contracts* anexo ao conceito de Blockchain 2.0, que contempla o Blockchain não atrelado e exclusivo ao Bitcoin com novos recursos incorporados além das criptomoedas. Enquanto o Blockchain original está focado mais na descentralização de moedas, o Blockchain 2.0 visa descentralizar mercados financeiros em geral e com protocolo específico para este fim, o Ethereum. Neste caso, existe um ambiente que aceita apenas sua própria criptomoeda denominada *ether*. Conforme Swan (2015) o modo de funcionamento do Blockchain se mantém, com uma pilha de três camadas: Blockchain, protocolo (Ethereum) e moeda (*ether*), modificando apenas a finalidade principal englobando áreas financeiras e econômicas.

Para estes contratos inteligentes uma série de acordos contratuais computadorizados é consentida por múltiplas partes, podendo ser utilizado para o câmbio de dinheiro, tratativas sobre propriedade intelectual, ou ainda itens quaisquer considerados próprios para negociação. Então não é preciso envolver gestores financeiros, conselhos, tribunais e outros atores habituais nestas ações centralizadores de autoridades. Outras áreas em estudo e desenvolvimento com a tecnologia Blockchain são a saúde no monitoramento de pacientes, indústria da música, quanto a propriedade e direitos autorais no uso da música (Griggs *et al*., 2018; Sitonio; Nucciarelli, 2018; Hasan; Salah, 2018; Ulrich, 2014). A concepção do contrato na rede *Blockchain* é uma organização autônoma descentralizada, por Shermin (2017), governando um grupo de pessoas que compartilham os mesmos interesses e objetivos. Estes são executados de acordo com um conjunto de regras de governança evitando a necessidade de envolvimento do gerenciamento humano.

Os contratos inteligentes têm vantagens, Attaran e Gunasekaran (2019), que se sustentam no funcionamento do Blockchain. Então as características permanecem as mesmas, como a inexistência da necessidade de terceiros, nesse caso os contratos podem ser verificados sem uma autoridade legal. Outra característica importante é a rastreabilidade aprimorada, pois as informações dos contratos inteligentes são armazenadas no Blockchain como todas as outras transações, e os comportamentos são registrados. Aliado a isto existe também a propriedade de melhorias contínuas da tecnologia, devido ao desenvolvimento da tecnologia de forma distribuída, com novos adeptos aumentando.

O *Smart Contract* é um dos conceitos com mais estudos e históricos de validação da tecnologia Blockchain, salvo o *Bitcoin* e outras criptomoedas. Novos cenários estão surgindo

tais como o *OpenBazaar*, similar a serviços oferecidos tais como ao *ebay.com*, e mercadolivre.com.br, sendo uma solução P2P, plataforma *marketplace* e com o suporte da rede Blockchain. Uma nova iniciativa é o *Arcade City*, programado a partir do *Ethereum* (plataforma que usa a tecnologia Blockchain), análogo ao conceito do *uber.com*, mas sem dependências do terceiro regulador, sem o intermediário onerando a tarifa, mas sim a troca voluntária entre dois indivíduos, ou seja, o trâmite acontece entre passageiro e motorista. Demais atividades existem, tais como atividades notariais, titularidades de imóveis de terra, permitindo a independência cada vez maior entre as partes interessadas sem atrelamento a quaisquer órgãos reguladores de processos, com o interesse em minimizar a desintermediação (Ulrich, 2014).

2.9 FERRAMENTAS PARA BLOCKCHAINS (DLTS)

As tecnologias Blockchain ganharam popularidade e inicialmente um dos motivos, era devido à independência de um intermediário e a descentralização dos nodos. Desde então, existe um crescente interesse de diferentes domínios e casos de uso. Uma rede Blockchain pode ser caracterizada com ou sem permissão, então existem as chamadas Blockchains Privadas, diferente das Blockchain Públicas da Internet, pois específicas situações de negócios não necessitam compartilhar de forma pública as transações.

No Blockchain Privado também chamados de *Permissioned Blockchain*, não existe o mecanismo de consenso *Proof of Work*, mas outros são implementados, dependendo das empresas ou consórcio de organizações que estão como mantenedoras destes referidos projetos. Em alguns casos existem mais de um mecanismo privado de consenso, estes são conhecidos por usarem a DLT (*Distributed Ledger Technology* – Tecnologia de Ledger Distribuído) (Lyra, 2019; Shermin, 2017). Estas arquiteturas privadas DLT, foram criadas com uma particularidade diferente ao Blockchain do Bitcoin, pois os nodos neste caso são conhecidos na rede. A grande diferença é o sistema, mecanismo de consenso do Blockchain, existente no Bitcoin, *Proof of Work* (prova de trabalho), computacionalmente criada por meio dos mineradores, comprovando que determinada transação é válida (Lyra, 2019; Thakkar; Nathan; Viswanathan, 2018; Ulrich, 2014). Existem autores que trazem a importância em desvincular Blockchain Público de Blockchain Privado comentando que Blockchain do tipo privado devem ser chamados de DLTs (Tecnologia de Ledger Distribuído).

Brown (2018) indica o contraste do Blockchain com as DLTs devido à necessidade de uma abordagem à privacidade. Em algumas situações é cogente trabalhar com dados

confidenciais ou canais mais rigorosos. Esses projetos logicamente não possuem interesse em suportar uma rede global que concerne vários aplicativos e ativos interoperáveis. O objeto é um documento digital que registra a existência, o conteúdo e o estado atual de um contrato entre duas ou mais partes. Destina-se a ser compartilhado apenas com aqueles que têm uma razão legítima para visualizá-lo. Neste caso, o propósito de funcionamento distribuído continua, mas como pode ser atrelado a organização particulares com dados críticos a entrada de qualquer participante na rede deve ser autorizada e determinada sobre regras intrínsecas de cada implementação. Com este diferente propósito de arquitetura DLT, novas tecnologias surgiram para implementar esse conceito similar, mas diferente de uma rede originalmente Blockchain.

2.9.1 Corda

O Corda (corda.net), do consórcio R3 (r3.com) com mais de 70 instituições financeiras é uma solução *opensource* e com o foco para a indústria financeira. Valenta e Sandner (2017); Thakkar, Nathan e Viswanathan (2018) tratam o Corda, como um *ledger* distribuído para o registro, gerenciamento e execução de contratos financeiros, entre corporações, instituições financeiras e clientes, ou seja, só quem realmente é legítimo e está envolvido no processo possui acesso e interage com todo o ambiente.

Conforme Hearn e Brown (2019) o Corda tecnicamente possui diferenças significativas do Blockchain original. O Corda emprega o protocolo *need-to-know basis protocol*, que distinto ao Bitcoin (usa *gossip protocols*), encaminha mensagens apenas para quem está envolvido na transação, isto é conhecido por *privacy by design*, diverso da visão do Blockchain implementado junto ao Bitcoin com os membros possuindo uma cópia das transações, mesmo não fazendo parte desta. Em relação ao funcionamento, algumas questões são elementares que distinguem a tecnologia Corda. No Quadro 4, por Hearn e Brown (2019), são listados os componentes de uma rede Corda, a saber.

Quadro 4 – Elementos de uma rede Corda.

ELEMENTO	DESCRIÇÃO
nodes (nodos)	Nodos comunicando usando protocolo AMQP 1.0 (*Advanced Message Queuing Protocol*) sobre TLS (Transport Layer Security).
identity (identidade)	Serviço de identidade que executa uma autoridade de certificação com padrão de criptografia X.509.
network map services (serviço de mapa de rede)	Serviço de mapa de rede que publica informações sobre como conectar-se a nodos na rede.

Continua...

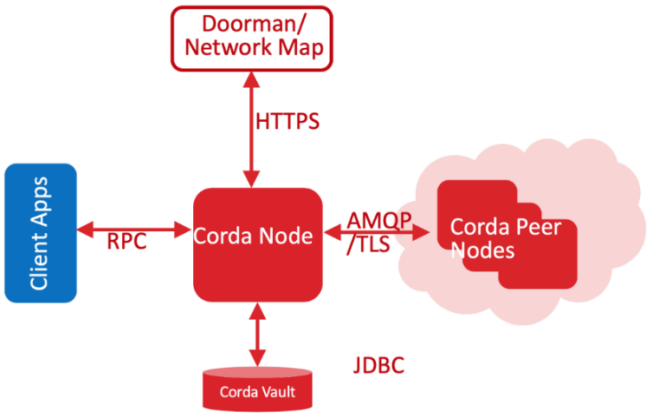
ELEMENTO	DESCRIÇÃO
notary services (serviços notariais)	Pode existir um ou mais serviços notariais dependendo da divisão e negócios na redes com Corda.
oracle services (serviços *oracle*)	Podem existir ou não os serviços *oracle*, no qual declaram um fato como verdadeiro.

Fonte: Elaborado pelo autor.

Além dos elementos citados, a estrutura do ambiente possui uma técnica que identifica os integrantes da rede e a cada entrada de um novo integrante autorizada, um evento de atualização da relação de participantes ocorre. Os serviços no ambiente Corda disponibilizados são conhecidos como *notary pools* (conjuntos notariais) e cada um deles podem oferecer diferentes recursos de validação para as transações. Em uma transação no ambiente Corda a validade do processo é realizada entre os *notary nodes*, nodos da transação.

O Corda associa um nome em união a uma chave pública e endereço de rede dos nodos, nas transações com importância para os nodos observadores regulatórios e supervisórios, tipos possíveis de nodo em uma rede Corda. As negociações são validadas a partir de um serviço chamado *notary service* que além de corroborar a transação aplica técnicas para garantir a não-duplicidade. Outra característica do Corda, não existente na tecnologia originária do Blockchain é a possibilidade de execução das transações em uma determinada janela de tempo, podendo então as negociações ocorrerem com hora marcada, ou restringir para horários com monitoramento (Holbrook, 2020; Brown, 2018; R3, 2018). Os componentes do Corda, e protocolos de comunicação que o Corda emprega em suas operações são representados na Figura 4, considerada como uma visão geral do Corda.

Figura 4 – Visão geral da tecnologia CORDA



Fonte: R3 (2018).

Na Figura 4 é possível visualizar os nodos da rede Corda, estes se comunicam usando um protocolo assíncrono, AMQP (Advanced Message Queuing Protocol) / TLS (Transport Layer Security). Pode ser, por R3 (2018), identificado também uma comunicação com o protocolo HTTPS (Hypertext Transfer Protocol Secure), de uso para o registro inicial de cada nodo e para o compartilhamento dos locais de endereço dos nodos por intermédio do Mapa de Rede. Rede permitida para identidades conhecidas de nós adicionadas por meio do serviço Doorman. Os aplicativos cliente, por Holbrook (2020), que precisam de comunicação com os nodos realizam isto utilizando chamadas RPC (Remote Procedure Call).

Os nodos Corda podem executar vários CorDapps (Corda Distributed Applications). Cada CorDapp pode ser personalizável como o Código do Contrato e Fluxos para diferentes casos de uso. As transações para o aplicativo são personalizadas para cada caso de uso e permitem especificamente o alinhamento de grandes transações. É válido comentar que quando uma transação é proposta, ela é enviada apenas às partes que precisam saber (via protocolo AMQP ponto a ponto) e coleta assinaturas para essa transação. Todas as partes envolvidas realizam um consenso em tempo real. O serviço *notary service* fornece a exclusividade, a validação e o carimbo de data e hora para evitar gastos duplos (Holbrook, 2020; R3, 2018).

Como supracitado a tecnologia Corda restringe comunicações dos nodos de sua estrutura. O acesso ao nodo Corda na Internet ocorre apenas para nodos com certificados de identidade válidos. Outras características como a não exigência de criptomoedas, pois o consenso não é alcançado via mineração, distinguem o modelo de funcionamento com estruturas Blockchain (Holbrook, 2020; R3, 2018). Na seção seguinte será abordado outra estrutura DLT que surgiu a partir dos conceitos e propósito idealizado do padrão Blockchain.

2.9.2 Hyperledger

Outra solução considerada um padrão de Blockchain Privado é o Hyperledger (hyperledger.org), mantido pela Linux Foundation, mas com várias empresas que contribuem assiduamente no desenvolvimento da tecnologia. É uma solução com foco em áreas como cadeia de suprimentos, logística, saúde e áreas de seguros. Em Ban, Anh e Son *et al.* (2019) se enumera cinco (5) subprojetos, *frameworks*, Hyperledger: Fabric (IBM), Sawtooth (Intel), Indy (Sovrin), Burrow (Monax) e Iroha (Soramitsu). Cada projeto deste é originário de uma empresa que apoia a Linux Foundation, sendo o Fabric, o projeto mais maduro e ativo. Todos os projetos

Hyperledger seguem uma filosofia de estrutura que inclui uma abordagem extensível modular, ou seja, na medida da extensão do projeto, novas funções são incorporadas, a interoperabilidade com outros DLTs, a abordagem independente de *token*, ou seja, sem criptomoeda nativa e o suporte a diversas integrações com aplicativos externos.

Os componentes básicos das estruturas Hyperledger são comuns a todos os projetos. Um registro distribuído, ocorrendo somente acréscimos, um algoritmos de consenso para confirmar as alterações no registro, privacidade de transação por meio da configuração de permissões de acesso (Blockchain privada ou híbrida) e contratos inteligentes para processar solicitações de transação. No entanto, a partir disto as estruturas são diferentes com fluxo de trabalho próprio. No Quadro 5 resumidamente são exibidos os projetos Hyperledger supracitados com as principais características.

Quadro 5 – Frameworks Hyperledger

	CONSENSO	**REDE**	**TRANSPARÊNCIA**
Fabric	Kafka	Privada	Transações apenas para os canais participantes
Sawtooth	*PoET*, *PoET Simulator,* Dev_mod, Raft	Privada	Todo nodo possui acesso de leitura na rede.
Indy	*PBFTP*	Privada com acesso público	Todo nodo possui acesso de leitura na rede
Burrow	*Tendermint*	Privada	Todo nodo possui acesso de leitura na rede, mas pode ter restrições.
Iroha	Sumeragi	Privada	Todo nodo possui acesso de leitura na rede, mas pode ter restrições.
Besu	Ethash e IBFT	Privada	Transações apenas para os canais participantes

Fonte: Elaborado pelo autor.

Cada projeto tem um propósito diferente, até mesmo porque, são mantidos por instituições distintas e com clientes, investimentos, desenvolvedores e propósitos distintos. Nas próximas seções são detalhadas mais de cada subprojeto Hyperledger.

2.9.2.1 Fabric

Por Ban, Anh e Son *et al.* (2019) o Hyperledger Fabric é o primeiro *framework* para Blockchain permissionado, ou seja, os participantes se conhecem, mesmo que não exista confiança entre estes. Este subprojeto Hyperledger não possui uma criptomoeda nativa para que exista a mineração. O Hyperledger Fabric utiliza uma interface exclusiva para contratos inteligentes denominada *chaincode*, este explica as instruções da lógica de negócios, no qual o cerca, para quaisquer intervenções. A única forma de interação com um *chaincode* são então as

transações. Todas as transações na rede precisam ser corroboradas, sendo que somente essas podem ser consideradas como realizadas. Os *chaincodes* podem ser utilizados em uma nova transação e serem inclusos em uma rede de transações após a corroboração da ação ou podem também ser referenciados quando forem invocados para uma específica função que algum cliente solicitar em certo contexto. O Hyperledger Fabric é caracterizado principalmente por ser modular, acoplando os módulos quando necessário. É o que ocorre com as funções de consenso, gerenciamento das ingressões de nodos nas redes, e funções de transação.

No Hyperledger Fabric as transações são privadas e os nodos mineradores precisam ser verificados na rede. As entidades estão descritas no Quadro 6 (Valenta; Sandner, 2017; Thakkar; Nathan; Viswanathan, 2018).

Quadro 6 – Descrição e características das entidades

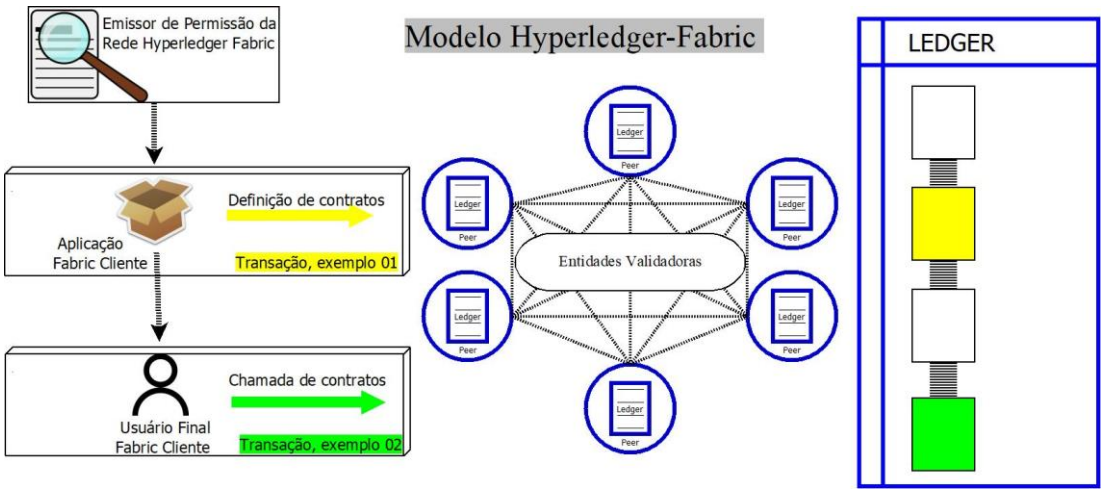
ENTIDADE	DESCRIÇÃO
Nodos	Uma cadeia de "blocos Fabric" abrange um conjunto de nodos que formam uma rede. Todos os nodos participantes da rede adquirem uma identidade a partir do MSP (*Membership Service Provider* - Fornecedor de Serviços para Membros), que fornece e gerencia a identidade dos nodos de uma organização em específico. Os nodos, assim podem ser classificados em: *clients* (cliente) – submetem transação propostas para serem executadas e transmitidas; *peers*– executam as transações propostas e validam as transações, sendo que todos os *peers* mantém o registro, mas somente nodos específicos (nodos de consenso) que avaliam as transações; e *ordering service nodes* (nodos do serviço de ordenação) – estabelecem a ordem de todas as transações.
Blocos	Os blocos são transmitidos a todos os pares e possuem três segmentos: cabeçalho, dados e metadados.
Transações/Contratos Inteligentes (*Smart Contracts*)	Lógica de transação que vai permitir uma transação executar, as regras, de quem participa da rede, qual o ativo a ser transacionado e qual é a transação. Um *smart contract* no Fabric é denominado de *chaincode*. Após a execução, as transações entram na fase de pedidos que emprega um protocolo de consenso conectável (*plug and play*) para produzir uma sequência ordenada de transações aprovadas e agrupadas em blocos. Cada transação contém o estado atualizado e dependências junto às assinaturas criptográficas dos pares que aprovaram a transação.
Channels (canais de transação)	Definição lógica entre dois ou mais pares. Se existem pares que decidem executar uma transação é criado um canal entre eles.
Consenso	O Hyperledger Fabric utiliza mecanismos de consenso escaláveis e adaptáveis, e quem desenvolve consegue escolher de acordo com a necessidade. O Hyperledger Fabric possui algumas possibilidades então, como o algoritmo Kafka. Este algoritmo apresenta a abstração de uma fila compartilhada, sendo que os nodos precisam concordar com a mesma ordem de transações. O nodo que tem a responsabilidade de ordenar lê os blocos do seu sistema de arquivos e os envia para os pares. Quando o par recebe os blocos, ele também os envia para outros pares o que garante a sincronia.

Fonte: Elaborado pelo autor.

Os contratos inteligentes existem nos *peers* e, após, instanciados em canais de transação. Obrigatoriamente todos os membros que almejam enviar transações ou ler dados

consumindo um contrato inteligente devem instalar o contrato em seu *peer*. Após a instalação o contrato é instanciado por um único membro no canal de transação e o livro razão é atualizado. Na Figura 5 é visto um resumo das entidades e forma de funcionamento do Hyperledger *Fabric*.

Figura 5 – Resumo dos recursos oferecidos pelo Hyperledger Fabric.



Fonte: Adaptado de Dhillon, Metcalf e Hooper (2017).

Conforme Figura 5, se pode perceber que em um ambiente Hyperledger Fabric os nodos recebem transações de clientes, tais clientes podem ser exemplificados por aplicativos de dispositivos smartphones e dispositivos de dentro de uma organização. Existe uma prévia para verificar a identidade, credenciais de acesso, do participante da transação. Após isso os nodos que organizam definem a transação em um bloco e os participantes da rede, ficam cada um com uma cópia, atualizando o estado das transações para cada um. O Fabric é o projeto mais conhecido da família Hyperledger possuindo inúmeras ferramentas de conciliação dos livros-razão distribuídos e serviços acopláveis (Dhillon; Metcalf; Hooper, 2017). Além deste, existem outros *frameworks* que a partir da próxima seção serão descritos.

2.9.2.2 Sawtooth

O subprojeto Hyperledger Sawtooh, abordagem inicialmente da Intel para Blockchain, em Chowdhury *et al*. (2019), possui características elementares, como não ter tolerância às falhas bizantinas, ser o único da família Hyperledger com capacidade de configurar um Blockchain Público, sem tratativas de permissão e utilizar mais de uma implementação de consenso apesar de ter como padrão, o Proof of Elapsed Time (PoET). Neste tipo de consenso,

cada um dos nodos envolvidos na aprovação da transação recebe aleatoriamente um tempo de espera, o nodo que possuir o menor tempo de espera, será o que aprovará a transação.

O Hyperledger Sawtooth é tido como utilizador de recursos mínimos de consumo e em larga escala. Apresenta arquitetura modular e integrações com outros subprojetos Hyperledger, sendo tal arquitetura composta por cinco componentes centrais: 1) uma rede P2P para transmitir mensagens e transações entre os nodos; 2) um registro distribuído que contém uma lista ordenada das transações; 3) uma camada lógica de máquina de estados para os contratos inteligentes com intuito de processar o conteúdo das transações; 4) um armazenamento distribuído dos estados, para guardar o resultado posterior ao processamento das transações; 5) um algoritmo de consenso para obter consenso em toda a rede, ordem das transações e o estado resultante (Olson *et al*., 2018).

Detalhando a arquitetura e estrutura de funcionamento é válido mencionar que os nodos dos ambientes Hyperledger Sawtooth se comunicam enviando mensagens uns para os outros (para todos da rede) com informações sobre as transações e blocos, mantendo o padrão da tecnologia Blockchain originária no Bitcoin. Apesar disso o Hyperledger Sawtooth suporta redes permissionadas por intermédio das listas de controle de acesso, com informações sobre quem pode se conectar à rede, quem pode enviar mensagem sobre o consenso e participar do processo de consenso, e quem pode visualizar os estado das transações (Chowdhury *et al.,* 2019; Olson *et al*., 2018).

Conforme já citado, quanto ao consenso, o Hyperledger Sawtooth, tem quatro (4) cenários, por padrão é ofertado o PoET (Proof of Elapsed Time – Prova do Tempo Decorrido) – este consenso caracteriza-se por um nodo líder ser eleito por meio de uma loteria, situação na qual todos os nodos possuem a mesma possibilidade de encontrar um bloco. Durante cada descoberta de bloco, o nodo precisa aguardar por um intervalo de tempo aleatório e quem registrar o menor tempo é o responsável pelo próximo bloco (Chan; Abdullah; Khan, 2019).

Uma crítica a este algoritmo recai sobre a dependência de *hardware*, pois só é executado sobre *hardware* específico da Intel. Para isso ser minimizado existe como possibilidade o Simulador PoET, que permite o mesmo consenso PoET sob qualquer *hardware* e em um ambiente em nuvem e virtualizado. Além deste padrão existem outras possibilidades de consenso. O *dev_mode* é uma alternativa de consenso para este framework, ele é um mecanismo exclusivo para testes de desenvolvedor. Existe também o mecanismo de consenso denominado Raft, também utilizado por outros frameworks Hyperledger (Chowdhury *et al.,* 2019; Olson *et al*., 2018).

Conforme Chowdhury *et al.* (2019); Olson *et al*. (2018) esse protocolo é tolerante a falhas de parada e trabalha com a ideia que todos os nodos se conhecem não existindo a possibilidade de falhas bizantinas no ambiente. É um algoritmo que funciona no estilo de uma eleição, quando cada nodo pode se tornar um candidato se não receber uma resposta de um nodo líder em um intervalo de tempo arbitrário. Caso não existam líderes no processo, os candidatos então solicitam votos de outros nodos e com mais da metade dos votos estes se tornam líder e conseguem acrescer um bloco ao final da cadeia. O líder nesse caso se propõe a manter os registros atualizados das transações e os outros nodos devem aceitar estes registros para manter a consistência da cadeia. Por fim vale reforçar o Hyperledger Sawtooth como um livro-razão distribuído que acopla uma variedade de algoritmos de consenso, isto é importante para tratar diversas transações de diferentes espécies, o que o torna extremamente customizável.

2.9.2.3 Indy

Desenvolvido inicialmente pela Sorvin Foundation, conforme Hyperledger (2019) o Indy é um projeto DLT Hyperledger criado para oferecer suporte à identidade independente em *ledgers*, com ferramentas, bibliotecas e componentes reutilizáveis que possibilitam o gerenciamento descentralizado destas identidades. O Hyperledger Indy é considerado um Blockchain permissionado com acesso público, se necessário tem possibilidade de permissões e regras na estrutura, sendo que os membros (nodos) registrados gerenciam sua própria identidade com possibilidade de ler o conteúdo da Blockchain. O livro razão é mantido pelos nodos, que executam como consenso o PBFTP (*Plenum Byzantine Fault Tolerant Protocol*) para concordar com a ordem das transações no livro razão (Soltani, 2018).

O Hyperledger Indy possui um funcionamento diferente para armazenamento de informações, em vez de armazenar os dados no livro-razão e fornecer acesso ao uso de dados, o Hyperledger Indy induz os usuários a guardar os dados por conta própria e a manter a privacidade dos dados. Para Soltani (2018), a principal característica do Hyperledger Indy é o DID (*Decentralized Identifier* - identificadores descentralizados), eles são globalmente únicos e independentemente resolvíveis sem exigir nenhuma autoridade centralizada, para registrar, resolver, atualizar ou revogar os identificadores.

O DID é criado, por meio do fornecimento inicial pelo usuário de algum dado de identificação única, depois disso, a informação intrínseca ao usuário é convertida em um código ou chave exclusiva, tal qual chamado de Identificadores Descentralizados (DID) no livro-razão.

Cada DID possui um DDO (DID *descriptor object*), e com o uso do DDO os usuários adquirem um canal privado criptografado à entidade correspondente e através desses canais criptografados, as entidades podem trocar livremente credenciais verificáveis entre si. A criptografia por trás do DID é conhecida como infraestrutura de chave pública (PKI) e como os DIDs residem em uma contabilidade pública distribuída, pode-se definir que tal arquitetura referencia conceitualmente uma PKI descentralizada (DPKI) indicando a armazenagem descentralizada de dados dos valores-chave (Hyperledger, 2019; Soltani, 2018).

A arquitetura do *framework*, Soltani (2018), constitui de uma estrutura elementar formada por nodos validadores, agentes e carteiras digitais. Os nodos validadores são responsáveis por executar o algoritmo de consenso PBFTP. Os agentes são *softwares* designados para agir em nome dos proprietários da identidade (por exemplo, usuários) para interagir com outros agentes. Os agentes normalmente têm acesso a uma carteira digital para armazenar chaves criptográficas e executar operações criptográficas. Além destes existe o nodo validador, entidade com permissão para registrar novos identificadores no livro-razão. O Projeto Indy está em constante desenvolvimento por intermédio da Linux Foundation e suas propriedades e características tendem a seguir a descentralização das identidades.

2.9.2.4 Burrow

Este subprojeto Hyperledger, foi iniciado pela Monax e Intel em 2014 e representa a adaptação dos contratos inteligentes da Blockchain *Ethereum* para uso em redes corporativas, permissionado. Em Chowdhury *et al.* (2019) o Hyperledger Burrow se difere dos outros subprojetos Hyperledger, pois o foco é a execução dos contratos inteligentes a partir da Ethereum Virtual Machine (EVM), oriunda da tecnologia de Blockchain Ethereum. Por Saraf e Sabadra (2018) o Hyperledger Burrow apresenta elementos distintos na arquitetura: módulo cliente a partir da EVM, que executa contratos inteligentes em um ambiente com funções e ações definidas por usuário; o mecanismo de consenso de *Tendermint*, tolerante a falhas bizantinas com característica específica de tornar desnecessária a mineração, devido ao processo de escolha dos nodos validadores por votação; Aplicação de Contrato Inteligente, neste caso o código do contrato inteligente está incluso em cada conta do Hyperledger *Burrow*, implícito aos nodos, sendo executado a partir da chamada do cliente na EVM; Interface de Aplicação Blockchain - Application Blockchain Interface (ABCI), como interface entre o mecanismo de consenso e a aplicação de contratos inteligentes; e uma Interface Binária de

Aplicativo – Application Binary Interface (ABI), utilizada para compilação, implantação e vinculação de contratos inteligentes, além de fornecer a opção de chamada de transações e chamadas para outros contratos inteligentes.

É válido citar, em Saraf e Sabadra (2018), que o mecanismo de consenso *Tendermint* (também chamado de *Proof of Stake*) é rápido na execução, pois não exige cálculos de *hash*, utilizando um sistema de votação entre os nodos que já são conhecidos em determinada rede. O algoritmo de consenso consiste em três (3) partes para adicionar o bloco à cadeia. Primeiro o proponente deve propor a transação e ficar visível para todos os validadores no prazo estipulado, senão, a proposta é descartada. Após isso, existem duas fases de votação chamadas, pré-votação e pré-confirmação, quando mais de dois terços dos validadores pré-votam no mesmo bloco, se denomina como polca e toda pré-confirmação deve ser justificada por uma polca na mesma rodada. Este modelo de consenso possui falhas, tal como, todo o sistema pode parar se um terço ou mais de um terço dos validadores estiverem sem comunicação. O projeto Burrow possui o estado de incubado e tem vantagem por usar a maturação do Blockchain Ethereum podendo integrar os contratos inteligentes das duas tecnologias, aliado a isto utilizar um mecanismo de consenso constitui a não necessidade de configurações robustas de *hardware* (Chowdhury *et al*., 2019; Saraf; Sabadra. 2018).

2.9.2.5 Iroha

Este subprojeto Hyperledger surge em 2016 por meio da empresa Soramitsu, com base no desenvolvimento do Hyperledger Fabric, com indicação para gerenciar ativos digitais, tais como criptomoedas, dados médicos pessoal, números de séries, patentes e também dispositivos IoT (Ban *et al.,* 2019; Podgorelec; Kersic; Turkanovic, 2019). É um Blockchain permissionado, com restrições a participação de usuários, Khan *et al*. (2021); Ban *et al*. (2019) explicam para este Hyperledger como mecanismo de consenso o Sumeragi que define o YAC (Yet Another Consensus), algoritmo de consenso descentralizado com tolerância a falhas bizantinas, funcionando com base na reputação de pares para escolher a ordem no qual os nodos processam as transações, no entanto, existe possibilidade do uso da Prova de Trabalho – Proof of Work (PoW), como algoritmo de consenso.

Em se tratando de arquitetura, por Ban *et al.* (2019), esta é composta por 4 (quatro) camadas, a saber: API *level*, fornece a interface de entrada e saída para clientes; *Peer interaction level*, toda e qualquer interação com a rede de pares; *Chain business logic level*, simulador para

captura do estado atual das transações e validação destas, com verificação sobre as regras de negócio e a validade de transações ou consultas; *Storage Level*, denominado como Ametsuchi, sendo o componente de armazenamento, que armazena blocos e um estado gerado a partir dos blocos, chamado World State View.

Para as transações existem alguns conceitos. O Hyperledger Iroha suporta o modo de interação *push* e *pull* com um cliente. Um cliente que usa o modo *pull* solicita atualizações sobre o estado das transações dos pares, enviando *hashes* de transações e aguardando uma resposta. Por outro lado, *push*, a interação é feita por meio da escuta de um fluxo de eventos para cada transação. Em qualquer um desses modos, o estado da transação é o mesmo (Khan *et al*., 2021; Ban *et al*., 2019).

Estas transações podem acontecer por meio de lotes, com o envio de várias transações, ocorrendo o pedido de uma só vez e o lote pode conter transações criadas por contas diferentes. Já os dados da transação são permanentemente registrados em arquivos chamados blocos, tais blocos são organizados em uma sequência linear ao longo do tempo. Os blocos são assinados com as assinaturas criptográficas dos pares da estrutura de ambiente do Hyperledger Iroha e o conteúdo assinável é chamado de carga útil, portanto, a estrutura de um bloco consiste em carga útil externa (*hash*, assinaturas) e interna (altura, registro de data e hora, corpo, quantidade de transações, *hash* anterior) (Khan *et al*., 2021; Ban *et al*., 2019; Podgorelec; Kersic; Turkanovic, 2019).

Em se tratando dos tipos de nodos, Ban *et al.* (2019), explicam que existem três em uma rede *Hypperledger* Iroha. Os clientes, que podem consultar dados, executar uma ação ou transação de alteração de estado. Os pares, que mantém o estado atual e sua própria cópia do *ledger* compartilhado, sendo que um par é uma entidade única na rede e tem um endereço, identidade e confiança. E por fim, o serviço de pedidos, para integrar e realizar transações de pedidos conhecido.

2.9.2.6 Besu

O Hyperledger Besu, desenvolvido pela Pegasys, estende a tecnologia do Blockchain Ethereum, adicionando recursos como privacidade e permissão para criar redes Blockchain adequadas para consórcios e ambientes privados. Por Hasan *et al.*, (2020) o *framework* possui a especificação EEA (*Enterprise Ethereum Alliance*), que visa padronizar as interfaces a serem usadas em projetos desenvolvidos com o Blockchain Ethereum de forma a serem

interoperáveis. O Hyperledger Besu utiliza também a EVM (*Ethereum Virtual Machine*), que permite a implantação e execução de contratos inteligentes. Algumas vertentes do Hyperledger Besu são os contratos inteligentes e os *dApps*, aplicativo descentralizado em ambientes P2P, como o Blockchain. Ele permite que a privacidade seja implementada, gerenciando transações privadas entre duas ou mais partes envolvidas, sem que o restante possa acessar o conteúdo das transações (Hyperledger Besu, 2019).

Conforme Hyperledger Besu (2019) esta ramificação do Hyperledger possui dois tipos de nodos: *full node*, permite enviar e assinar transações, verificar saldos atuais e acessar o atual estado da rede; e os *archive nodes*, que além de executarem as mesmas funções dos *full node*, adiciona a propriedade de guardar o último estado da rede, armazena também os estados intermediários de cada conta desde o bloco original de transação, ainda assim, permite trabalhar com diferentes protocolos de consenso, como: Ethash (protocolo de consenso do tipo PoW) e IBFT 2.0 (protocolo de consenso PoA). Uma das características deste Hyperledger, tal como outros é a capacidade de gerenciar transações privadas entre os participantes envolvidos, sem que os outros participantes da rede possam ver nem o conteúdo dessas transações nem a lista de participantes envolvidos nessas transações. Este Hyperledger está sendo referenciado para ambientes presenciais em específico para gerir consórcios de empresas.

Foram apresentados seis *frameworks* Hyperledger com detalhamento para as formas de consenso, como praticam as transações, informações importantes do funcionamento dos nodos e as validações dos processos. Nas próximas seções serão são referenciados outros tipos de DLTs que trabalham com conceito da Blockchain.

2.9.3 Quorum

O Quorum, conforme Espel, Katz e Robin (2017), mantido pela J. P. Morgan com apoio da Microsoft, foi lançado em 2017 com objetivo de implementar com permissões o protocolo Ethereum e ofertar a privacidade nas transações e contratos de Blockchain. Com a vantagem de utilizar a maturidade do projeto Ethereum, conforme Baliga, Kamat e Chatterjee (2018), o Quorum fornece suporte ao conceito de confidencialidade devido ao suporte de transações públicas e privadas, entrega um ambiente permissionado com alternativas, se necessário for, somente participantes pré-definidos acessam a rede. Respeitando a origem do conceito Blockchain, o Quorum é descentralizado sem dependência de um serviço centralizado

ou sem a dependência alocada a um participante da rede. O Quorum possui ambiente permissionado com controle de quais nodos podem se conectar a outros nodos de rede.

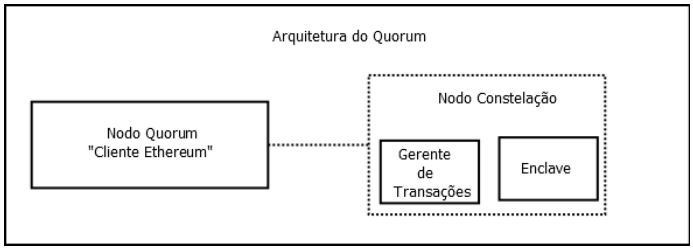
Como mecanismo de consenso é possível, conforme Baliga, Kamat e Chatterjee (2018), usar distintos dependendo do negócio a ser implementado e estes são baseados em mecanismos de votação, ao invés da *Proof of Work*. Além de resolver problemas de privacidade, isto melhora o desempenho que Blockchains públicos como Ethereum possuem e isso é cooperado com o tipo de mecanismo de consenso se utiliza nos ambientes Quorum. Então o Quorum emprega um enfoque diferente com relação ao consenso, utilizando o consenso com base na votação por maioria, sendo que nem todos os nodos possuem a permissão para votar.

Para Baliga, Kamat e Chatterjee (2018) o Quorum usa modelos fundamentados no Istanbul BFT e no Raft. O Raft é um protocolo de consenso que tolera a falhas de parada, neste caso todos os nodos são conhecidos não existindo necessidade de resolver o problema das falhas bizantinas. Os nodos podem possuir três estados: líder, seguidor ou candidato, sendo que o líder aceita o ingresso do cliente, replica tais ingressões em outros nodos além de gerir os estados dos nodos. O termo seguidor se refere a nodos que somente respondem solicitações de interações a pedidos do líder e dos candidatos, já o nodo candidato possui função de eleger um novo líder quando necessário. O IBFT é um algoritmo de consenso baseado na tolerância a falhas bizantinas e fornece proteção para os blocos gerados na Blockchain. Neste tipo de consenso, no viés de Baliga, Kamat e Chatterjee (2018), antes de cada rodada, os nodos escolherão um deles como líder, que neste caso será o proponente, função pela qual propõe novos blocos na rede. São aceitos três fases neste mecanismo de consenso (PRE-PREPARE, PREPARE e COMMIT);

Os nodos que não são proponentes são validadores. O proponente indica a criação de um novo bloco e dissemina na rede, a mensagem “PRE-PREPARE”, depois os validadores, iniciam o estado “PRE-PREPARED”, e distribui agora o modo “PREPARE”. Ao receber a mensagem “PREPARE”, o validador inicia o conceito de “PREPARED” e dissemina a rede a mensagem “COMMIT”, última etapa para os validadores aceitarem o bloco gerado, podendo ser então unida à cadeia de blocos. O último momento ocorre após a confirmação de 51% dos validadores recebendo a mensagem “COMMIT”, para posteriormente iniciar o estado de “COMMITED” e então uma nova rodada de negociações pode ser iniciada (Baliga; Kamat; Chatterjee, 2018).

Para suportar as transações o Quorum possui arquitetura a partir do Ethereum, vislumbrando três componentes, a saber: Nodo Quorum, Gerenciador de Transações e Enclave, conforme associação pode ser visualizada na Figura 6.

Figura 6 – Arquitetura do Quorum



Fonte: Elaborada pelo autor adaptado de Baliga, Kamat e Chatterjee (2018).

Segundo Baliga, Kamat e Chatterjee (2018) e Espel, Katz e Robin, (2017), a composição do nodo quórum, ocorre pelo geth (o Ethereum Go-Cliente) e a constelação que é o gerenciador de privacidade. O Nodo Quorum é uma modificação de um dos clientes de acesso à plataforma Blockchain Ethereum, sendo que o código de implementação em si é derivado de geth (o Ethereum Go-Cliente) e modificado para as necessidades do Quorum.

Já a constelação é definida como uma responsabilidade de duas partes, nele o aplicativo principal implementa os recursos de privacidade do Quorum e o gerenciador de transações armazena e permite o acesso a dados de transação criptografados, trocas dados e cabeçalhos criptografados, mas não tem acesso a nenhuma chave privada sensível. Finalizando a arquitetura existe o enclave, que armazena as chaves privadas e é essencialmente um HSM (*Hardware Security Module*) virtual com métodos criptográficos de proteção, então o enclave executa a ação de criptografar e descriptografar. Em suma a constelação sustenta que os dados adicionadas ao Blockchain conservem-se seguros (Baliga; Kamat; Chatterjee, 2018; Espel; Katz; Robin, 2017).

O Quorum é mais uma possibilidade para implementação dos conceitos de Blockchain, adicionado a preocupações extras com segurança e melhoria de desempenho. As próximas seções trazem outras propostas de tecnologias similares, também tratando de DLTs.

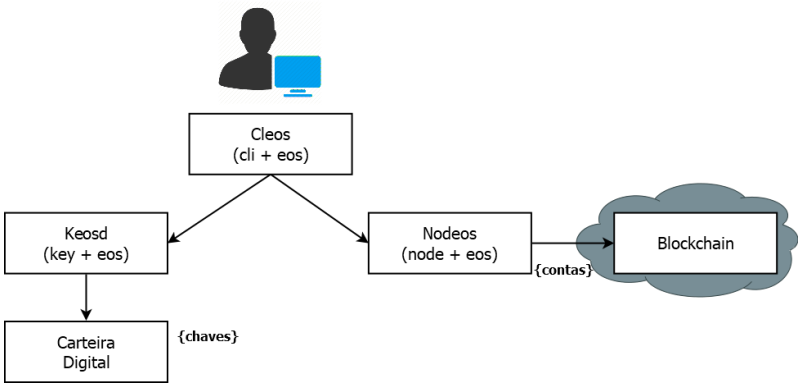
2.9.4 EOS.IO

A *startup* Block.one em 2017 idealizou o projeto EOS.IO e o lançou em 2018. O EOS.IO, por Berg, Berg e Novak (2020) é um protocolo Blockchain que explicitamente foi criado para permitir aos desenvolvedores construir *dApps*. Em Berg, Berg e Novak é descrito mecanismo de consenso denominado DPoS (*Delegated Proof of Stake* - Prova de participação delegada), no qual o EOS.IO emprega, no qual resulta de um maior velocidade de transação e redução de energia, por dispensar os mineradores, tais como outros DLTs supracitados. Em geral, a abordagem DPoS da EOS.IO permite que os detentores de moedas votem em uma classe de usuários conhecidos como "produtores de blocos" que validam transações e adicionam novos blocos ao Blockchain EOS.IO. Somente esses produtores de blocos escolhidos podem criar blocos e são recompensados pelo ambiente EOS.IO.

Os produtores de blocos podem conseguir uma votação expressiva exibindo os valores que tem aos votantes da rede, tais como capacidade de produzir blocos, infraestrutura e outras formas de impressionar tecnologicamente. Berg, Berg e Novak (2020) comentam que o processo de escolher os melhores produtores de blocos se mostra frágil devido a intenções não formalizadas com a compra de votos. Então, as Blockchains DPoS restringem as entidades validadoras por meios políticos, e não econômicos e isso implica que os produtores de blocos ajam de maneiras subjetivas para permitir ou impedir que transações e códigos sejam executados no protocolo.

O EOSIO, por Huang *et al.* (2020), foi atestado para transferência de importâncias monetárias, criação de contas e chamadas de contratos. Possui desempenho melhor do que tecnologias afins nas transações e mínimo gasto de energia. Os autores comentam sobre as contas, nas quais precisam de manutenção devido a características e tipos, tais como: contas *bots* (conta para simulação humana que se repete), contas silenciosas que nunca iniciaram uma transação, problemas relacionados a perfis indevidos de contas não transparecendo a verdadeira identificação de determinada conta. São destacadas também atividades hostis contra o ambiente EOSIO resultando em perdas significativas da moeda nativa. Em Block.one (2020) é colocada uma arquitetura básica de funcionamento do EOSIO, que segue na Figura 7.

Figura 7 – Arquitetura Básica de funcionamento do EOS.IO.



Fonte: Adaptado de Block.One (2020).

É possível identificar na Figura 7 os componentes de funcionamento da arquitetura do EOSIO. Por Berg, Berg e Novak (2020) é exibido uma interação inicial entre o aplicativo do usuário final e o Cleos, interface de linha de comando para interagir com o Blockchain e gerenciar as carteiras. O Nodes é o arquivo principal de execução do nodo EOSIO, o nodo propriamente dito, já o Keosd é o componente que armazena as chaves EOSIO nas carteiras. As contas dos usuários são definidas na rede EOSIO e possui além do relacionamento entre contas, carteiras e chaves criptográficas.

O EOS possui semelhança ao ambiente Ethereum, todavia a arquitetura foi concebida para melhorar desempenho e uso de *hardware*, conseguindo assim mais números de transações por um tempo específico.

2.9.5 XRPL

O XRPL é a uma tecnologia tratada como DLT na Ripple Labs Inc. A Ripple, empresa detentora desta ferramenta tecnológica lança o produto em 2012, com muitos predicados por Chase e MacBrough (2018), diferentes dos outros DLTs de mercado e se caracteriza por diversificar a maneira de funcionamento do livro razão, moeda XRP, mecanismo de consenso e estrutura de negócio. Para contextualizar, a Ripple surge no mercado com o intuito em atender a problemática da transferência internacional segura de dinheiro, sem intermediários.

Idealizado a partir da criação do Bitcoin o XRPL surge. Este trabalha tal qual um sistema econômico distribuído, todavia não exclusivamente registra dados contábeis dos partícipes da rede, mas, além disso, provê serviços de câmbio em pares de moedas diversos, tais como moedas fiduciárias e criptomoedas. O livro razão XRP, por Roma e Hasan (2020) é,

na verdade, uma série de livros ou versões contábeis individuais gerenciados por nodos de servidores distribuídos, titulados de *rippled*, sendo cada instância com propriedade informações sobre servidores, banco de dados e outras configurações relacionados ao processo no ambiente Ripple iniciado.

Os nodos em um ambiente Ripple, conforme Armknecht *et al.* (2015) são classificados em três entidades, como usuários finais, que podem fazer e recebem pagamentos, os formadores de mercados que garantem a rotatividade do ambiente gerando a liquidez monetária por negociar as moedas, e os servidores de validação que verificam e autorizam as transações do ambiente, não existindo portanto o papel de mineradores.

Por Chase e MacBrough (2018) as transações da tecnologia Ripple são avalizadas e processadas pelos membros da rede, por intermédio de um mecanismo de consenso personalizado, o XRP LCP (XRP *Ledger Consensus Protocol*), antigamente denominado RPCA. O mecanismo de consenso possui algumas particularidades. Cada usuário configura a própria lista de nodos exclusivos de validadores, os UNLs (Unique Node List), que terão validade durante o processo de consenso. Então cada nodo só necessita consultar a própria lista de UNL não precisando ter validação de todo o ambiente para chegar ao consenso. Os UNLs determinam quais transações devem ser adicionadas ao XRPL. Tal consenso é conseguido se em pelo menos 90% dos validadores concordarem. Qualquer nodo, segundo Armknecht *et al.* (2015), encaminha transações com intuito de conseguirem validar as transações e tentar incluir as já validadas, no entanto, somente as encaminhadas por meio dos UNLs serão consideradas. Esse mecanismo de consenso no ambiente da Ripple é aplicado em até 5 segundos em todos os nodos para existir e sustentar uma harmonia entre as entidades. O modo de operação do XRP LCP resumidamente é uma máquina de estados com réplicas, que neste caso é mantido por cada nodo integrante da rede e com a mudança dos estados das transações é gerado uma nova ordem de negócios no XRPL, livro razão da Ripple. É importante notar que o XRP LCP faz a compilação dos estados quanto ao conjunto de transações e não dos conteúdos e resultados, pois iria onerar muito o processo.

3 ASPECTOS METODOLÓGICOS

Neste capítulo são descritos os quesitos metodológicos, no qual compõem esta dissertação, bem como as etapas para alcançar a finalização do projeto. Consonante a Gil (2017), uma pesquisa é o procedimento racional e sistemático com o objetivo em oferecer respostas aos problemas indicados. A fim de tornar o conhecimento científico é imprescindível constatar as técnicas e métodos que corroboram a sua averiguação com o intuito de chegar ao conhecimento.

Existem razões distintas para o surgimento e realização de uma pesquisa. Esta pode de maneira geral ser destinada exclusivamente à ampliação do conhecimento, não se preocupando com possíveis benefícios, classificada como pesquisa básica pura ou voltada a aquisição de conhecimento com o intuito em aplicar para um específico caso, denominada pesquisa aplicada Gil (2017). Em detrimento dos conceitos explicados no autor supracitado, este trabalho é classificado como pesquisa aplicada por obter conhecimento em Blockchain e tecnologias que a cercam e aplicar definindo um modelo aplicável a ambientes de Saúde 4.0.

A aquisição dos conhecimentos para o desenvolvimento do modelo proposto e a realização deste trabalho, são provenientes de pesquisas efetuadas em materiais já publicados composto especialmente por artigos científicos, jornais, teses, dissertações, anais de eventos científicos e livros, o qual aponta para caracterizar este documento como uma pesquisa bibliográfica Gil (2017).

Os fundamentos bibliográficos fornecem subsídios para a compreensão das tecnologias aplicadas, do ambiente desenvolvido e do modelo proposto, além dos aspectos inerentes de segurança. Com a proposta é necessário entender os sistemas de saúde postulados como 4.0. O objetivo é agregar conhecimento nos ambientes virtuais de saúde com possibilidade de validar este método, além de examinar a anuência com a proposta, Kauark, Manhães e Medeiros (2010) ponderam que entender fenômenos tendo em vista associar significados caracteriza o trabalho como uma pesquisa qualitativa.

Em outro sentido esta pesquisa conforme Gil (2017) é considerada como exploratória, pois têm como finalidade conceder maior vinculação ao problema. O autor explica que a maioria das pesquisas acadêmicas possuem o aspecto de pesquisa exploratória, indicando num momento inicial do projeto como pouco provável a definição clara do que irá ser investigado pelo pesquisador (Gil, 2017).

Com o interesse em alcançar os objetivos expostos, esta pesquisa acompanha uma organização fundamentada no objetivo geral, os objetivos específicos e aspectos metodológicos delineada no Quadro 7.

Quadro 7 – Estrutura da pesquisa

Objetivo Geral	Propor um modelo utilizando Blockchain para a privacidade dos dados no escopo da Saúde 4.0.			
Objetivos Específicos	Identificar os métodos de Blockchain em sistemas de Saúde 4.0	Elaborar um modelo conceitual com a inclusão do conceito de privacidade para que o paciente estabeleça permissões de acesso sobre o seu próprio dado sensível	Desenvolver um estudo de caso prático, com um protótipo usando ambiente Blockchain e métodos criptográficos, aplicado ao modelo	Avaliar o modelo proposto em um ambiente simulado e controlado
Método	Revisão Sistemática da Literatura e Análise Exploratória	Revisão Bibliográfica da Literatura, Revisão Sistemática da Literatura e Modelagem	Revisão Sistemática da Literatura, Análise Qualitativa, Desenvolvimento e Testes	Aplicação de um Estudo de Caso
Dados	IEEE xplorer, ACM Digital Library, Springer, Web Of Science	Leitura Científica (Ciência da Computação e Afins) e bases RSL	Leitura Científica (Ciência da Computação e Afins), bases RSL e Documentação Tecnológica	Sistemas de Saúde 4.0 e bases RSL
Resultado	Resultado da Revisão com análise e sumarização	Definição de Arquitetura do Modelo	Protótipo desenvolvido e aplicado ao modelo com exemplo de interação entre usuário e paciente	Validação do Modelo

Fonte: Elaborado pelo autor.

A partir das características apresentadas nos aspectos metodológicos, para a efetivação da pesquisa são listadas, com mais detalhes, os procedimentos metodológicos para a realização do trabalho, necessários para a execução deste projeto de pesquisa.

3.1 PROCEDIMENTOS METODOLÓGICOS

1ª Etapa: Revisão Bibliográfica para fundamentar este trabalho relacionado aos temas: Blockchain, Privacidade, Criptografia e Saúde 4.0. Para a escrita da Revisão Bibliográfica deste projeto de pesquisa, foi realizada a busca por artigos em mecanismos de buscas acadêmicos, IEEE Xplore, ACM Digital Library, Springer Link e Web of Science, livros, dissertações e teses nacionais e internacionais que abordassem os conceitos de Blockchain, Privacidade, Criptografia e Saúde 4.0 e também a relação destes. Foi necessária uma abordagem para conhecer o escopo Blockchain, com origens, ferramentas e características destas para a escolha correta das tecnologias deste trabalho. Da mesma forma o conceito Saúde 4.0 foi tratado para

entender as demandas sobre essa temática, termos similares e tecnologias envolvidas. Seções sobre Privacidade e também Criptografia foram propostas para fundamentar parte do modelo proposto que se preocupa com o compartilhamento dos dados sensíveis dos pacientes.

2ª Etapa: Revisão Sistemática da Literatura para coleta e análise de trabalhos que proporcionaram modelos suportados em Blockchain e sistemas de saúde 4.0. Nesta etapa, foi necessário entender num primeiro momento o problema da pesquisa, após isso existiu a definição das bases de pesquisa para o projeto, logo foi realizada uma pesquisa com foco nos conceitos norteadores deste trabalho. Após isso existiu a necessidade da avaliação das contribuições encontradas, aplicando critérios de inclusão e exclusão, sintetizando os textos e reproduzindo uma documentação conforme os resultados da análise. A RSL é detalhada na Seção 3.2 deste trabalho.

3ª Etapa: Proposta de um modelo de privacidade dos dados em Blockchain para sistemas de Saúde 4.0. Nesta fase da pesquisa, após considerações de autores no processo de construção bibliográfica e o entendimento dos trabalhos selecionados na RSL (Revisão Sistemática da Literatura), foi criado um modelo para compartilhar dados sensíveis em ambientes de saúde, minimizando problemas relacionados ao conceito de Privacidade. Foram exploradas as carências dos projetos encontrados na RSL, e segmentado a proposta em visões, também recorrendo aos conceitos envolvidos nas pesquisas dos autores anteriores estudados. A concepção do modelo é projetada a partir de tecnologias apresentadas no referencial teórico e indicadas também por trabalhos elencados na revisão sistemática. Além disso, são colocados ambientes e perfis de acesso também de acordo com as melhores proposições dos autores estudados, mas aliando o conceito de Saúde 4.0 que remete a tecnologias atuais.

4ª Etapa: Apresentação e análise do estudo de caso por intermédio do modelo proposto. Esse passo compreende o detalhamento de cenário, indicando as tecnologias, possibilitando a interação entre os perfis de acesso aos dados sensíveis, contemplando os serviços providos. Foi exibido também o modelo proposto sendo aplicado ao cenário controlado, comentando as particularidades do cenário junto ao modelo e os resultados com a aplicação. As formas de possíveis funcionamentos do ambiente de teste estão explicadas para ratificar quaisquer ações a serem dispostas aos usuários do cenário.

5ª Etapa: Crítica aos resultados obtidos. Ao final é apresentada uma descrição das deliberações tomadas junto ao cenário, analisando a prática, explorando e avaliando as determinações do modelo, compreendendo as conexões e interações que precisam existir para o funcionamento do processo de compartilhamento de informações e respeitando o desejo do

paciente. Essa descrição indica o que o modelo trouxe de contribuição, possíveis ambientes e tecnologias integradoras de maiores contribuições e como foi realizado para entender a análise. Pela observação dos aspectos analisados também foi possível ratificar o objetivo geral deste trabalho.

3.2 REVISÃO SISTEMÁTICA DA LITERATURA

O projeto em questão propõe um modelo para privacidade de dados a partir da tecnologia Blockchain em saúde 4.0 com foco em registros pessoais. É fundamental entender o vigente estado da arte e os tipos de perspectivas sobre problemas análogos apresentados para adaptar estratégias, princípios e descobrir inovações na temática. Assim, esta seção devido ao cunho científico, enfoca as buscas por produções protocolares a partir dos mecanismos de buscas acadêmicas (Buchinger; Cavalcanti; Hounsell, 2014), encaminhando a Revisão Sistemática da Literatura.

Para Siddaway, Wood e Hedges (2018) a revisão da literatura envolve a discussão seletiva da literatura sobre um determinado tópico, com o objetivo de posicionar argumentos, cujo um novo estudo formará uma contribuição importante para o conhecimento. Um dos gêneros utilizados da revisão de literatura é a Revisão Sistemática da Literatura, por Galvão e Ricarte (2019) se trata de uma modalidade de pesquisa, com protocolos específicos realizados para o projeto de pesquisa, com o objetivo de entender e prestar sensatez a uma estrutura de documento. Siddaway, Wood e Hedges (2018) explicam que as revisões sistemáticas são caracterizadas por serem metódicas, abrangentes, transparentes e replicáveis. Esta tem por interesse também o intuito de oferecer as bases de dados bibliográficas consultadas, as estratégias de busca que foram construídas para cada base, as etapas para escolher os artigos científicos, além de trazer as limitações de cada artigo analisado, assim bem como as limitações da própria Revisão Sistemática da Literatura.

A Revisão Sistemática da Literatura é autossuficiente no sentido de possuir seus próprios objetivos, metodologia e demais características que não a deixam ser somente uma parte de um documento (Galvão; Ricarte, 2019). A Revisão Sistemática de Literatura estabelece a seleção de conteúdos confiáveis, exclusão de artigos que não indicam referência adequada para o projeto de pesquisa especificamente e mostra como o tema da pesquisa é considerado e trabalhado por demais estudos da área. A partir da Revisão Sistemática de Literatura uma série de questões são abordadas, tais como o método de pesquisa mais empregado, as principais

tendências e quais as conferências e bases de dados publicaram mais artigos sobre a temática trabalhada (Faria, 2019).

Este capítulo discorre a RSL utilizada neste trabalho, baseada no procedimento de Kitchenham (2004) obedecendo à aplicação dos critérios de inclusão e exclusão aos artigos selecionados, podendo assim indicar os artigos relevantes para o projeto de pesquisa e atingindo uma posterior análise. A RSL foi executada entre os meses de janeiro e fevereiro de 2022, a partir de publicações existentes entre o ano de 2018 a 2023 mapeadas a partir dos mecanismos de buscas acadêmicas IEEE Xplore, ACM Digital Library, Springer Link e Web of Science.

Esta RSL tem o objetivo de identificar os modelos, métodos, técnicas e ferramentas em aplicações da Blockchain com foco na privacidade em ambientes da Saúde 4.0. A orientação do projeto responde ao problema de pesquisa acerca da tecnologia Blockchain e a possibilidade desta auxiliar na privacidade do compartilhamento de registros pessoais em sistemas de Saúde 4.0, com a finalidade em entender como a temática da tecnologia Blockchain vem sendo proposta sobre os sistemas de Saúde 4.0 e também quais os principais conceitos sobre segurança de dados aplicados. A partir de Xiao e Watson (2019); Siddaway, Wood e Hedges (2018); Senivongse, Bennet e Mariano (2017) e Kitchenham (2004) foram definidas as etapas para a produção desta RSL em três fases principais: planejamento da revisão, condução da revisão e relatório da revisão.

No planejamento, se identificou a utilidade da revisão, especificou a questão de pesquisa, identificou o público e foi desenvolvido o protocolo de revisão. Já na condução da revisão foram verificados e selecionados os estudos primários, extraindo a partir dos critérios estabelecidos, analisando e sintetizando os dados. O relatório da revisão é o fechamento da RSL sendo realizada a apresentação das pesquisas da revisão da literatura.

As bases de pesquisas, já mencionadas, IEEE Xplore, ACM Digital Library, Springer Link e Web of Science, são reconhecidas internacionalmente e foram escolhidas para o desenvolvimento da RSL deste trabalho, devido ao reconhecimento da comunidade científica e acadêmica, tecnologia de acesso aos recursos de busca, recursos de refinamento, recursos auxiliares e o tamanho da base de dados com trabalhos científicos existentes na área pesquisada, além de indexarem um cômputo expressivo em periódicos relacionados à temática do trabalho (Buchinger; Cavalcanti; Hounsell, 2014).

Nas quatro bases de pesquisas descritas foram incluídos documentos de todas as áreas de pesquisa. Como opção de filtragem artigos, *journals* e periódicos acadêmicos foram selecionados. Processaram-se as buscas a partir da opção avançada em todos os campos de

pesquisa, com os termos "*Blockchain*", "*Telemedicine*", "*Health 4.0*", e "*e-health*". Restringiram-se a partir do ano de 2018 até o ano de 2023 o período de buscas. No Quadro 8 é exibido o resultado da aplicação dos termos nos mecanismos de buscas escolhidos, com a *string* utilizada, tipos de documentos elegidos e os resultados de documentos encontrados.

Quadro 8 – Resultados preliminares da RSL

Base	**String de Busca**	**Tipo**	**Total**
ACM Digital Library	(AllField:(Blockchain) AND AllField:(telemedicine)) OR AllField:("health 4.0") OR AllField:("e-health")	Research Article (Proceedings, Journals)	581
IEEE Xplore	("All Metadata":Blockchain) AND (("All Metadata":Telemedicine) OR ("All Metadata":"health 4.0") OR ("All Metadata":"e-health"))	Journal Article, Conference Paper, Early Access Article	159
Springer Link	"Blockchain" AND ("telemedicine" OR "health 4.0" OR "e-health")	Article, Conference Paper	656
Web of Science	ALL = Blockchain AND (ALL = telemedicine OR ALL = "health 4.0" OR ALL = "e-health")	Article, Proceedings Paper, Early Access	194
Total de artigo encontrados			1.590
Total de artigo únicos			1.565

Fonte: Elaborado pelo autor.

Tendo em vista o apresentado no Quadro 8 se observam as 4 (quatro) bases de publicações consultadas gerando 1.590 documentos. Como ação, durante a consulta ocorria também a importação dos documentos para a ferramenta Mendeley Desktop, a partir de extensão do Navegador Google Chrome.

3.2.1 Critérios de inclusão e exclusão

Depois do estágio de busca dos documentos nas bases de artigos supracitadas resultaram-se 1.590 publicações. Com o *software* Mendeley foram removidos os documentos duplicados e com isso persistiram 1.565. A partir da remoção das publicações repetidas as seguintes ações sobre os artigos resultantes aconteceram:

1. Leitura dos títulos e resumos (*abstract*);
2. Aplicação do critério de exclusão;
3. Aplicação do critério de inclusão.

Quanto aos critérios de exclusão foram definidos os seguintes, vide Quadro 9, a partir da questão de pesquisa:

Quadro 9 – Critérios de exclusão para as publicações encontradas.

CE.1	Artigos que apresentaram narrativas, mas sem mostrar modelos ou métodos ou técnicas da tecnologia Blockchain;
CE.2	Publicações sem propostas de arquitetura, de caráter somente teórico;
CE.3	Estudos sobre Blockchain, sem resultados finais discutidos;
CE.4	Textos que não apresentavam resumos (*abstracts*);
CE.5	Documentos que não apresentavam escritas na língua inglesa.

Fonte: Elaborado pelo autor.

Logo, os trabalhos contemplados em ao menos um dos quatro critérios de exclusão foram descartados. Após, são empregados sobre os documentos remanescentes, Quadro 10, os critérios de inclusão estabelecidos, a saber:

Quadro 10 – Critérios de Inclusão a partir de resultados dos critérios de exclusão.

CI	1. Artigos que contemplem um método, metodologia, modelo, *framework* ou arquitetura com tecnologia Blockchain em ambientes de Saúde;
CI	2. Artigos que mostrem como ocorre o tratamento do dado privado do paciente.

Fonte: Elaborado pelo autor.

Com a execução dos critérios são então selecionadas 21 publicações. Na próxima seção estão abreviadas todas as publicações resultantes no Quadro 11 e uma análise por documento a partir da leitura integral de cada artigo.

3.2.2 Análise das publicações selecionadas

Com os critérios de exclusão e inclusão aplicados do protocolo de Revisão Sistemática da Literatura, 21 documentos foram selecionados por estarem de acordo com a questão da pesquisa deste projeto. A leitura ocorreu de forma completa identificando o que foi realizado em cada publicação pelos autores com a tecnologia Blockchain e a aplicabilidade em um cenário na área da saúde. Os documentos selecionados estão listados no Quadro 11 e se encontram listados em ordem alfabética quanto ao título. Logo após são delineados, indicando um detalhamento sobre a contribuição da publicação para o trabalho corrente.

Quadro 11 – Síntese das publicações analisadas.

Nº	Título	Autor(es)	Base
1	A Blockchain-Based approach for privacy control of patient's medical records in the fog layer.	(SILVA; AQUINO JUNIOR; MELO, 2019)	ACM Digital Library
2	A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data	(AMOFA *et al.*, 2018)	IEEE Xplore
3	BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain	(NGUYEN *et al.*, 2021)	IEEE Xplore
4	BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records	(VORA *et al.*, 2018)	IEEE Xplore
5	Blockchain-based approach for e-health data access management with privacy protection	(HIRTAN *et al.*, 2019)	IEEE Xplore
6	Blockchain-based Multi-role Healthcare Data Sharing System	(YU *et al.*, 2021)	IEEE Xplore
7	Blockchain-based Personal Health Data Sharing System Using Cloud Storage	(ZHENG *et al.*, 2018a)	IEEE Xplore
8	Blockchain-Based Remote Patient Monitoring in Healthcare 4.0	(HATHALIYA *et al.*, 2019)	IEEE Xplore
9	Decentralized e-Health Architecture for Boosting Healthcare Analytics	(KOTSIUBA *et al.*, 2018)	IEEE Xplore
10	Design and Implementation of a Blockchain-Based E-Health Consent Management Framework	(AGBO; MAHMOUD, 2020)	IEEE Xplore
11	Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform	(XU *et al.*, 2019)	IEEE Xplore
12	Dynamic consent management for clinical trials via private blockchain technology	(ALBANESE *et al.*, 2020)	Springer Link
13	FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data	(ZHANG *et al.*, 2018b)	Web of Science
14	Health 4.0: On the Way to Realizing the Healthcare of the Future	(AL-JAROODI; MOHAMED; ABUKHOUSA, 2020)	IEEE Xplore
15	Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT	(HEWA *et al.*, 2020)	IEEE Xplore
16	Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain	(MAHORE *et al.*, 2019)	IEEE Xplore
17	Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain	(ZHANG; LIN, 2018)	Springer Link
18	Harmonizing Sensitive Data Exchange and Double-spending Prevention Through Blockchain and Digital Wallets: The Case of E-prescription Management	(SCHLATT; SEDLMEIR; TRAUE *et al*., 2023)	ACM Digital Library
19	A novel framework paradigm for EMR management cloud system authentication using blockchain security network	(THILAGAVATHY; RENJITH; LALITHA *et al*., 2023)	Springer Link
20	An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone	(MAHMUD; RAHMAN, 2021)	Springer Link
21	PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms	(ZALA; THAKKAR; JADEJA, 2022)	IEEE Xplore

Fonte: Elaborado pelo autor.

3.2.3 Trabalhos Relacionados

Publicação 01: A Blockchain-Based approach for privacy control of patient's medical records in the fog layer (SILVA; AQUINO JUNIOR; MELO, 2019).

No trabalho "A Blockchain-Based approach for privacy control of patient's medical records in the fog layer" é relatado o problema com a privacidade dos dados de pacientes indicando uma proposta independente e descentralizada da gestão destes dados. Os autores indicam o uso da Blockchain e os pacientes como proprietários dos dados com a capacidade de autorizar e limitar o uso destes por aplicações e terceiros, em possíveis manipulações das informações. Descrição sobre estratégias de controle existentes, quanto a outras propostas sobre privacidade com Blockchain são levantadas, e exaltada à crítica por serem implementadas todas baseadas em *Cloud*, gerando atrasos intoleráveis nas aplicações. Na proposição os autores consideram como melhor cenário o ambiente de *Fog Computing*, desenvolvendo uma arquitetura dividida em quatro camadas.

As camadas propostas neste trabalho possuem funções específicas, a saber: a camada de aplicação possui função para paciente e terceiros que interagem ofertando e solicitando informações, a camada de sensor (*gateway*) recebe os dados dos sensores que monitoram os pacientes, a camada *fog* gerencia os dados para as aplicações podendo ser implementado por servidores para validar transações e a camada de nuvem que concentra todos os dados de pacientes e autorizações de acesso. Além do citado, os autores abordam conceito de carteiras digitais (interação entre paciente, terceiros e sensores) e mineradores (nodos na camada *fog* que validam transações). As principais contribuições desta publicação são: {1} o conceito de *Gateway* que filtra e valida credenciais para manipulação de dados; {2} a carteira digital na questão de armazenar as interações aos dados dos pacientes e; {3} abordagem de armazenamento de dados dos pacientes fora do ambiente Blockchain para consumir menos recursos tecnológicos junto às transações.

Publicação 02: A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data (AMOFA *et al*., 2018).

Este trabalho "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data", evidencia a abordagem centrada no usuário e propõe papeis distintos na troca de informações em saúde. Os autores especificam a criação de blocos particulares na

proposta, aproveitando a estrutura original da Blockchain. O esquema criptográfico do projeto é explicado, assim como a função dos *smarts contracts* no mecanismo proposto. O projeto do sistema é baseado em atuações na cadeia de transação dos dados críticos a serem acessados.

São elementos do projeto: usuários (médicos, pacientes, entre outros) com identificadores por direito de acesso, o gerenciador de consultas com função de buscar a política associada às possíveis interações com os dados, o centro de contrato inteligente criador dos *smarts contracts*, nós de processamento para tratativas dos acessos aos dados auxiliando o gerenciador de consultas nas validações das solicitações, armazenamento local, espaço rápido para salvar e consultar políticas de acesso e *tokens* nas concessões aos dados e a rede Blockchain, área com registros de acesso e detalhes das transações processadas. Como principal contribuição é destaque as etapas criptográficas para acesso aos registros de saúde, com preocupação no andamento do acesso e validade temporal das informações.

Publicação 03: BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain (NGUYEN *et al*., 2021).

O artigo "BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain" retrata uma arquitetura descentralizada na área da saúde em rede hospitalar cooperativa, denominada BEdgeHealth. Os autores integram o conceito de Blockchain, MEC (Mobile Edge Computing) e QoS (Quality of Services). Problema relacionado à privacidade ao compartilhar dados por dispositivos móveis é apresentado e proposto a partir de servidores MEC, alocados em cada hospital, como possível boa prática, melhorando o custo, tempo de processamento e uso geral com relação às restrições de compartilhamento. Foi desenvolvido, junto à rede hospitalar, um esquema no acesso de informações a partir da cooperação do ambiente Blockchain, MEC, *smart contract*, e IPFS (Interplanetary File System) oportunizando a descentralização da arquitetura.

Os autores detalham como funciona a integração dos hospitais, transferência dos dados, servidores MEC (coordenadores de dispositivos *mobile*), usuários do ambiente de saúde, dispositivos *mobiles*, IPFS *storage* e *smart contract*. Existe também no especificado ao projeto um esquema de transferência de dados, retratando um modelo próprio com regras para definir cada tarefa quanto aos dados em saúde se podem ser executados diretamente no dispositivo móvel ou no servidor MEC. O artigo trouxe como contribuição: {1} integração do *smart contract* ao IPFS permitindo novas formas de uso do *hash*; {2} o processo de recuperação de

dados entre hospitais, respeitando regras hierárquicas nas conversações; {3} conceito de semiconfiável indicado para os servidores MEC e usuários de saúde.

Publicação 04: BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records (VORA *et al*., 2018).

A proposta em "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records" é estruturada sobre a temática Saúde 4.0 e o objetivo de proteger os dados médicos, neste artigo denominado por EHRs. A arquitetura sugerida traz cinco perspectivas: rede de fornecedores de dados em saúde, ambiente Blockchain gestor dos contratos e registros, nodo paciente local da origem dos registros, *proxy nodes* criado para tratar aspectos criptográficos nas transações e *pool of votes* para auxiliar na validação dos nodos adicionados à rede e manutenção da integridade das transações.

Toda transação é suportada nas validações do ambiente, sendo explicada a adição de bloco, adição de paciente, gestão dos acessos, adição de registro, recuperação de registro e transferência de registros, a partir de algoritmos para cada ação. As questões criptográficas explicada por autores procuram minimizar acesso não autorizados nos dados dos pacientes. Como principais contribuições para esta pesquisa estão: {1} algoritmos genéricos representante de várias ações na cadeia de transações; {2} relacionamento das entidades dentro arquitetura validando as etapas da transação e; {3} categoria própria de nós da cadeia de blocos da arquitetura proposta.

Publicação 05: Blockchain-based approach for e-health data access management with privacy protection (HIRTAN *et al.*, 2019).

No artigo "Blockchain-based approach for e-health data access management with privacy protection" é apresentado uma separação de estrutura de ambientes Blockchain, uma privada, a *sidechain*, local para guardar informações sobre a identidade verdadeira do paciente e outra pública, o *mainchain*, área para armazenar informações sobre os dados de saúde dos pacientes marcados com uma identificação temporária. Os autores propõem que as informações sejam compartilhadas entre hospitais, clínicas médicas e institutos de pesquisa com base nas políticas de acesso definidas pelos pacientes, reconhecidos como proprietários dos próprios dados e com controle total sobre eles.

O ambiente proposto foi implementado com Hyperledger Fabric. Como usuários contemplados existem, pacientes, médicos, instituições (hospitais, clínicas, entre outros) e

demais entidades (seguradoras, institutos de pesquisa, serviços de emergência). Com a estrutura dividida em *sidechain* e *mainchain* é implementado o controle de acesso considera dois tipos de nós (nodos) confiáveis e não confiáveis, onde dependendo do nível de confiança dos nós, estes podem acessar apenas o ambiente Blockchain público, *mainchain*, ambos, ou somente ambiente Blockchain privado, *sidechain*. Os pontos importantes de contribuição para este trabalho são: {1} a segmentação do acesso dependendo do tipo de usuário, confiável ou não confiável, uma opção para controlar a gestão aos dados; {2} encapsulamento de informações pessoais e modo de compartilhamento centrado no paciente e; {3} identificação temporária em determinadas transações para minimizar vulnerabilidades nos acessos.

Publicação 06: Blockchain-based Multi-role Healthcare Data Sharing System (YU *et al*., 2021).

No documento intitulado "Blockchain-based Multi-role Healthcare Data Sharing System" é disposta a carência de protocolos de compartilhamento direcionados para dados médicos e dados pessoais de saúde. Logo, os autores sugerem um sistema de compartilhamento de dados de saúde com base em Blockchain. É indicado o armazenamento de dados colaborativo junto ao conceito de IPFS. Além disso, é trabalhado o *smart contract* e dois protocolos distintos para tratar a dados médicos e dados pessoais de saúde separadamente. O modelo do sistema de compartilhamento de dados em saúde para múltiplos papéis baseado em Blockchain apresentado utiliza prova de trabalho (PoW) como mecanismo de consenso padrão, existe verificação dos usuários por entidades mineradoras por meio da assinatura digital. Ainda é utilizado o conceito de *merkle-root* (técnica usada para verificação de integridade) na análise a estrutura dos registros médicos.

A utilização do IPFS é realizada para minimizar o custo computacional com a Blockchain implementada, ou seja, se uma grande quantidade de dados for enviada diretamente para a Blockchain, o custo será muito alto, então os autores direcionam os dados para o serviço IPFS e, em seguida, o arquivo *hash* resultante para o ambiente Blockchain. As interações entre os atores do modelo também são abordados passo a passo explorando os processos de envio e recebimento de dados e como ocorre o armazenamento e gerencia de acesso aos tipos de dados. O trabalho trouxe notória contribuição, a saber: {1} diferença e tratamento distinto para dados pessoas de saúde (*personal health data*) e dados médicos (*medical data*) com protocolos específicos para gerir de forma única e; {2} diagrama de interação das entidades do sistema,

com as especificidades para pacientes, donos dos dados, com autoridade sobre a informação para compartilhamento, atualização e revogação.

Publicação 07: Blockchain-based Personal Health Data Sharing System Using Cloud Storage (ZHENG *et al*., 2018a).

O trabalho "Blockchain-based Personal Health Data Sharing System Using Cloud Storage" é concentrado em um tipo de dado de saúde chamado dados dinâmicos e contínuos, estes refletem a atividade do usuário durante um período de tempo, tais como os coletados e observados por dispositivos em atividades específicas de monitoramento. A arquitetura proposta de armazenamento e compartilhamento de dados em saúde é proposta a partir de três papéis: usuários que enviam e compartilham dados pessoais de saúde, *key keppers* para gerir chaves privadas e transações com estas chaves e os clientes que usufruem dos dados.

Quanto à privacidade, os autores utilizam criptografia nos dados dos pacientes, acesso restrito a nuvem de dados, descentralização de armazenamento das chaves criptográficas e rede Blockchain que oculta a identidade verdadeira dos pacientes. É proposto também que somente dados transacionais e metadados estejam salvos e compartilhados na Blockchain. Este trabalho elucidou os seguintes aspectos: {1} descrição da arquitetura geral e o fluxo de trabalho do sistema proposto com papéis e ações do usuário, *key keepers* e cliente e; {2} camadas de proteção descritas para salvar informações em nuvem dos pacientes.

Publicação 08: Blockchain-Based Remote Patient Monitoring in Healthcare 4.0 (HATHALIYA *et al*., 2019).

No documento "Blockchain-Based Remote Patient Monitoring in Healthcare 4.0" é visualizado o conceito da Saúde 4.0 no monitoramento remoto de pacientes (RPM - Remote Patient Monitoring) e considerado como maneira de aumentar a segurança e privacidade dos dados do paciente à aplicação da tecnologia Blockchain neste sentido. O artigo traz um modelo baseado em Blockchain projetado para a saúde com o intuito de minimizar ações hostis aos dispositivos da Saúde 4.0. A arquitetura proposta pelo artigo integra conceitos de Blockchain, Redes de Computadores, Inteligência Artificial e compara a proposição com modelos anteriores, defendendo o projeto a partir da IA descentralizada colocando os pacientes como ponto focal da estrutura que abriga as informações, tornando-as seguras conforme a arquitetura descentralizada proposta que depende da anuência do paciente para disponibilizar os dados pertinentes.

Os autores também colocam o paciente como autoridade maior sobre os registros pessoais de saúde e sugerem a IA descentralizada como suporte para gestão de várias ações, junto aos pacientes, profissionais de saúde, pesquisadores e organizações em saúde. Como colaboração este artigo traz aspectos gerais de como o Blockchain pode colaborar na privacidade do paciente, tornando ambientes confiáveis. Além da sugestão de tornar o hospital como a valência que conecta todos os outros atores da arquitetura preponderando como principal entidade.

Publicação 09: Decentralized e-Health Architecture for Boosting Healthcare Analytics (KOTSIUBA *et al*., 2018).

Em "Decentralized e-Health Architecture for Boosting Healthcare Analytics" é apresentado uma visão geral dos problemas associados à análise e segurança dos dados médicos e ofertado uma solução para a melhoria da qualidade dos serviços médicos. A proposição da arquitetura para dados de saúde descentralizado baseado em um Blockchain ocorre então para proteger os dados médicos confidenciais. Está arquitetura é baseada na tecnologia Exonum, plataforma de código aberto para o mercado de saúde.

Nessa estrutura, a tecnologia Blockchain atua como um mecanismo de monitoramento e registro de dados sobre alterações em prontuários médicos. A arquitetura descentralizada envolve o armazenamento de dados em vários nós, que podem ser bancos de dados ou sistemas computacionais. Os pacientes podem rastrear o histórico médico e fornecer acesso a especialistas de diferentes organizações médicas na mesma plataforma, além de oportunizar o compartilhamento de informações médicas despersonalizadas para profissionais em saúde e pesquisadores. Este artigo trouxe contribuições no {1} conhecimento de aplicabilidade da plataforma Exonum para ambientes de saúde, na {2} visão de mudança do modelo de negócio proposto para compartilhamento de dados pessoais com garantias e vantagens aos pacientes junto a plataforma de acesso, e na {3} solução Blockchain criada que comporta informações disponíveis e indisponíveis dependendo do propósito de atuação da transação a ser finalizada.

Publicação 10: Design and Implementation of a Blockchain-Based E-Health Consent Management Framework (AGBO; MAHMOUD, 2020).

No artigo "Design and Implementation of a Blockchain-Based E-Health Consent Management Framework" é dissertado sobre o conceito PMR (Patient Medical Records), Registros Médicos do Paciente contemporizando que este é a compilação de interações clínicas

entre pacientes e profissionais da área da saúde, bem como dados de saúde coletados por meio de sensores médicos. Os autores também trazem pacientes como proprietários dos dados, e os prestadores de serviços de saúde e outras entidades que podem querer consumir os dados do paciente são indicados como consumidores de dados.

Os dados críticos dos pacientes são salvos em nós distribuídos na rede Blockchain, onde as operações são aprovadas por elementos da rede descentralizados que validam transações. Para entender como ocorre o projeto é explicada as interações tecnológicas, atores e componentes. Em complemento são mostradas as autoridades certificadoras e como estas são utilizadas por pacientes. Estas são utilizadas para assinar transações, registrar identidades por nó e interagir com a rede. O funcionamento e implementação dos *smarts contracts*, também são divulgados, mostrando como estes funcionam para a rede e junto ao paciente. Por possuir etapas bem definidas na construção da arquitetura este projeto contribui para: {1} sedimentar possíveis interações de pacientes com profissionais de saúde a partir dos registros médicos do paciente, {2} entender possíveis interações tecnológicas não visualizadas anteriormente em outras publicações e {3} compreender mais funções atreladas a autoridades certificadoras junto a rede de dados.

Publicação 11: Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform (XU *et al*., 2019).

O trabalho "Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform" discorre uma plataforma de gerenciamento de registros eletrônicos de saúde (CB-EHRs) com base em Blockchain. A plataforma é caracterizada por praticar o conceito de descentralização, inviolabilidade de dados e mecanismos de manutenção coletiva na rede, para garantir a privacidade dos usuários.

A arquitetura proposta da plataforma CB-EHRs é projetada em 3 camadas, que correspondem a: camada do usuário empregada para exibir dados e receber informações de entrada do usuário, a camada de lógica de negócios utilizada para encapsular os dados do usuário em transações e ativos, e após isso transferir estas transações e ativos para nós na rede Blockchain. Existe também a camada de acesso a dados, usada para manter a operação dos registros, ou seja, receber solicitações de verificação de transação, gerar blocos e propor novos blocos. O mecanismo de consenso utilizado nesta arquitetura é o *Delegated Byzantine Fault Tolerance* (dBFT) e a estrutura de rede permite a cada nó na rede a replicação completa dos dados eletrônicos de saúde. Esta publicação trouxe como contribuição para este trabalho a {1}

comparação das características de mecanismos de consenso que podem ser aplicados por soluções Blockchain, {2} modelagem das camadas no provimento de EHRs e, {3} uma visão particular da distribuição descentralizada dos EHRs no ambiente de saúde.

Publicação 12: Dynamic consent management for clinical trials via private blockchain technology (ALBANESE *et al*., 2020).

O documento "Dynamic consent management for clinical trials via private blockchain technology" mostra o SCoDES como abordagem para gerenciamento confiável e descentralizado do consentimento dinâmico em ensaios clínicos, baseado na tecnologia Blockchain. A perspectiva do SCoDES mostra atuações de perfis específicos. Institutos de Saúde, Indústrias privadas como as farmacêuticas, Universidades, profissionais de saúde, pesquisadores e pacientes. Os usuários possuem como outras arquiteturas já abordadas interações e comportamentos distintos para acessar, manipular e autorizar informações de saúde.

A arquitetura proposta apresenta 3 camadas. Na primeira camada como estrutura DLT foi implementado o Hyperledger Fabric para armazenar o histórico das transações. A camada intermediária apresenta um sistema computacional que se comunica com a infraestrutura Blockchain (DLT), sendo utilizada a tecnologia Hyperledger Composer para definir regras de controle de acesso e consultas. A terceira camada é a interface oferecida para exploração de dados a partir de funções do escopo de ensaios clínicos. O projeto SCoDES foi útil por contribuir: {1} no desenvolvimento do ciclo completo do provimento da informação em saúde, exibindo desde o ambiente Blockchain até a interface com o usuário final, além disso {2} proporcionou detalhamento simplificado do uso prático da tecnologia Hyperledger em um ambiente para salvar dados das interações clínicas.

Publicação 13: FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data (ZHANG *et al*., 2018b).

O texto do artigo "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data" apresenta o FHIRChain, estrutura baseada em Blockchain, projetada para atender aos principais requisitos técnicos definidos pelo mapa de interoperabilidade ONC (*Office of the National Coordinator*), órgão no qual estabelece as estruturas para tecnologias da informação aplicadas à gestão e operação dos sistemas de saúde. Conforme os autores defendem a FHIRChain é colocada como uma arquitetura geral de compartilhamento de dados integrável

a sistemas de tecnologia da informação. O projeto emprega o acesso aos dados a partir de várias configurações como participação de médicos certificados e filiados a organizações de saúde. A estrutura assim como outras propostas, trabalha com par de chaves criptográficas públicas e privadas, para cada provedor de dados participante.

A estrutura do FHIRChain também suporta características interessantes como *smart contracts* para manter a identificação dos usuários sem expor informações pessoais na Blockchain. Os *smart contracts* então associam os usuários as identidades digitais, contemplam os tipos de acesso, ou seja, as autorizações de permissão entre os participantes, criando assim uma base de dados rastreável sobre as possíveis permissões e registros das transações. Pontos importantes de contribuição de publicação são: {1} a arquitetura disponibilizada que separa o armazenamento de dados das outras informações do sistema, minimizando possíveis problemas com atualizações em requisitos funcionais e não funcionais da arquitetura e; {2} aplicações da arquitetura em estudos de caso detalhando, implantação e resultados.

Publicação 14: Health 4.0: On the Way to Realizing the Healthcare of the Future (AL-JAROODI; MOHAMED; ABUKHOUSA, 2020).

No trabalho "On the Way to Realizing the Healthcare of the Future" é relatado de uma maneira geral o conceito de Saúde 4.0 e o caminho a percorrer para conseguir maturidade do relacionamento entre saúde e tecnologia. O artigo traz também os benefícios da adoção da Saúde 4.0, que inclui melhorar a flexibilidade, escalabilidade, confiabilidade, agilidade, custo-benefício e qualidade de serviços e operações de saúde. É proposto um *middleware* orientado a serviços para oferecer serviços em comum aos desenvolvedores de aplicativos, facilitando a integração de serviços para construir soluções sob a ótica das tecnologias de Saúde 4.0.

O trabalho explora a temática de possibilidades para conversar tecnologias com a área de saúde, trazendo à tona o porquê do termo Saúde 4.0. O *framework* abordado no artigo é denominado SOM (*service-oriented middleware*), indicando uma estrutura de *middleware* avançada para Saúde 4.0. É esperado com a utilização deste a aplicação dos princípios da Saúde 4.0, tais como interoperabilidade, virtualização, descentralização, capacidade em tempo real, orientação de serviço e modularidade dos sistemas.

O artigo se completa com as camadas projetadas pelo SOM e os serviços de suporte existentes, sendo o *framework* projetado a principal contribuição do artigo. Em se tratando de privacidade de dados o SOM promete dados anonimizados ao utilizá-lo em integrações de coletas específicas de informações e possibilidade em ocultar informações confidenciais

específicas durante o processo de coleta e transferência de dados. Tais abordagens podem ser implementadas e fornecidas como um serviço na estrutura SOM.

Publicação 15: Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT (HEWA *et al*., 2020).

O artigo "Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT" propõe uma arquitetura de serviço baseada em Multi-access Edge Computing (MEC), tecnologia Blockchain e transações de dados em tempo real entre IoT, MEC e nuvem. Os autores propõem ainda, um esquema próprio para transferência de dados e gestão dos dispositivos que computam informações críticas. As tecnologias atuantes foram os *smarts contracts* no controle de acesso e a plataforma Blockchain, Hyperledger Fabric com dispositivos Raspberry Pi para simular a atividade dos sensores médicos.

A arquitetura é proposta a partir de nuvem IoT-MEC, atrelado ao ambiente Blockchain e a tecnologia IPFS. Os elementos existentes na estrutura são: o paciente, hospital, dispositivo, nó MEC, camada de serviço Blockchain (BSL), servidor em nuvem e entidades/atores terceiros. Práticas são implementadas junto aos elementos existentes minimizando ações hostis nas transações como: verificação de assinatura e autenticação dos nós MEC por meio do conceito Schnorr (modo de conectar múltiplas chaves de carteira a uma única assinatura), validação de política de segurança e controle de acesso na camada de serviço Blockchain, anonimização dos dados de paciente e controle de acesso a partir dos *smarts contracts*. Este artigo traz contribuições no que tange {1} integrações de tecnologias para contemplar a privacidade da informação desde o dado coletado até a análise; {2} solução escalável para armazenamento de dados e; {3} esquema de recompensa para compartilhamento de dados por meio dos *smarts contracts.*

Publicação 16: Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain (MAHORE *et al*., 2019).

Em "Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain" é visualizado uma proposta para segurança em sistemas de saúde focada na privacidade do gerenciamento de registros usando Blockchain. Existe o debate do problema quanto aos pesquisadores na área da saúde encontrarem atrasos nas comunicações, dados dispersos e fluxos de trabalho médicos morosos. É proposto um modelo que salienta sobre o fornecimento de dados de saúde a pesquisadores para análises estatísticas e fornece

privacidade ao mesmo tempo, com segurança dos dados trafegados, utilizando técnicas, tais como: criptografia assimétrica e proxy criptografado. No modelo proposto o paciente possui controle total dos dados, garantindo a privacidade a partir do Blockchain junto à área médica.

A proposta traz as entidades paciente, hospitais, pesquisadores e agências. Como tecnologia Blockchain permissionada é utilizado o Hyperledger Fabric controlando as entidades da rede e atribuindo chaves criptográficas e certificados. A metodologia da proposta indica a criação de registro para o paciente no ambiente *cloud* quando este necessita ir ao hospital, atrelado a isso os metadados (id de dados, id *cloud*, id paciente, id médico, id hospital, id do agravo, *hash* do registro e *timestamp*) são armazenados na Blockchain. O modelo diferencia dados sensíveis, informações pessoais que podem revelar a identidade de um paciente e não sensíveis informações de diagnóstico detalhadas por meio das quais identificar um paciente não é possível, sendo que os pacientes possuem domínio e ações de possíveis restrições aos dados sensíveis. O {1} formato objetivo da arquitetura com as características e detalhamento das entidades e {2} a estrutura das transações são os aspectos de contribuição desta arquitetura.

Publicação 17: Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain (ZHANG; LIN, 2018).

No trabalho "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain" é a abordado o conceito de *Personal Health Information* (PHI) e um esquema de compartilhamento com preservação de privacidade baseado em Blockchain. São colocados dois tipos de Blockchain, o Blockchain Privado responsável por armazenar o registro PHI original dos pacientes em uma possível ida ao hospital e Blockchain de Consórcio para manter registros dos índices PHI, utilizados por terceiros. A arquitetura proposta possui 3 entidades, gerente do sistema, serviço médico provedor (hospitais) e os usuários (pacientes).

Uma nova estrutura de Blockchain foi projetada (blocos, tamanho, *hash*, criptografia, *timestamp*, cabeçalho de bloco e carga útil) e também foi adaptado o mecanismo de consenso PoC (*Proof of Conformance*) para ambos os Blockchains adotados. A estrutura foi concebida com 3 camadas: camada de geração de dados que conectam os pacientes aos serviços providos por hospitais, camada de armazenamento de dados responsável por salvar os PHIs encriptados no Blockchain Privado e camada de serviço de dados funcionando a partir do Blockchain de Consórcio provedor dos serviços indexados e requisições de hospitais cooperados. A contribuição ocorreu {1} a partir da utilização mesclada de dois tipos de ambientes Blockchain

distintos; {2} as adaptações e explicações da estrutura Blockchain e mecanismo de consenso e; {3} a forma de compartilhamento de dados entre hospitais que explorou a ideia de serviços e requisições em comum.

Publicação 18: Harmonizing Sensitive Data Exchange and Double-spending Prevention Through Blockchain and Digital Wallets: The Case of E-prescription Management (SCHLATT; SEDLMEIR; TRAUE *et al*., 2023).

O artigo "Harmonizing Sensitive Data Exchange and Double-spending Prevention Through Blockchain and Digital Wallets: The Case of E-prescription Management" traz um sistema de gerenciamento de receitas médicas eletrônicas (*e-prescriptions*) com suporte da tecnologia Blockchain e utilização do conceito das carteiras digitais, propondo a partir disto a privacidade do paciente. Os autores, com o sistema, explicam que os médicos geram as receitas médicas eletrônicas e as enviam diretamente para as carteiras digitais dos pacientes, estas sendo acessadas apenas por usuários autorizados.

No contexto da criptografia, a troca de chaves é utilizada para garantir que somente as partes autorizadas (médico, paciente, farmácia) tenham acesso às informações da receita médica, e cada usuário autorizado possui uma chave pública e uma chave privada única. A preocupação com a receita é notória durante o artigo que também trata a duplicidade de receitas, minimizando esta possibilidade no sistema a partir das técnicas da Blockchain. Existe a aplicação de criptografia para proteger os dados do paciente e da receita médica na transmissão e armazenamento, onde a troca de chaves criptográficas é empregada.

Este artigo auxiliou, pois teve: 1} abordagem para a troca de chaves criptográficas entre os usuários (médicos, pacientes e farmácias) envolvidos no processo de gerenciamento de E-Prescriptions, pois as chaves criptográficas são baseadas em identidade, e não em autoridades certificadoras centralizadas, onde cada usuário gerencia a própria chave privada, pelas carteiras digitais, para assinar as transações. Foi possível também {2} entender de modo prático as plataformas de DLTs Quorum e Indy, onde os dois podem ser utilizados para o conceito de privacidade, além de serem escaláveis para ambientes de saúde, e suportarem dados criptografados.

Publicação 19: A novel framework paradigm for EMR management cloud system authentication using blockchain security network (THILAGAVATHY; RENJITH; LALITHA *et al*., 2023).

Em "A novel framework paradigm for EMR management cloud system" é proposto um *framework* chamado B-EMR, definido em quatro componentes principais: a interface com o usuário (autenticação e interação com a base de informações na Blockchain), a base de dados do Blockchain (conjunto de regras e protocolos de segurança que são aplicados na topologia da rede blockchain, sendo responsável por gerir as chaves criptográficas), a Rede Pública Blockchain (envolve contratos inteligentes, *ledgers* distribuídos e nós de blockchain da rede pública Blockchain.), o Banco de dados na Nuvem (repositório dos registros de saúde oriundos das transações na Blockchain).

Os autores trazem uma arquitetura a partir da tecnologia Ethereum e com sequência de transações bem definidas entre a interface de acesso e o ambiente Blockchain e a comunicação para o armazenamento em nuvem. Os *smart contracts* na rede Blockchain proposta, automatizam a execução de ações específicas, como o compartilhamento de registros médicos eletrônicos entre diferentes instituições de saúde, no entanto, os médicos não precisam da anuência do paciente e possuem gestão sobre os dados, após autenticação bem sucedida no ambiente Blockchain. As abstrações junto a este artigo permitem {1} compreender uma logística diferente de manipulação de dados em dois momentos distintos, no acesso à rede Blockchain e no armazenamento dos registros em nuvem. Quanto ao processo criptográfico {2} é interessante apontar o processo para gerir as chaves (com base no algoritmo ElGamal) e o formato de como cada usuário carrega o par de chaves gerados durante o processo de registro.

Publicação 20: An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone (MAHMUD; RAHMAN, 2021).

A proposta em "An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone" traz a dispensa das criptomoedas nas transações com o conceito de anonimicidade durante as interações entre pacientes e médicos, que usam *tokens* nos acordos de acesso aos dados e retornos médicos. A concepção do artigo foi desenvolvida sob uma aplicação para *smartphone* que acessa o ambiente Blockchain e por meio de chaves públicas tem acesso aos dados em saúde, sendo descriptografados somente a partir da chave privada armazenada no *smartphone*. Os autores defendem que o projeto mitiga a adulteração de dados, e o esquema de guardar o *hash* e senha criptografadas na Blockchain se refere a isso,

visto que ficam em local diferente da chave privada, armazenada somente no dispositivo móvel do usuário (paciente).

Além disso, existem 3 camadas de atuação explicadas no artigo: a camada do usuário, camada lógica de processamento e a camada de armazenamento. A primeira camada de acesso do usuário serve para garantir a segurança dos pacientes, com a geração do par de chaves criptográficos, também traz os acessos as transações e interações médicas com os dados clínicos. A segunda camada também trata de aspectos criptográficos, gestão dos contratos inteligentes, processamento de relatórios, com implementação das funções a partir da linguagem Python e bibliotecas e tecnologia Node JS. Já a terceira camada consiste no armazenamento Blockchain e IPFS, com as transações com IPFS, *hash* de arquivos do usuário e a senha criptografada armazenadas na Blockchain, com os arquivos criptografados armazenados em uma rede IPFS. Como contribuição este artigo {1} formaliza o modo da troca e armazenamento de chaves criptográficas junto a Blockchain e {2} direciona uma estrutura de interação entre paciente e médico apoiada em camadas distintas com funções bem definidas.

Publicação 21: PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms (ZALA; THAKKAR; JADEJA, 2022).

No documento "PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms" os autores possuem a preocupação central em como compartilhar e gerenciar os dados de saúde com perfis diferentes de acesso, também investem tempo para explicar os processos criptográficos utilizados para garantir a privacidade e projetam a estrutura a partir de arquiteturas em nuvem. De modo geral, como chamam a atenção implantando os gateways (GW) e os data centers (DC) que são nós intermediários com camadas de segurança adicionais. Os gateways são indicados para autenticação e validar credenciais de acesso, já os data centers são responsáveis por armazenar e processar os dados do paciente.

Os autores separam o funcionamento do PRMS (Patient's E-Healthcare Records Management System) em dois momentos e esclarecem que os componentes críticos e confidenciais do sistema, como o banco de dados que armazena os registros eletrônicos de saúde dos pacientes e a camada de aplicação do sistema que realiza a lógica de negócios são executados em nuvem privada, localizada na instituição de saúde que usa o sistema PRMS. Já na nuvem pública, são executados componentes menos críticos como a interface de usuário, a

e serviços de autenticação e autorização. Para a comunicação entre a nuvem pública e a nuvem privada é possível a ocorrência realizada por meio de um gateway seguro.

Em suma este artigo traz a importância de {1} separar os perfis de acesso aos registros em saúde. Apesar da preocupação com o conceito de privacidade, além do paciente, o profissional de saúde e o administrador do sistema também possuem como editar os dados (históricos, diagnósticos, medicamentos e resultados) dos pacientes. Os pacientes podem modificar informações, no entanto, alguns dados críticos como diagnósticos e tratamentos somente são liberados sem limitação para os profissionais de saúde. A {2} arquitetura do projeto, também traz menções as boas práticas para o conceito de privacidade, minimizando vulnerabilidades colocando os serviços críticos em ambiente privado com acesso controlado.

3.2.4 Discussão sobre a análise dos trabalhos relacionados

As contribuições dos artigos resultantes da RSL foram contundentes no direcionamento dos próximos passos da pesquisa. As publicações trouxeram modelos, métodos ou arquiteturas implementados a partir da tecnologia Blockchain considerando aspectos percebidos nas fragilidades das implementações ao compartilhar dados dos pacientes. É interessante observar os diferentes aspectos em que se trataram as tecnologias para abrigar os dados dos pacientes perante o conceito de privacidade, permitindo sempre absorver novas práticas em cada ambiente estudado.

Os critérios estabelecidos de inclusão e exclusão contribuíram para melhorar na escolha dos artigos considerados como pertinentes no processo de escrita da RSL. A leitura dos artigos elegidos baseou o entendimento sobre os processos de compartilhamento, detalhes das implementações e escolha das principais entidades que interagiam nos ambientes propostos. Foram compreendidos também técnicas criptográficas, tipos de tecnologias Blockchain implementadas, locais de armazenamento dos dados de pacientes e das transações, métodos de consenso escolhidos, e estruturas de compartilhamento propostas. Em todos os documentos lidos se interpretou o domínio do paciente sobre os dados pessoais, independentes da nomenclatura ou atributos atrelados adotado. Alguns artigos apesar de exibirem as técnicas de avaliação dos métodos não tratam da melhor forma os resultados finais e comentários pós-aplicação da solução proposta o que indica uma nova possível abordagem dependendo do cenário aplicado. O Quadro 12, a seguir, exibe uma confrontação acerca dos trabalhos selecionados a partir de propriedades mais relevantes encontradas.

Quadro 12 – Comparação das publicações analisadas

Autor(es)	Implementação Blockchain	Nome da Tecnologia	Criptografia dos dados armazenados	Armazenamento dos registros médicos	Moderação do dado compartilhado
Silva, Aquino Junior e Melo (2019)	Privada	Ethereum Harmony	Sim	off-chain	Manual por paciente
Amofa *et al.* (2018)	Privada	Ethereum	Sim	off-chain (dados) on-chain (metadados)	Paciente criam políticas no registro que determinam as ações.
Nguyen *et al.* (2021)	Privada (Global entre Hospitais) Privada (Dentro dos Hospitais)	Hyperledger Fabric para Blockchain Local e Blockchain Global	Sim	on-chain	A partir da arquitetura BEdgeHealth acontece a autenticação e os perfis estão nos *smarts contracts.*
Vora *et al.* (2018)	Pública	Ethereum	Sim	on-chain	Conforme o que está descrito nos *smarts contracts*.
Hirtan *et al.* (2019)	Pública (mainchain) Privada (sidechain)	Hyperledger Fabric	Sim	off-chain (dados) on-chain (transações)	Definida em cada paciente na Blockchain.
Yu *et al.* (2021)	Privada	B-MRHDS (Blockchain Based e IPFS)	Sim	on-chain	Por meio de chaves públicas cadastradas em um "lista branca" de acesso atrelado ao smart contract
Zheng *et al.* (2018a)	Pública	Ethereum	Sim	off-chain	Dados na nuvem e acessados por compartilhamento de chaves definido pelos pacientes
Hathaliya *et al.* (2019)	Privada	Blockhain Generic	Somente na autenticação	off-chain	Pacientes decidem junto aos pedidos existentes na Blockchain
Kotsiuba *et al.* (2018)	Pública (Ambiente Aberto) Privada (Ambiente Fechado)	Exonum Blockchain Framework (parte aberta e parte fechada)	Não	off-chain	Definido na Plataforma mediante ao perfil de acesso
Agbo e Mahmoud (2020)	Privada	Hyperledger Fabric	Não	off-chain	Paciente decide acesso parcial ou total na 1ª interação na rede Blockchain

Continua...

Autor(es)	Implementação Blockchain	Nome da Tecnologia	Criptografia dos dados armazenados	Armazenamento dos registros médicos	Moderação do dado compartilhado
Xu *et al.* (2019)	Pública	Blockhain Generic	Sim	on-chain	Conforme regras da Plataforma Blockchain CB-EHRs os usuários com cadastro possuem acesso
Albanese *et al.* (2020)	Privada	Hyperledger Fabric	Sim	on-chain	Gerado automaticamente conforme origem, com permissão configurada por pacientes no SCoDES
Zhang, *et al.* (2018b)	Privada	Ethereum	Sim	on-chain	A partir do FHIRChain (par de chave pública e privada)
Al-jaroodi, Mohamed e Abukhousa (2020)	Pública	Blockhain Generic	Não	off-chain	Por meio de dados e serviços existentes no Framework SOM
Hewa *et al.* (2020)	Privada	Hyperledger Fabric	Sim	off-chain	No registro do paciente (par de chave pública e privada)
Mahore *et al.* (2019)	Privada	Hyperledger Fabric	Sim	on-chain	No momento do cadastro no hospital (par de chave pública e privada)
Zhang e Lin (2018)	Privada (Hospitais) Pública (Consórcio dos Hospitais)	Protocolo BSSP e Plataforma JUICE	Não	híbrido	Na 1ª interação entre médico e paciente por token
Schlatt; Sedlmeir; Traue *et al*. (2023)	Pública	Ethereum, Quorum, Indy	Sim	on-chain/off-chain	Por perfil e carteira digital
Thilagavathy; Renjith; Lalitha et al. (2023)	Pública	B-EMR (Blockhain Generic)	Sim	off-chain	Por meio de perfil de acesso a partir dos Smarts Contracts
Mahmud; Rahman (2021)	Público	BigchainDB	Sim	on-chain	A partir dos *smarts contracts* junto a autenticação de dois fatores

Continua...

Autor(es)	Implementação Blockchain	Nome da Tecnologia	Criptografia dos dados armazenados	Armazenamento dos registros médicos	Moderação do dado compartilhado
Zala; Thakkar; Jadeja (2022)	Pública	Blockhain Generic	Sim	off-chain	Acesso de dados por meio de perfis de usuários, a partir de um módulo de controle
Modelo da Pesquisa – BIMHE (2023)	Pública	Ethereum (Ganache) em conjunto com técnicas de criptografia	Sim	on-chain	No registro do paciente (par de chave pública e privada)

Fonte: Elaborado pelo autor.

Com relação à proposta da Revisão Sistemática de Literatura, esta pode ser refinada e melhorada no que tange ao escopo da Saúde 4.0 melhorando as *strings* de busca aplicadas nas bases das produções bibliográficas, mas é possível afirmar que o objetivo da mesma foi alcançado, pois os artigos selecionados indicaram métodos ou modelos, arquiteturas e ainda sistemas a partir da tecnologia Blockchain, preocupando-se em destinar atenção a privacidade de dados dos pacientes e avançando nos cenários propostos. Ainda cabe notar, que a revisão sistemática permitiu estudar os principais pontos que podem contribuir para a evolução do trabalho proposto e melhor compreensão do problema definido.

4 BIMHE - BLOCKCHAIN IMPLEMENTATION MODEL FOR HEALTHCARE ENVIRONMENTS

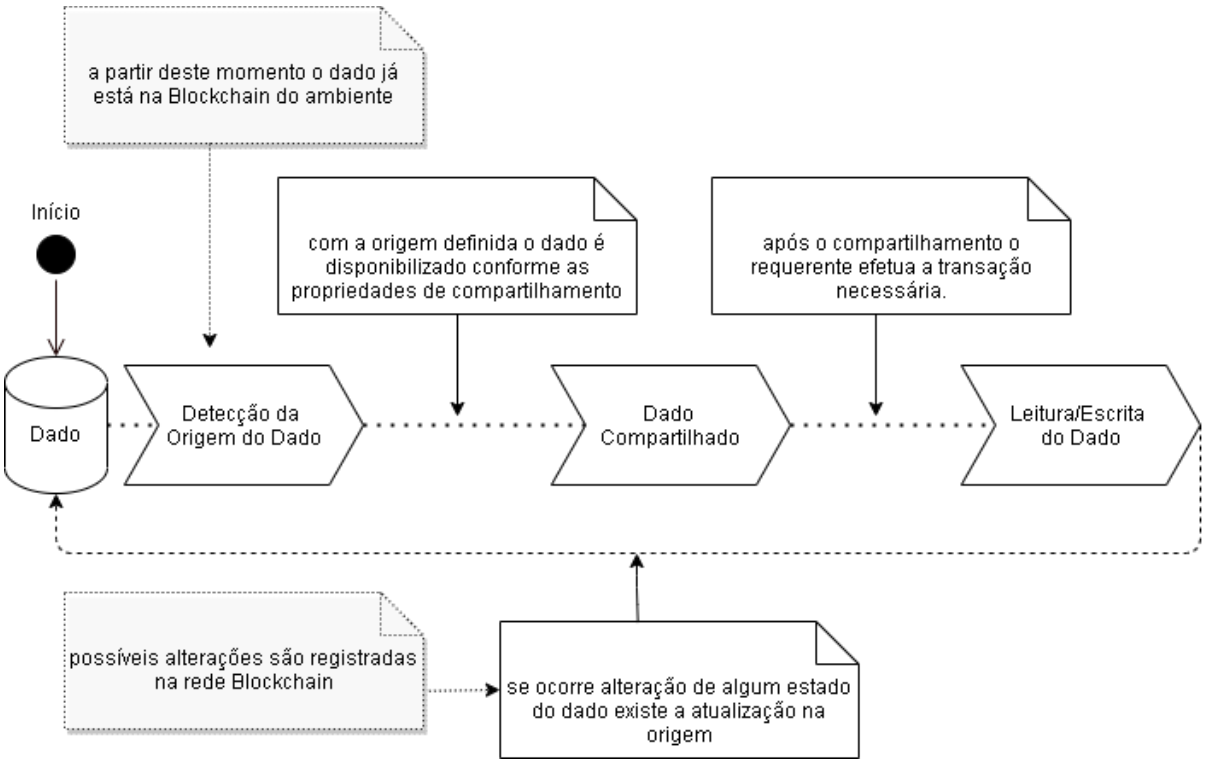
Este capítulo apresenta três visões a partir do qual se implementou o conceito de compartilhamento de dados junto a tecnologia Blockchain. A construção das três visões ocorreu após a Revisão Bibliográfica da Literatura e Revisão Sistemática da Literatura compilando as abordagens dos projetos avaliados e compreendendo a temática proposta, entidades participantes do modelo (paciente, médico, unidade organizacional de saúde) e tecnologias a serem implantadas. Logo, os modelos precedentes, trouxeram vantagens e desvantagens que favoreceram a proposta indicando como utilizar os conceitos aprofundados no referencial teórico. Este projeto vem a dispor de uma proposta para buscar maturidade ao tratar dados sensíveis dos pacientes utilizando Blockchain em ambientes de saúde, com o suporte de conceitos criptográficos.

Dados sensíveis em ambientes de saúde é praxe. A forma como os ambientes tratam tais dados, ainda possui heterogeneidade e discussões onde envolvem pacientes, profissionais de saúde e a organização que está intercambiando estas informações, seja ela privada ou pública. Ao acessar um ambiente de saúde o usuário se depara com sistemas de informação que podem possuir disparidade na forma de autenticação, transmissão e armazenamento. As tecnologias de informação que podem existir ao aceder cenários de saúde precisam ser bem conhecidas e claras no funcionamento, senão podem atrapalhar a experiência do usuário visando o bem-estar. Dados compartilhados por tecnologias devem dispor de regras, cumprindo questões de privacidade, dispondo de mecanismos que indiquem o que pode ser disponibilizado para terceiros e demais condutas sobre as informações pessoais.

Este modelo (BIMHE) visa contemplar o paciente como detentor dos direitos e propriedades sobre seus dados. A preocupação em colocar o paciente como detentor das decisões de liberação no compartilhamento dos dados já foi justificado nos autores dos modelos abordados durante a RSL e conduz a utilização da tecnologia Blockchain. A tecnologia Blockchain, norteadora do modelo, é atuante no controle do ambiente com a informação a ser protegida oferecendo independência ao paciente para detectar o que compartilhar e para quem deve ser disposta estas informações. A primeira ação do modelo é obter o entendimento de como funciona o ambiente Saúde 4.0, pois deve ser possível compreender como os dados serão dispostos, quais dados serão consumidos, para quem os dados serão possíveis de serem utilizados e qual a finalidade.

Para mostrar o fluxo de funcionamento do modelo a Figura 8 exibe uma sequência de etapas corretas para a obtenção do dado minimizando possíveis erros de compartilhamento ou acesso não autorizado. Nesta figura é possível observar a sequência de fatos ocorridos na solicitação de uma informação e a compreensão que desde o primeiro acesso as informações já devem transitar sob a tecnologia Blockchain.

Figura 8 – Sequência proposta para compartilhamento de dados.

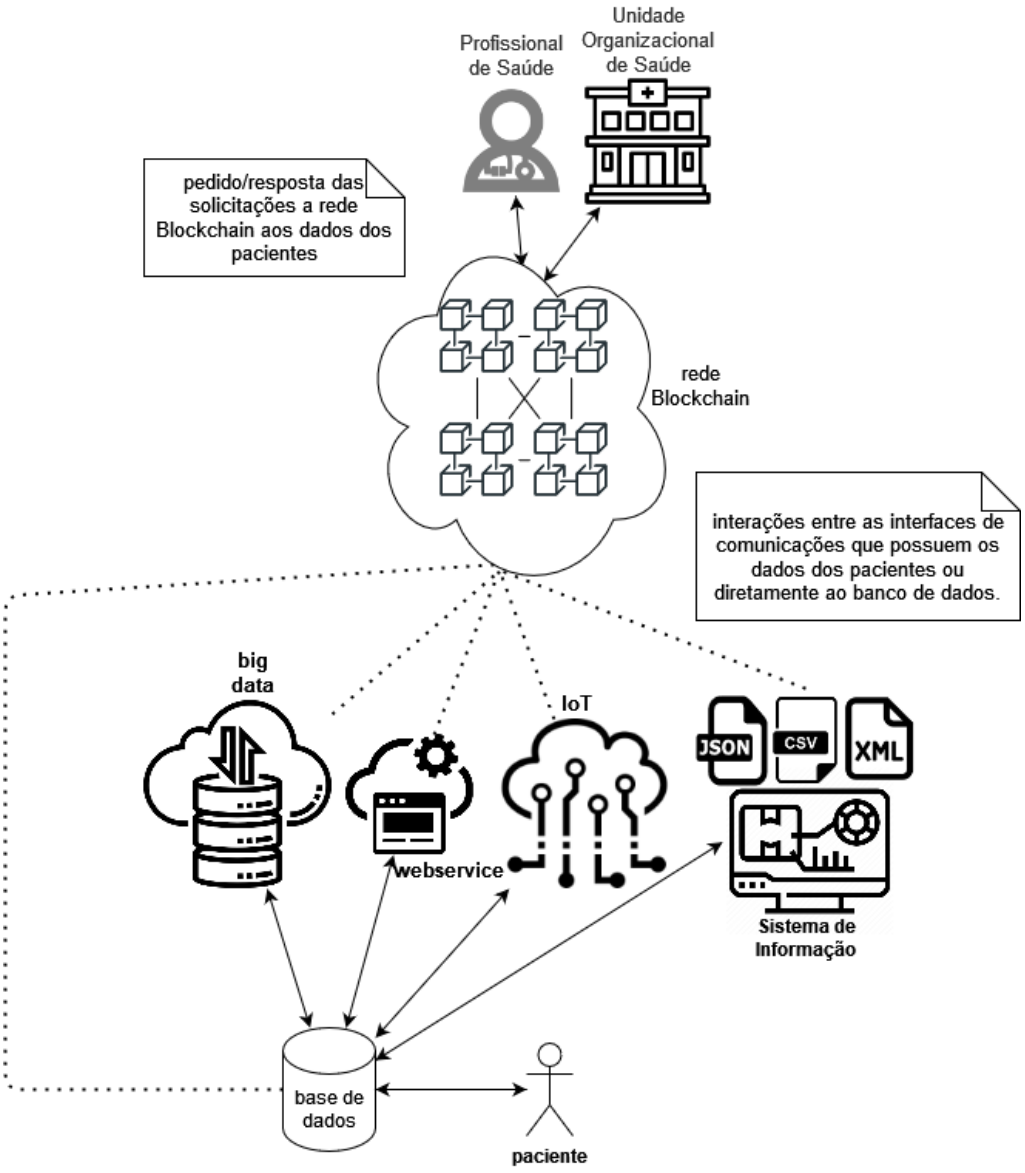


Fonte: Elaborada pelo autor.

Na detecção da origem do dado o usuário e requerente são conhecidos e ocorre autorização do consumo dos dados conforme o que está sendo solicitado e o perfil do requerente. A Blockchain a partir deste momento já faz parte do cenário, identificando os pares e registrando transações. A Figura 8 demonstra o dado compartilhado com a consideração do aceite de compartilhamento do usuário. Caso não exista a autorização nenhuma informação é registrada na Blockchain. Os pacientes (usuários) na rede Blockchain possuem o direito de estabelecer transação com o destino que estes entenderem como válidos, não existindo base de informações pré-cadastradas para isso, mas sim uma autorização prévia e temporária para contemplar o acesso de qualquer origem. Então o médico, por exemplo, para ter acesso aos dados sensíveis do paciente necessita da autorização do paciente e este por sua vez pode aceitar

ou não, ficando esta informação memorizada, dependendo do contexto existente. Na Figura 9 é explorado como acontece à etapa de detecção da origem do dado.

Figura 9 – Detecção da origem do dado.



Fonte: Elaborada pelo autor.

A etapa da detecção da origem do dado é importante, pois é neste momento que se constata a possibilidade do compartilhamento de informações junto ao usuário. Como o objetivo deste trabalho é promover a privacidade do paciente é necessário que exista o consentimento do paciente para o compartilhamento a qualquer interação. Na Figura 9 estão representadas possíveis tecnologias para validar a concepção do modelo. O propósito é definido

a partir da rede Blockchain que inspeciona quaisquer solicitações aos dados dos pacientes, sendo neste caso as interações registradas em cada solicitação, prevendo depuração completa sobre a origem do pedido de leitura/escrita, aos dados, que podem vir por diferentes fontes de acesso e até mesmo de forma direta na base de dados.

Na operação de caracterizar ambiente e dado deve ser possível entender qual a origem do dado, sistema computacional e tecnologia provedora da informação. É importante também identificar a orientação quanto ao fluxo do dado. Sendo o paciente dono e responsável por sua informação a orientação é sempre buscar as propriedades atreladas ao dado, ou seja, as preferências quanto à privacidade deste. Ao procurar a informação necessária deve existir sempre a consulta ao dono do dado que como resultado deve retornar quais variáveis podem ser consultadas e se existe algo sigiloso conforme o perfil do requerente (profissional de saúde, organização, *hardware*, ou até mesmo outro sistema de informação).

Ao solicitar a interação com um dado de paciente, este deve ser utilizado conforme regras definidas pelo usuário e dispostas junto à tecnologia Blockchain. O solicitante ao dado e quem tem a propriedade (paciente), trocam informações criptografadas por meio da rede Blockchain. A rede Blockchain ao reconhecer que a transação pode ser realizada, ou seja, entender que o solicitante possui acesso ao dado executa a transação e concede acesso. Após o conhecimento da transação, esta é registrada na rede Blockchain permitindo auditoria posterior. É válido entender que o modelo propõe a identificação da transação junto à rede Blockchain. A base de dados, neste modelo, está contida na rede Blockchain e possui os dados criptografados visto que é um ambiente público e aberto por padrão. Como o dado estará criptografado, existe a validação de chave pública e privada para depois descriptografar a informação ao solicitante do acesso. As seções seguintes estão dispostas para elucidar o aproveitamento do modelo entendendo diferentes perspectivas de aplicação.

4.1 TERMINOLOGIAS DO MODELO

O modelo possui conceitos que precisam ser esclarecidos para apontar as especificidades da dinâmica e funcionamento do trabalho.

- Paciente: usuário que é o dono do dado e permite a interação a partir da liberação no sistema, acionando assim a ação da troca de chaves. Este usuário é capaz de liberar o acesso à informação ao médico. Este é o único usuário com possibilidades em publicar informação na Blockchain;

- Médico: usuário que necessita da informação do paciente e para isso necessita liberação do paciente na Blockchain, seja para escrita ou leitura na Blockchain;
- Estabelecimento de Saúde: local onde são cadastrados pacientes e médicos;
- Carteira: identificador único de usuário na Blockchain que é necessário para definir as ações solicitadas;
- Blockchain: ambiente Ethereum simulado por meio da tecnologia Ganache que contém todas as transações realizadas no sistema de informação, além do *Smart Contract* e demais regras de acesso.

4.2 VISÕES DO MODELO

O termo "visões" foi utilizado por ser apropriado para se referir a diferentes perspectivas ou abordagens na visualização ou entendimento de um sistema ou modelo. As três (3) visões descritas nas próximas seções são organizadas, para separar atribuições e fundamentar uma melhor compreensão do modelo. O enfoque da **Camada** traz uma forma comum de divisão de níveis ou componentes, enquanto o **Mapa Estrutural** e o **Barramento de Dados** fornecem informações sobre a arquitetura e o fluxo de dados do modelo.

4.2.1 Camadas

As abstrações de camada do modelo existente concebem os serviços de cada camada e como estas são representativas para cada ação a ser realizada. Foram definidas quatro (4) camadas explicadas sobre a ótica *top-down*, a saber. A Camada de Aplicação representa o acesso à estrutura completa do modelo, permitindo quaisquer usuários ou demais aplicações que venham a existir, usufruir dos recursos existentes no ambiente. Na Camada de Acesso são definidas as regras de negócio contemplando as permissões dos usuários, ou seja, tipo de ações que estes podem realizar observando os dados, configurações e propósitos gerais. A Camada Blockchain representa o conjunto de *smart contracts* com as informações sobre cada papel de usuário e associação aos tipos de registros e também contempla as possíveis transações existentes para cada dado provido e/ou inserido. Na Camada de Registro são hospedados os registros dos pacientes, dados pessoais e dados sensíveis sem associação de regras já definidas nas camadas superiores. A Figura 10 representa as camadas e os serviços dispostos entre estas.

Figura 10 – Camadas do Modelo

Fonte: Elaborada pelo autor.

A partir da definição das camadas fica pré-estabelecido uma conduta dependente da ação destas, obrigando a sequência de ações para disponibilização (representação) da informação, ou inserção de um novo dado. Uma camada depende do serviço oferecido da camada subsequente, sendo que os serviços são ações provenientes de um pedido de usuário sobre o dado de algum paciente. As camadas não possuem verificações de erros no próprio modelo, estas estão implícitas no serviço das camadas sendo dependente das tecnologias de comunicação entre as camadas.

Na **Camada de Aplicação** está o suporte de acesso aos usuários finais, neste caso pacientes e profissionais de saúde, que podem interagir, transmitir e receber informações, sua função é definir ou desenvolver aplicações e tecnologias para os próprios ambientes. Então, a Camada de Aplicação serve para os usuários trocarem informações sobre os dados que estão inclusos na Blockchain, a partir de um Sistema de Informação, por exemplo, sendo cada usuário responsável diretamente por acionar cada ação desta camada. Em relação aos serviços que utiliza da camada inferior a Camada de Aplicação necessita das regras contidas na Camada de Acesso, local para tratar a gestão do perfil de cada usuário.

Quanto a **Camada de Acesso**, esta configura a melhor situação do usuário na relação com o dado, seja restringindo ou apontando permissão, garante a segurança dos pacientes, com a geração do par de chaves criptográficos, por exemplo, também traz os acessos às transações e interações médicas com os dados clínicos. Os serviços criptográficos são possibilidades de serviços existentes nesta camada que coloca a condição inicial de acesso a informação como uma das tratativas estabelecidas neste nível de acesso, aplicando por exemplo, critérios de segurança. Neste sentido a camada representa mais uma proteção ao dado e busca na Camada de Blockchain referências de cadastro dos usuários, ratificando o processo completo de acesso ao dado entendendo o perfil dos usuários e possibilitando a informação ser obtida caso a origem solicitante passe em todos os filtros de regras aplicados até o destino, neste modelo o Servidor Blockchain.

Já a **Camada Blockchain** proporciona a interface para a tecnologia Blockchain que habilita o acesso as informações da base Blockchain e registros por ela inclusos nas transações, com a permissão ao dado fornecido após a verificação da carteira de origem, ID de acesso, conferida como válida e com autorização no ambiente Blockchain. Possui também os *smarts contracts* com a escrita das regras de acesso aos dados, demais diretrizes e propriedades do perfil de cada utilizador dos dados a serem transacionados na Blockchain. Esta camada tem por função básica a comunicação com o dado antes de ser inserido na Blockchain, podendo ser este dado oriundo de qualquer interface, base de dados, sistema computacional ou *hardware* de acesso que antes tenham contemplados as questões exigidas na Camada de Acesso.

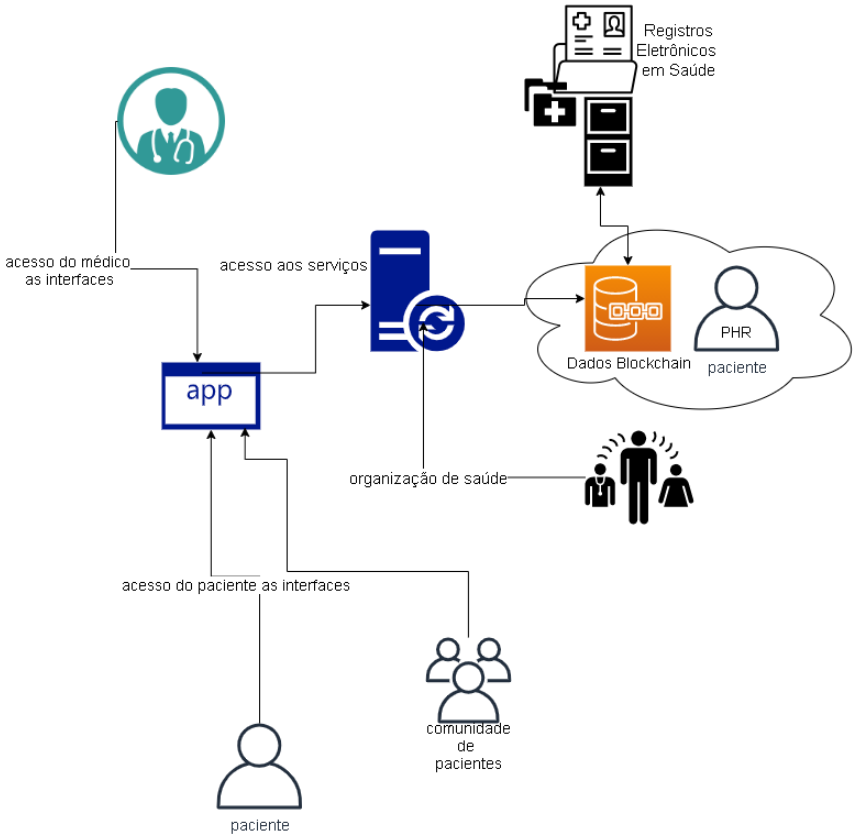
Em relação a **Camada de Registro** esta é a base da cadeia de acesso as informações, pois contém o dado primário de um ambiente Blockchain, ou seja, o conteúdo que tanto médico, assim bem como, o paciente precisam para associar as suas transações. Estes dados obrigatoriamente precisam ter regras associativas da camada superior para serem entregues e manipulados. A informação por si só está criptografada e está protegida por todo o processo de criptografia e vínculo de perfil da forma como a tecnologia Blockchain constrói o armazenamento na base de acesso e contenção dos dados.

4.2.2 Mapa Estrutural

O propósito do Modelo de Negócio, Figura 11, é indicar os possíveis intercâmbios entre as entidades e qual a disposição das informações para quem deseja efetuar alguma ação sobre estas. Para este modelo foram idealizadas três tipos de entidades, classificadas como

“usuário paciente”, “usuário médico” e “usuário organização”. O Mapa Estrutural proposto na Figura 11 exibe o “usuário paciente” em dois aspectos. No primeiro existe a condição da apropriação dos Registros Eletrônicos em Saúde já em um ambiente Blockchain e a comunicação com um sistema computacional servidor que possui interfaces de acesso ao “usuário médico”, “usuário organização” e “comunidade de usuários”, dependendo do controle de acesso.

Figura 11 – Modelo Geral de Negócio



Fonte: Elaborada pelo autor.

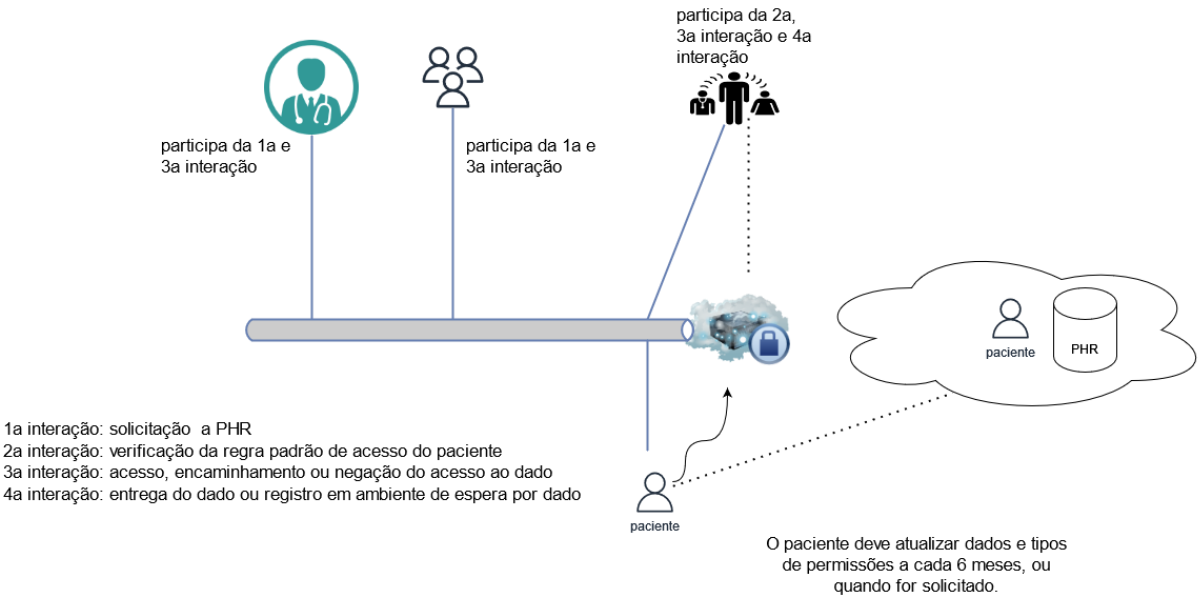
É importante compreender que o “usuário paciente” define as condições de acesso aos dados, em *smarts contracts* junto ao ambiente Blockchain, que também é acionado para registrar as transações de acesso a qualquer informação. O “usuário organização” é representado pela própria aplicação e o “usuário médico” e demais usuários somente podem acessar as funções predispostas em interfaces de uso geral. Os dados do paciente então são armazenados no ambiente Blockchain que trata das permissões de usuários e interações das interfaces de acesso. Na Figura 11 é representado um sistema computacional de coloração azul

que representa todos os serviços oferecidos as aplicações (sistemas) antes de terem conexão com o ambiente Blockchain, neste trabalho o serviço representado é o servidor de chaves para comprovar a liberação a partir de uma determinada carteira digital do requerente.

4.2.3 Barramento de Dados

A reprodução do Barramento de Dados, vide Figura 12, remete as possibilidades lógicas de cada entidade junto ao modelo. O fluxo estabelecido monta a sequência de interações ideal para entregar um dado solicitado. Na 1ª interação ocorre a solicitação do registro privado de saúde, podendo ocorrer por interesse do médico, por exemplo. A organização de saúde fica excluída desta 1ª interação por sem representada por sistemas de saúde, neste caso. Na 2ª interação ocorre a apuração da regra de acesso do paciente para cada dado existente e referenciado. Em se tratando das regras de acesso, existem situações não abordadas na modelagem, no entanto, é uma boa prática a atualização quanto as regras do *smart contract* a cada seis (6) meses para melhor gerir os acordos controlados pela Blockchain. A 3ª interação é o ato sobre os dados solicitados, dependendo do perfil do usuário. E a 4ª interação é o resultado da ação anterior aplicado direto ao dado solicitado.

Figura 12 – Barramento de Dados do Modelo.



Fonte: Elaborada pelo autor.

O Barramento de Dados depende do domínio de usuário para cada ação solicitada. Os dados permanecem sobre propriedade dos pacientes que podem revogar ou dispor informações

de acordo com o interesse e relacionamentos a serem desenvolvidos conforme for à vivência dos pacientes em cada organização de saúde. O barramento aponta um fluxo de dados do modelo onde às ações ocorrem entre emissor (solicitante da informação) e receptor (paciente) que interagem nas solicitações de informação.

5 ESTUDO DE CASO

Este trabalho de pesquisa aplicado em um ambiente controlado suportou o modelo denominado BIMHE descrito no capítulo 4. Foram utilizadas tecnologias para prover o cenário de interação entre paciente e médico, simulando as solicitações e entrega de dados sensíveis. Visto que é um projeto piloto, os dados são hipotéticos e as ações para validar o modelo foram articuladas respeitando o escopo definido nesse trabalho.

A escolha de qual tecnologia Blockchain utilizar foi fundada a partir das características técnicas necessárias para gerir uma estrutura complexa como o Ethereum. A tecnologia proposta nesta pesquisa, Ethereum, requer cuidados especiais para situações específicas e críticas, tais como: espaço em disco, pois o Blockchain do Ethereum ocupa atualmente mais de 1 TB de espaço em disco e em constante crescimento. Além do espaço em disco, a manutenção da Blockchain do Ethereum requer muitos recursos de processamento e memória, o que afetariam os testes do BIMHE, pois seria necessário a sincronização completa com os pares da rede, outro problema a ser gerido, devido a obrigatoriedade em manter conexões confiáveis e constantes com outros nós da rede para validar as transações.

Com as dificuldades definidas foi escolhido o Ganache (Simulador Ethereum), devido à natureza específica em reproduzir um ambiente Ethereum e com a opção de carregar os *smarts contracts* para serem executados na Blockchain simulada. Outra facilidade do Ganache é a da manipulação das chaves criptográficas, isto é importante para os testes executados na validação do objetivo proposto que visa a privacidade dos dados, além disso, por possuir uma interface gráfica acessível é possível visualizar de maneira mais amigável as transações, carteiras digitais dos usuários e registros (*logs*). Complementarmente é importante citar que a mineração dos blocos é automática da própria ferramenta então as transações são instantâneas sem intervenção do usuário, permitindo simulação de transações e contratos inteligentes localmente, em um ambiente seguro e isolado, sem a necessidade de gastar recursos ou taxas na rede Ethereum.

Já para a construção dos *smarts contracts* a linguagem Solidity com a IDE Remix, foi escolhida devido a compatibilidade com a Ethereum e também em consequência de apresentar recursos integrados de segurança que auxiliam a prevenir vulnerabilidades comuns, como: *Stack overflow*, *Integer overflow*, *Reentrancy attacks* e chamadas a contratos desconhecidos. Os contratos então ficam armazenados na Blockchain e são componentes essenciais das regras de negócio do modelo proposto. Na Blockchain também ficam os registros dos pacientes, mas

como o ambiente é aberto os dados são criptografados e respeitam os contratos inteligentes e a troca de chaves do requerente e do paciente proprietário da informação.

A estratégia da pesquisa se preocupou também com a arquitetura do projeto devido as interações e ecossistema de tecnologias existente. É importante entender que o solicitante quando necessita da informação de tal paciente deve requerer autorização a informação, respeitando as decisões do paciente. No entanto, já que a rede Blockchain utilizada foi suportada pela tecnologia Ganache, se teve a necessidade em criptografar os dados para dificultar possíveis hostilidades. Na interação entre solicitante e detentor do dado ao identificar a origem do requerente, existe então a troca de chaves para que a transação ocorra.

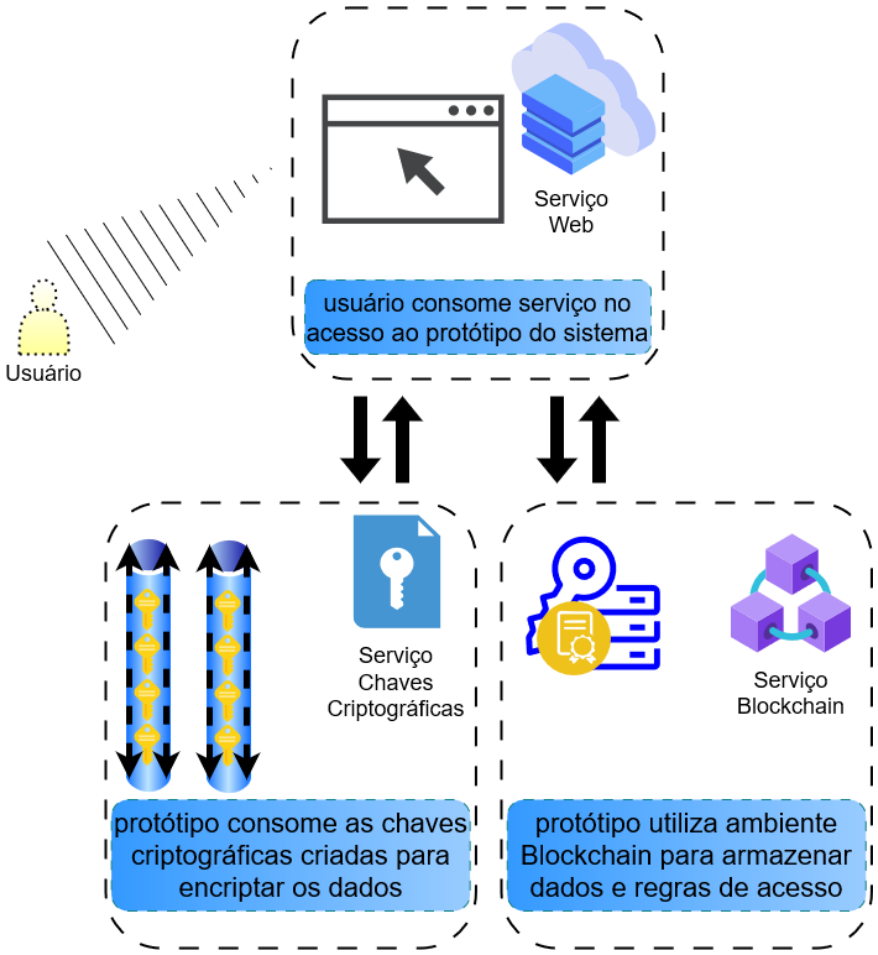
5.1 ARQUITETURA DO PROJETO

Para o BIMHE foi desenvolvido um ambiente, onde são simulados os serviços oferecidos. De modo a simplificar o que foi formulado, uma arquitetura básica do projeto é exposta na Figura 13, e de forma genérica delimita o escopo tecnológico e serviços oferecidos. Os serviços na arquitetura podem ser descritos da seguinte forma, a saber:

- Serviço web: foi desenvolvido um protótipo de aplicação *web* com o objetivo de tornar válido o processo mínimo de funcionamento de um sistema, com opções de leitura e escrita, atrelada a identificação da carteira do usuário. Neste caso o processo mínimo possui o cadastro do médico e paciente em cada estabelecimento de saúde (protótipo), além da consulta das informações da Blockchain. O serviço *web* foi instalado e configurado a partir da tecnologia Apache e desenvolvido a partir do HTML 5 e Java;
- Serviço Chaves Criptográficas: também, a partir da linguagem Java foram desenvolvidas duas funções para criptografar os dados antes de serem incluídos na Blockchain e descriptografar os dados na consulta de informações. O conceito de criptografia assimétrica foi utilizado com o compartilhamento da chave pública do paciente quando necessário. A chave pública do paciente é utilizada pelo paciente e também compartilhada pelo médico via sistema de informação (protótipo) quando este necessita do acesso a informações na Blockchain. A chave privada do paciente é armazenada no servidor de chaves para depois ocorrer o acesso ao dado na Blockchain. O *framework* Quarkus foi utilizado para gestão das chaves e comunicação junto ao ambiente Blockchain;

– Serviço Blockchain: os dados criptografados ficam armazenados no ambiente Blockchain, neste projeto, instalado e configurado a partir da tecnologia Ganache que simula um ambiente Ethereum. Junto ao Ganache está também o *Smart Contract* escrito para este projeto, onde existe o critério para aceitar a escrita e leitura dos dados na Blockchain, a partir da carteira de identificação do solicitante. Os dados chegam a Blockchain criptografados, mas são acessados a partir das regras do *Smart Contract* que avalia se a origem solicitante, o endereço da carteira, possui permissão para a ação requerida.

Figura 13 – Arquitetura Básica do Projeto.

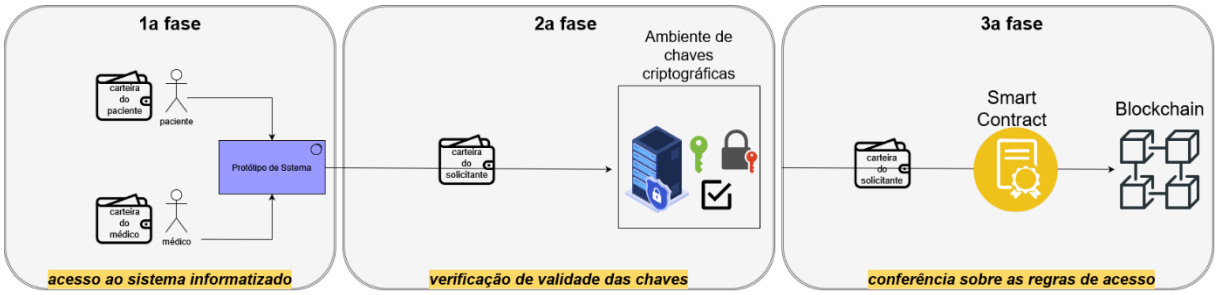


Fonte: Elaborada pelo autor.

A arquitetura do projeto, representada na Figura 13, mostra a sequência e interação dos funcionamento dos serviços. Estes processos, na Figura 14, são detalhados em três fases de interação do projeto, apoiadas na ideia do BIMHE em fixar o paciente como dono da sua própria

informação, com as fases do projeto limitadas a partir dos serviços oferecidos e resultados das interações após cada processo construído.

Figura 14 – Fases de interação dos serviços oferecidos.



Fonte: Elaborada pelo autor.

Num primeiro momento, na 1ª fase, ocorre o processo natural da utilização do sistema de informação, neste caso o protótipo implementado. Este oferece a interface ao médico ou paciente, com cadastro e consulta, onde o médico pode, a partir da seleção do paciente, por exemplo, escrever o prontuário ou efetuar consultas, sendo que na 1ª fase o médico e paciente ao acessarem o sistema informam a carteira vinculada a Blockchain, existindo assim a identificação do solicitante. Quando o paciente utiliza o sistema, este já possui a ação em liberar a carteira digital do médico entregue após a Blockchain, todavia, se o usuário no sistema for o médico é necessário a liberação anterior para assim conseguir o acesso ao dado na Blockchain, já que o médico não possui acesso inicialmente a liberação a partir dos perfis de acesso.

Então, na fase inicial, existe a identificação do usuário no sistema, que acontece a partir do acesso, onde contém as informações de cadastro, tal como a carteira digital para existir a identidade estabelecida no sistema e no ambiente Blockchain. Após isso, na 2ª fase o objetivo é criptografar a informação para manipular o dado na Blockchain, assim acontece a comunicação do sistema de informação com o servidor de chaves criptográficas, que armazena a chave pública e privada do paciente e gerencia o tempo de utilização de cada par de chave. Assim, a partir do sistema de informação ocorre a ação de criptografia do dado com a chave pública e privada do paciente armazenada no servidor de chaves criptográficas, posteriormente sendo o dado encaminhado à Blockchain.

No processo de tráfego do dado, o servidor de chaves criptográficas atua depois da 1ª fase para conferir a origem da informação enviando para o ambiente Blockchain o dado criptografado. Quando o dado é devolvido da Blockchain para o Sistema de Informação existe também o processo inverso da criptografia, onde no Servidor de Chaves Criptográficas a ação

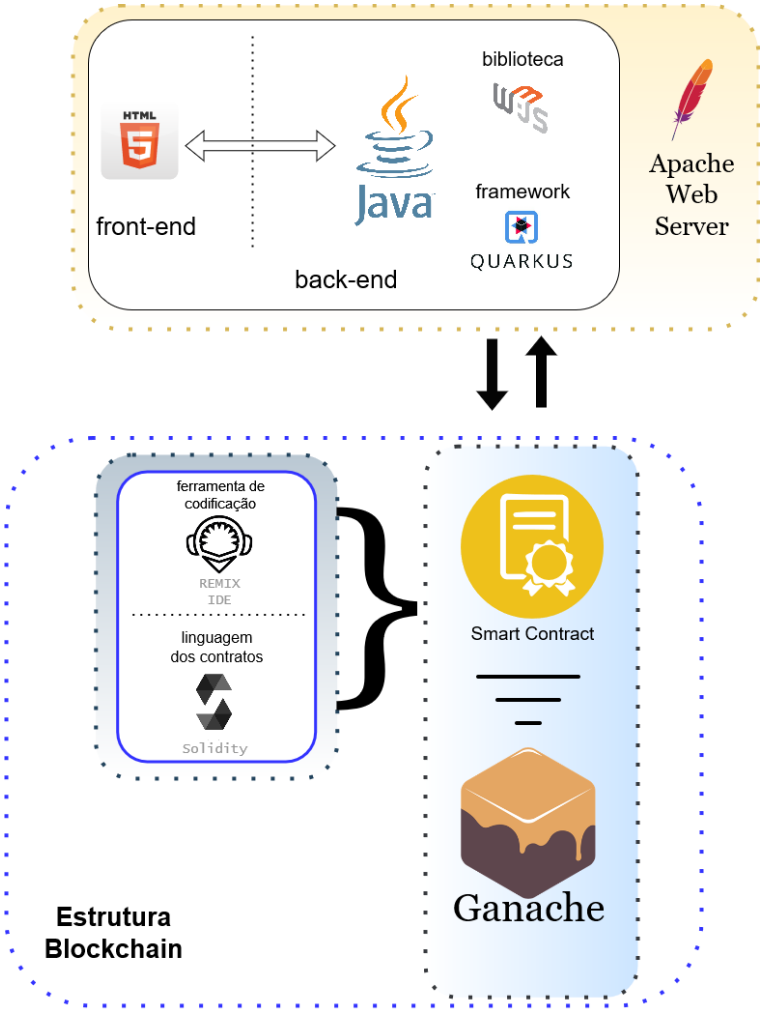
para descriptografar o dado ocorre a partir da verificação do par de chaves, encaminhando assim a informação legível para o sistema de informação.

A 3ª fase é dedicada as regras existentes na Blockchain a partir do *Smart Contract* desenvolvido. No *Smart Contract* existe a definição das chamadas possíveis ao ambiente Blockchain, vinculações de carteira, cadastros e regras de acesso. O dado é recebido e enviado criptografado e as requisições respeitam o processo normal da tecnologia Blockchain, a partir da tecnologia Ganache.

5.2 TECNOLOGIAS

Para o desenvolvimento do modelo foi necessário implementar uma ferramenta *web* que simulou o funcionamento da rotina do paciente, médico e estabelecimento de saúde. Diante deste aspecto as seguintes tecnologias, vide interação na Figura 15, foram utilizadas para a criação desta ferramenta, a saber: HTML, Java, a biblioteca de apoio web3.JS, Apache, Remix IDE, Solidity e Ganache.

Figura 15 – Interação das tecnologias para desenvolvimento do protótipo de ferramenta.



Fonte: Elaborada pelo autor.

A linguagem de marcação HTML, na versão 5, foi utilizada como linguagem de programação para a interface gráfica do projeto. Já, para possibilitar o desenvolvimento das regras de negócio da ferramenta *web* criada, se usou a linguagem de programação Java. Em conjunto com o Java uma biblioteca específica também foi aplicada: a web3.JS, particular para interagir com a tecnologia Blockchain acessando as transações geradas. Como servidor *web*, foi utilizado o Apache 2.4.54, provendo o conteúdo de acesso das páginas. Já para a tecnologia de servidor de chaves foi utilizado o framework Java de microsserviços denominado Quarkus, que também se comunica com o ambiente de Blockchain para gerir os acessos.

Na criação do ambiente Blockchain, que deu suporte ao projeto foi utilizado a tecnologia Ganache, versão 2.6.0, para emular a rede Blockchain onde são registradas as informações das transações e ocorre a persistência dos dados. Para a escrita e manipulação dos

Smarts Contracts, foi escolhido o aplicativo de programação Remix IDE, utilizando então a linguagem de programação Solidity, com intervalo de compilador de 0.7.0 a 0.9.0.

5.3 DOCUMENTAÇÃO

Esta seção possui a documentação do projeto com declarações sobre como o processo de negócio, sob qual a ferramenta foi desenvolvida, condicionou a criação do modelo. As lógicas apresentadas são direcionadas a construção das ações dos usuários, interpretando as situações de publicação, liberação e consulta dos dados pessoais e dados pessoais sensíveis.

5.3.1 Regras de Negócio

Segundo Pressman e Maxim (2016), as regras de negócio descrevem ao usuário os preceitos relacionadas à execução de sistemas, ou seja, definem ou delimitam as características dos processos de um negócio. Neste trabalho é importante definir as regras de negócio do modelo que precisam ser inclusas no protótipo da ferramenta para esclarecer quais relações podem existir nas transações. Para a escrita do *Smart Contract* e para a definição de como funciona a comunicação entre interface gráfica, *back-end* e ambiente Blockchain é crítico estabelecer as atribuições, limites e fluxo das ações de cada usuário. O Quadro 13 aponta as regras de negócio estabelecidas para o desenvolvimento da ferramenta.

Quadro 13 – Regras de Negócio do Protótipo de Sistema.

IDENTIFICADOR	NOME	DESCRIÇÃO
RN01	Validação do Paciente	Todo paciente precisa cadastrar os dados pessoais por completo para ser registrado em uma organização.
RN02	Dados Paciente	O paciente poderá compartilhar os dados pessoais e dados pessoais sensíveis mediante a liberação da carteira vinculada a solicitação.
RN03	Validação Médico	Todo médico precisa cadastrar os dados pessoais por completo para ser registrado em uma organização.
RN04	Liberação Dados Paciente	O médico poderá acessar os dados pessoais e dados pessoais sensíveis do paciente após solicitação individual ao paciente informando a carteira de origem.
RN05	Compartilhamento dos dados organizacionais	Uma organização não poderá compartilhar com qualquer entidade (pessoa, *hardware* ou sistema) os dados pessoais e dados pessoais sensíveis do paciente.
RN06	Compartilhamento dos dados organizacionais	Uma organização precisa o visto do paciente ao compartilhar dados pessoais e dados pessoais sensíveis entre instituições para fins estatísticos, informarndo a carteira de origem.

Continua...

IDENTIFICADOR	NOME	DESCRIÇÃO
RN07	Lógica para Publicar	O único usuário com permissão para publicar dados na Blockchain é o paciente.
RN08	Segurança para Publicar	O dado publicado na Blockchain deve ser criptografado.

Fonte: Elaborado pelo autor.

As regras de negócio foram estabelecidas mediante a construção do modelo. Estas propostas apenas se aplicam para o ambiente simulado e controlado em questão e definem os três perfis de usuários e as ações pertinentes com base no modelo. A cada usuário é associado um carteira, com um identificador que proporciona a referência da origem das ações.

5.3.2 Diagrama BPMN (Business Process Model and Notation)

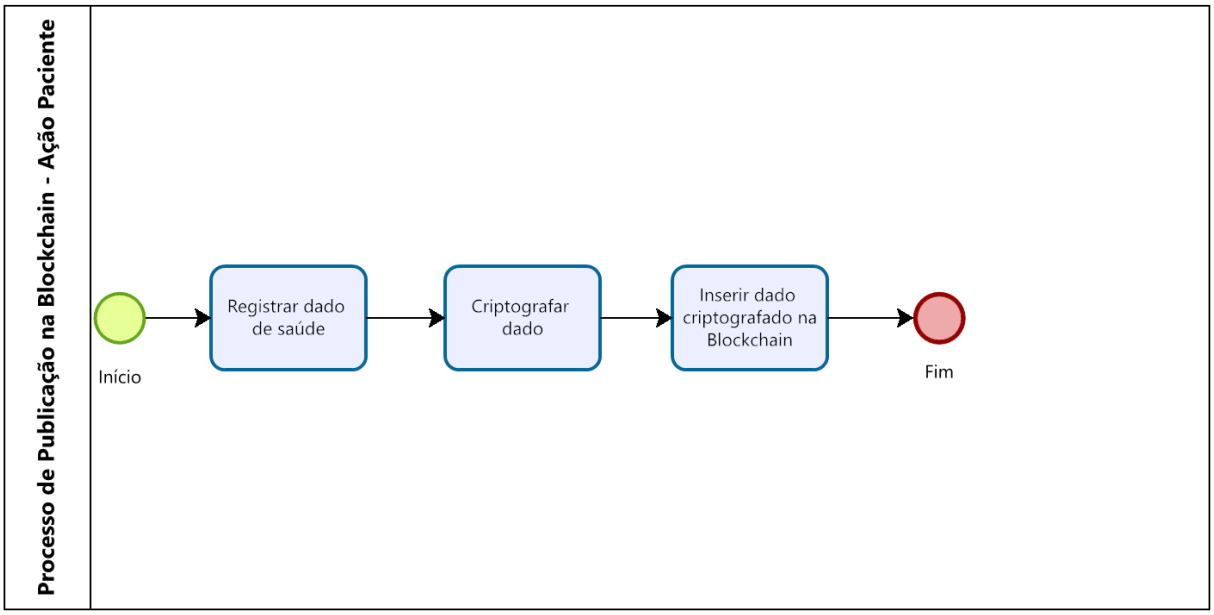
Um diagrama intitulado como BPMN é estabelecido para modelar, construir, identificar, executar, monitorar, continuar e melhorar processos de negócio (Object Management Group, 2022). Neste trabalho o conceito para construir este tipo de diagrama se utilizou para mostrar como e com que embasamento lógico de processos o modelo foi construído. São compreendidos três fases durante o modelo, 1) a ação do paciente em gravar informações na Blockchain; 2) a liberação no qual o paciente realiza para quem precisa do dado, a ele pertencente, contido na Blockchain; e 3) a solicitação de acesso aos dados do paciente contidos na Blockchain, neste caso, realizado pelo médico.

O paciente, no modelo, simboliza o dono da informação, tanto para os dados pessoais, assim bem como os dados pessoais sensíveis e possui autonomia para determinar quem vai ter acesso aos dados criptografados na Blockchain. Então, o modelo permite que o dado seja inserido na Blockhain somente pelo paciente, tendo outros usuários como opção a consulta da informação, se for autorizada. Toda solicitação está atrelada a uma carteira, que identifica e condiciona a ação mediante a permissão do paciente. São estas possibilidades que estão representadas nos diagramas de negócio a seguir.

O primeiro diagrama, Figura 16, explica a inserção de informação criptografada do paciente na Blockchain. A ação parte do paciente, e como este é dono do dado a carteira já é identificada como sendo autorizada, não precisando a verificação das credenciais de acesso, se limitando a informar os dados de saúde, criptografar os dados de saúde e após inserir os dados criptografados na Blockchain. É válido lembrar que o paciente é o único usuário neste modelo

previsto para publicar informações na Blockchain, devido aos conceitos projetados no modelo que atrelam quaisquer alterações de informações e liberação de acesso, ao dono do dado.

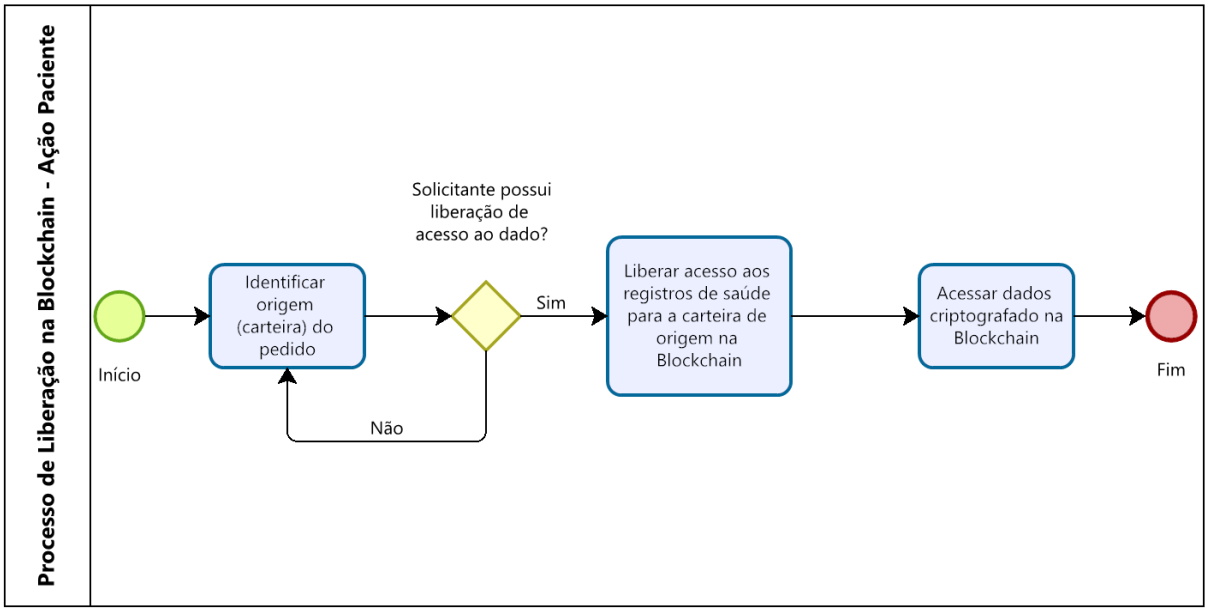
Figura 16 – Caminho para a publicação de dados.



Fonte: Elaborada pelo autor.

Já no segundo diagrama, na Figura 17, a ação esperada é a liberação aos registros de saúde para uma carteira. É preciso então permitir o acesso a determinada carteira na Blockchain e para isso existe a necessidade em identificar a origem (carteira) e condicionar o solicitante, ao paciente que está realizando a liberação. Está lógica de liberação configura uma carteira de um médico, por exemplo, ao acesso de um determinado paciente na Blockchain.

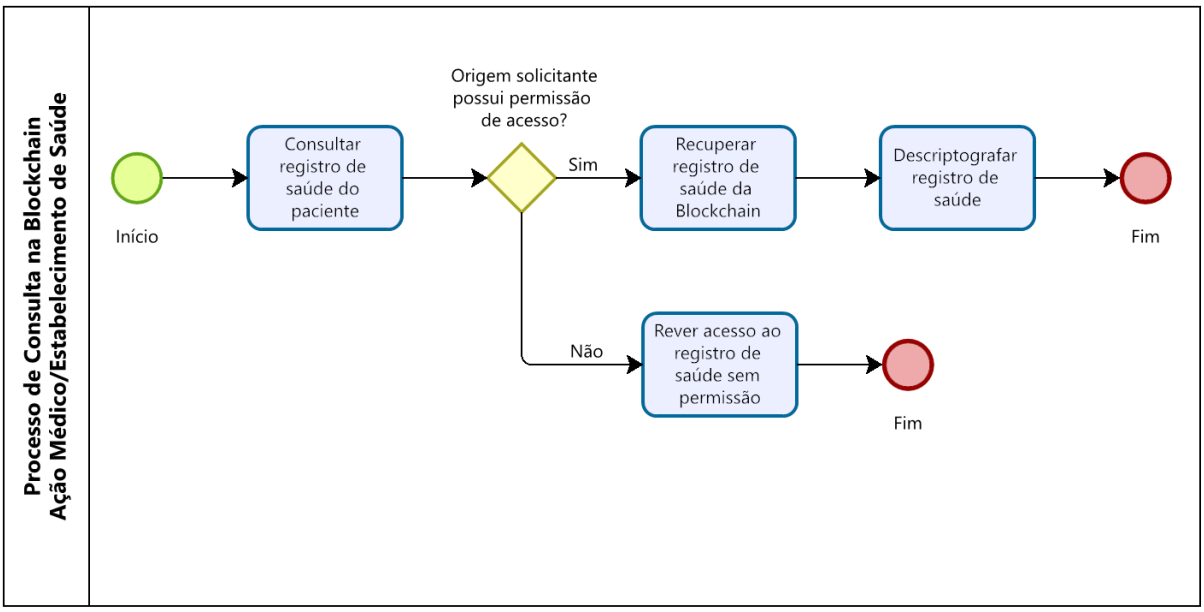
Figura 17 – Caminho para a liberação no ambiente Blockchain.



Fonte: Elaborada pelo autor.

No terceiro diagrama, vide Figura 18, existe a representação das consultas a Blockchain. É esperado o comportamento de condição para avaliar se a origem solicitante é uma carteira válida com permissão de acesso já estabelecido na Blockchain e caso exista a permissão o registro de saúde é recuperado da Blockchain e depois descriptografado sendo assim, entregue ao solicitante. No entanto, senão existir esta opção de conseguir o dado é informado que os registros solicitados foram recusados, sendo necessário novo pedido de consulta, ou seja o retorno dos dados existentes na Blockchain só acontece com a permissão para obter a informação, por meio da liberação de acesso pelo paciente.

Figura 18 – Caminho para consulta de informações na Blockchain.



Fonte: Elaborada pelo autor.

Os diagramas de negócio sustentam a ideia do modelo aplicado ao conceito do PHR, pois neste tipo de registro quem mantém a informação sob domínio é o próprio paciente, permitindo o uso somente quando lhe cabe. Gerado os diagramas fica claro a dependência do modelo no paciente que é consultado a todo momento quando é necessário a utilizado dos dados que lhe pertencem.

5.4 AMBIENTE SIMULADO E CONTROLADO

Todo o ambiente foi definido a partir de aspectos estabelecidos para validar a proposta do modelo entregando o cenário mínimo para executar os serviços esperados. Nesta seção são descritas as particularidades do projeto prático que procurou validar o BIMHE, com a possibilidade em implantar o mesmo modelo utilizando de outras tecnologias.

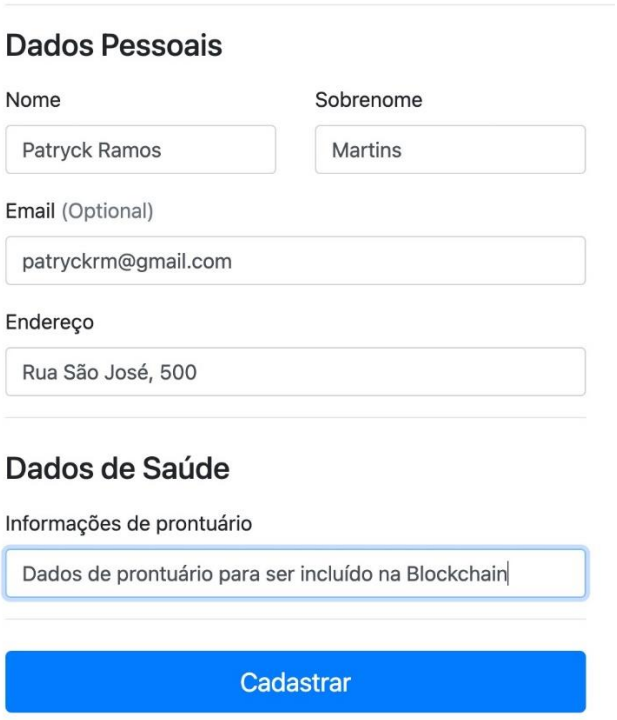
5.4.1 Protótipo Desenvolvido

Para entender as funções descritas no modelo um protótipo foi criado para simular as ações do médico e a interação com o paciente. É importante lembrar que as funções foram adequadas estimulando o conceito de privacidade e respeitando os aspectos codificados nos *smarts contracts*. A interface gráfica criada procurou mostrar os cadastros realizados por

médicos, os acessos devidos e indevidos, os dados criptografados e visíveis a partir do perfil encontrado nas regras do *smart contract*. É válido explicar que as janelas desenvolvidas são prova de conceito para o BIMHE, prática utilizada para demonstrar a possibilidade de validação de um protótipo, por exemplo, não sendo parte do projeto o desenvolvimento de um sistema por completo. A versão atualizada do protótipo está disponível no endereço https://github.com/patryckrm/.

A primeira janela exibida na Figura 19, foi criada para inserir novos registros na Blockchain. É uma janela com cinco (5) campos para demonstrar a interação com o Ganache que simulou o Ethereum, salvando os dados em um ambiente Blockchain, onde informações foram cadastradas, mas logo em seguida criptografadas com a chave pública existente no repositório de chaves. O serviço de chaves possui as chaves públicas e privadas e com isso é possível em certo momento também capturar a mesma informação cadastrada, descriptografando quando necessário ter acesso a esta.

Figura 19 – Tela de inserção de novos registros na Blockchain.



Fonte: Elaborada pelo autor.

Na Figura 20 é exibido o segundo recorte de interface que demonstra uma situação de proteção ao dado. A figura não deve ser entendida como uma tela de um sistema funcional, pois o propósito não foi a criação de um sistema para ser usado, mas sim para provar um conceito.

Então, esta janela só mostra que, mesmo se o paciente (usuário) Patryck fosse arriscar visualizar, inserindo, por exemplo, o ID de outro paciente, ou seja, tentasse de alguma forma ludibriar o sistema para carregar todos os registros, estes estariam criptografados. A exibição desta janela é só uma prova do conceito de privacidade sendo respeitado.

Na prática, em um sistema de informação, o usuário Patryck nem visualizaria, mas para isto não acontecer, poderia ser criado um sistema com filtro, não precisaria criptografar. A representação na Figura 20 foi só uma prova de conceito para demonstrar que mesmo o usuário listando ou na ausência de um filtro em um sistema o que vai ser retornado é o dado criptografado, demonstrando assim uma garantia a mais de segurança, que pode ser representado no modelo na Camada de Acesso.

Figura 20 – Dados na Blockchain de pacientes diferentes, pela visão do paciente Patryck.

Fonte: Elaborada pelo autor.

Já a Figura 21, capturada do protótipo remete a tentativa do médico em acessar informações não condizentes com o seu perfil. Como não teve liberação prévia do paciente o médico não possui a chave correta de acesso para a descriptografia da informação e o ID que este acessa também não está incluso na lista dos usuários permitidos. Se por algum motivo o médico tentar o acesso indevido as informações estarão criptografadas.

Figura 21 – Visão do médico sem liberação e visualização dos registros cadastrados.

Fonte: Elaborada pelo autor.

A quarta janela, Figura 22, mostra uma carteira a ser liberada de um médico que tem a necessidade em acessar informações de um determinado usuário (paciente). Neste momento acontecem duas ações a carteira é liberada no *smart contract* para acessar os registros do paciente que o liberou, além disso, a carteira tem acesso ao processo de troca de chaves (chave pública e chave privada), do paciente efetuando liberação. O médico não possui acesso às chaves porque estas não são liberadas, mas como este tem a permissão de acessar o dado existe a ação criptográfica para o retorno do dado.

Figura 22 – Paciente Patryck liberando o acesso aos dados para a carteira do Médico.

Fonte: Elaborada pelo autor.

Em seguida a janela da Figura 23 representa um médico após a ação de dois pacientes que liberaram a carteira específica, consegue alterar informações, no caso do usuário Patryck e visualizar no caso do usuário Leila. Independente do propósito, seja para editar ou verificar informações de um paciente o médico precisa da liberação deste, que identifica no Blockchain a partir dos *smarts contracts*, a permissão de acesso ao médico.

Figura 23 – Visão do médico após dois pacientes liberarem o acesso.

Fonte: Elaborada pelo autor.

Os recortes de janela representam o propósito geral de uma forma prática do que o modelo definiu onde o acesso do médico aos dados dos pacientes é uma questão crítica na área da saúde e representada neste modelo. Embora os dados dos pacientes sejam protegidos por direito, é necessário que os médicos possam acessá-los de maneira segura e eficiente para prestar um tratamento adequado. A criptografia utilizada neste modelo foi a RSA, onde o processo de transformação de informações legíveis em códigos ilegíveis, são propícias para maximizar o processo da privacidade dos dados, tornando as informações seguras para serem compartilhadas e quando os dados dos pacientes são armazenados em um sistema de gerenciamento eletrônico de registros médicos estes podem ser criptografados para protegê-los contra acesso não autorizado.

Para que os médicos possam acessar os dados criptografados dos pacientes, foi então necessário a criação de um *smart contract* que executa automaticamente os termos do contrato, com os termos e as condições do acesso aos dados dos pacientes onde existe o filtro da liberação das carteiras de médicos liberados respectivamente por cada paciente. Os *smarts* contracts junto ao processo de criptografia garantem que apenas usuários autorizados tenham acesso aos dados dos pacientes. O dado encriptado é a garantia mínima na Ethereum, para garantir que os dados dos pacientes permaneçam seguros, significando que mesmo alguém acessando os dados, não poderão entendê-los sem a chave de criptografia correta. O processo então exige que os médicos forneçam as carteiras, para verificar a identidade antes de permitir o acesso aos dados, adicionada ao processo de liberação realizado pelo usuário.

5.4.2 Características

Em termos de hardware foi utilizado um computador portátil (*notebook*) com processador Intel(R) Core(TM) i7-8565U com base de processamento em 1.80GHz, memória primária (RAM) de 8,00 GB, disco de armazenamento do tipo SDD de 500GB. O sistema operacional utilizado foi o MS Windows 11 Home Single Language, versão 22H2, com compilação de SO 22621.1265.

O sistema computacional descrito utilizado foi capaz de suportar o BIMHE a partir das tecnologias escolhidas que possuíam o escopo em validar o ambiente posto. Os serviços foram instalados e configurados localmente (modo *localhost*), sendo providos então a partir do sistema operacional no hardware já citado. As tecnologias funcionaram da seguinte maneira, a saber:

- Servidor Web Apache: porta 80 para provimento do front-end (telas);
- Simulador do Ethereum – Ganache (Ambiente Blockchain): porta 7545 para suportar a simulação da rede Ethereum, ambiente Blockchain com a vinculação do Smart Contract;
- Servidor de Chaves Criptográficas: porta 8080 para as regras de negócio existentes nas trocas de chaves e processo criptográfico.

Estes foram os serviços providos para permitir a validação conceitual do BIMHE, a partir do escopo local de funcionamento com os usuários e interações pré-estabelecidas.

5.4.3 Codificação

A etapa de codificação visa transformar as funcionalidades da prática do projeto que foram especificadas anteriormente, em código fonte. O código fonte deste projeto foi disponibilizado no endereço https://github.com/patryckrm, onde usuários autenticados podem efetuar o *download* do projeto completo. Em todos os serviços ofertados foi necessária a escrita de algoritmos para contemplar o propósito do projeto.

É importante destacar o *Smart Contract* criado, que teve como critérios as relações dos fluxos de negócio e o entendimento sobre a manipulação e tráfego da informação a ser consumida. Este também respeitou as interações entre os usuários levando em consideração os perfis de acesso. Na Figura 24 é disposto um trecho de código do *Smart Contract* desenvolvido para este trabalho.

Figura 24 – Trecho de código do Smart Contract.

```
function consultarRegistroSaude( uint index ) public view returns (RegistroSaude memory r) {
    console.log ("registros ", registros.length );
    if ( registros.length >= index ) {
        r = registros[index];
    }
    address solicitante = msg.sender;
    address paciente = r.dono;
    for
    return r;
}
```

Fonte: Elaborada pelo autor.

O trecho de código mostra uma função ao médico que disponibiliza todos os registros de saúde salvos em um paciente. Vale ressaltar que a interface de acesso disposta neste trabalho interage em diversos momentos com o Ganache (simulador Ethereum de Blockchain) onde é chamado o *Smart Contract* e funções existentes no código fonte. Demais códigos desenvolvidos que são importantes para este trabalho podem ser vistos no apêndice deste documento.

5.5 CONSIDERAÇÕES FINAIS DO AMBIENTE

O ambiente estabelecido para legitimar o BIMHE teve a essência em justificar o funcionamento do compartilhamento correto da informação respeitando o conceito de privacidade do dado entendendo que o dono precisa compreender o porquê de toda solicitação.

As tecnologias escolhidas para o ambiente foram definidas a partir do conhecimento do autor aliado as dificuldades encontradas com outras soluções análogas, mas custosas em termos de *hardware*, processamento e custos com hospedagem externa. Evidentemente que novas tecnologias de virtualização afetam positivamente o correto provisionamento dos requisitos mínimos de *hardware* exigidos, mas o foco do trabalho estava na validação do modelo, então a proposta em *hardware* local conseguiu atingir como finalidade simular as fases e visões de funcionamento do modelo.

Os problemas relacionados a implantação do ambiente prático foram encontrados no custo da tecnologia Blockchain e o processamento que esta precisa, e por isso a opção de implantação em *hardware* local ocorreu. Existiu a necessidade da criptografia dentro do Ganache, que é o simulador Ethereum (tecnologia Blockchain), pois os dados são públicos ficando mais vulneráveis senão houvesse a criptografia da informação. Quanto a criptografia se utilizou a assimétrica (par de chaves) com o algoritmo do tipo RSA, pois foi necessário a interação entre paciente e médico sendo mais propício o compartilhamento de chave pública para criptografar a informação e chave privada para descriptografar.

A implantação, na prática, prova que valorizando o dado armazenado e gerenciando a partir do paciente minimiza fatores subjetivos e garante a privacidade dos dados envolvidos no ambiente pré-especificado, além disso mostrou que o entendimento dos fluxos de processamento para conseguir a informação possibilitou uma melhor disponibilidade de todos os recursos funcionais envolvidos.

As interações ocorreram de forma gradual simulando as ações do paciente e posteriormente do médico, sendo o sistema atrelado a um estabelecimento de saúde. A sistemática da validação não se preocupou em quantidade de dados, ou outro tipo de parâmetro e ação. Não existiu uma amostragem definitiva de dados catalogados, pesquisados ou inseridos na Blockchain, a partir do conceito de amostragem não probabilística por conveniência, onde o autor pode definir a quantidade de amostras válida para um determinado projeto.

5.5.1 Métricas

Em se tratando do comportamento final do modelo é importante comparar suas funções e objetivos alcançados com os modelos dos autores detalhados na Revisão Sistemática da Literatura. É importante perceber que as características elencadas no Quadro 12, “Comparação das publicações analisadas”, trazem um panorama geral e traçado para os objetivos deste

trabalho, mas é interessante levantar outros pontos para melhorar a forma de compreensão da referida pesquisa.

Um aspecto conceitual importante que confronta o BIMHE, com os autores analisados é a forma de abordagem quanto aos trabalhos que possuem camadas de interação na descrição do funcionamento e serviços oferecidos em diferentes níveis de abstração. Dos trabalhos detalhados, nove (9) possuem referencial discorrendo sobre as camadas e como estas se comportam perante aspectos de segurança ou métodos criptográficos, gestão de perfis de acesso e até mesmo como se comporta a tecnologia Blockchain para provimento e armazenamento da informação. É interessante perceber que os projetos analisados possuem semelhança com o BIMHE por também descrever a interação entre serviços e tecnologias de maneira segmentada por meio de camadas para a abstração de cada momento das interações ocorridas e para melhor compreenssão do funcionamento e das ações a serem tomadas no compartilhamento dos dados.

No que tange ao comportamento de como salvar os dados em saúde é percebido que existem vantagens e desvantagens no tipo de armazenamento do registro que pode ocorrer dentro da Blockchain (on-chain) ou não (off-chain). Não há uma forma certa ou errada sobre qual abordagem é melhor, pois depende das necessidades específicas do projeto, como percebido no levantamento dos autores dos trabalhos correlatos, nove (9) destes optaram pelo armazenamento off-chain, já oito (8) preferiram o armazenamento on-chain, completando com quatro (4) autores que definiram o armazenamento híbrido como escolha. Isto posto, em se tratando dos aspectos conceituais que cercam a Blockchain, no geral, a abordagem on-chain é mais segura e confiável, pois todos os dados são registrados na Blockchain e, portanto, podem ser verificados por qualquer nó da rede, mas isso pode ser menos eficiente em termos de escalabilidade e custos, em função de cada nó da rede armazenar todos os dados, sendo um possível impeditivo para os projetos apresentados, como foi em (Thilagavathy; Renjith; Lalitha *et al*., 2023; Hewa *et al*., 2020; Hirtan *et al*., 2019).

Tiveram projetos que justificaram a abordagem off-chain, por ser mais escalável, com menos investimentos computacionais e custos gerais, já que os dados são armazenados em sistemas externos e somente referenciados na Blockchain, todavia, isso pode ser menos seguro e confiável, já que os dados não estão necessariamente disponíveis para todos os nós da rede. Além disso, a gestão informacional pode ser um problema a ser trabalhado devido a diversidade de fontes de dados para serem tratadas, como foi apresentado em (Agbo; Mahmoud, 2020; Kotsiuba *et al*., 2018). A abordagem híbrida, como mencionado anteriormente, também foi a

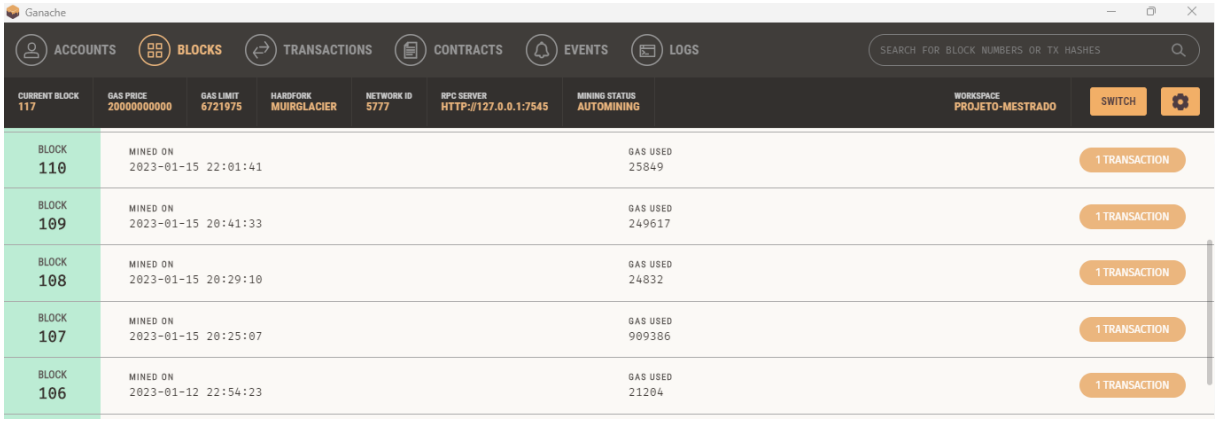
percepção de alguns autores, mas poucos, que combinaram elementos das duas perspectivas de utilização, com transações armazenadas de forma on-chain e dados de pacientes off-chain.

Como supracitado, a escolha da opção mais adequada depende de uma série de fatores, como a natureza da aplicação, os requisitos de segurança e a capacidade de processamento e armazenamento disponíveis. O modelo apresentado por este trabalho colocou como caminho a visão on-chain com a compreensão de que os nós da rede são fundamentais nos processos de validação das transações, mediante também ao conceito de privacidade que é mais possível quando todos os processos envolvidos nas interações entre as partes (médico, paciente e estabelecimento de saúde) estão dentro da Blockchain, não dependendo por minimizar vulnerabilidades também fora do escopo do ambiente Ethereum simulado. Armazenar os dados na Blockchain pode oferecer um alto nível de segurança, devido a imutabilidade e resistência à adulteração, ainda assim, outro ponto de vantagem do modo on-chain é a transparência da Blockchain, onde se permite que qualquer pessoa na rede verifique a validade das transações, tornando a rede mais confiável.

Outra característica importante abordada nos trabalhos correlatos é qual tecnologia Blockchain foi utilizada para implementação e isso pode ter relação com o porquê do armazenamento das transações dentro ou fora da Blockchain. Nos trabalhos correlatos a escolha da tecnologia Blockchain refletiu aspectos que perpassam fatores como suporte a funções de perfil de usuário, custo computacional, compatibilidade com linguagens de programação, sistemas gerenciadores de banco de dados, plataformas em nuvem. Tanto em Blockchain pública, como a Ethereum, quanto em Blockchain privada, como o Hyperledger, ainda que, a principal diferença entre a Blockchain pública e privada esteja relacionada ao acesso e controle do ambiente, não se exclui problemas relacionados a vulnerabilidades. Em uma Blockchain pública, qualquer nó pode participar da rede e validar transações, enquanto em uma Blockchain privada, apenas um grupo específico e autorizado possui acesso.

Como tecnologia Blockchain este modelo optou pelo Ethereum, devido ao suporte para *smarts contracts*, a comunidade ativa, compatibilidade com a linguagem Solidity e maturidade contra vulnerabilidades. A emulação da rede Ethereum por meio da ferramenta Ganache foi escolhida, por ser um ambiente isolado e controlado permitindo assim a simulação local com desenvolvimento e testes, sem precisar se conectar a uma rede Ethereum real, economizando tempo, possíveis gastos com taxas de transação, minimizando custo computacional e adquirindo recursos úteis, como as gestão de contas Ethereum simuladas, visualização da cadeia de blocos local, vide Figura 25 e permitindo também a depuração em um ambiente seguro e controlado.

Figura 25 – Demonstração de uma parte da cadeia de blocos utilizadas nos testes.



Fonte: Elaborada pelo autor.

O modo de como são geridos os perfis de acesso ao dado nos ambientes listados nos trabalhos correlatos também é importante ser comentado, pois subsidia o formato de construção da arquitetura lógica de projeto que acaba influenciando o modelo de compartilhamento de informações do paciente deste projeto. Após a análise dos trabalhos, se percebe maneiras distintas de como se compartilha o dado, ou seja, como se modera o acesso aos dados, onde grande parte dos trabalhos implementa por meio das regras do *smart contract* na Blockchain, ou seja, de acordo com o perfil do usuário este vai ter permissões de acesso ou não ao dado, sendo que as regras são definidas no cadastro do usuário, mas também na primeira interação entre médico e paciente. A escolha da abordagem para moderar o compartilhamento de dados depende das necessidades e requisitos específicos do projeto em questão e a utilização de *smart contracts* é uma forma para garantir que apenas as partes autorizadas tenham acesso aos dados.

O modelo neste trabalho apresentado traz um *smart contract* criado para controlar o acesso ao dado, ou seja, a implementação de regras deste contrato visa garantir que apenas as pessoas autorizadas tenham acesso aos dados do paciente, e a associação da carteira do médico pode facilitar o gerenciamento de acesso. Outrossim, existe e vale ressaltar, a ação do usuário, dono do dado que libera quando necessário as informações para o médico, com a intenção de determinar quem deve ter o direito sobre seu dado, sendo que a partir desta operação ocorre a liberação do par de chaves criptográfico e o aceite a partir do *smart contract*.

A abordagem da criptografia do modelo deste trabalho ao dado do paciente pode ser eficaz para garantir a privacidade, este usa a criptografia RSA para proteger as informações, que apenas as pessoas autorizadas podem acessar, por isso a importância da implantação do processo criptográfico ao se tratar de privacidade aplicada ao paciente. Comparado aos

trabalhos correlatos alguns autores não visualizam a criticidade da implementação criptográfica como em (Agbo; Mahmoud, 2020; Al-Jaroodi; Mohamed; Abukhousa, 2020; Hathaliya *et al*., 2019; Kotsiuba *et al*., 2018; Zhang; Lin, 2018) que implementam Blockchain do tipo privada e isso não garante a privacidade dos dados. Desperta maior interesse o trabalho de Kotsiuba *et al*. (2018), pois este menciona a implantação de um ambiente de Blockchain público e privado a partir de um framework denominado Exonum, no entanto não possui criptografia ao guardar os dados, o armazenamento é off-chain e o controle de privacidade existe a partir do perfil do usuário.

As principais características no modelo apresentado são premissas para entender que este possui o mínimo de técnicas, estrutura e tecnologia para praticar o conceito de privacidade em cenários de saúde 4.0. Naturalmente que problemas nas interações podem existir condicionante aos aspectos intrínsecos das transações que afetam os sistemas computacionais envolvidos. Adiante são orientados os resultados alcançados de forma a questionar a proposta a partir das interações de médico e paciente, visões do modelo e tecnologias.

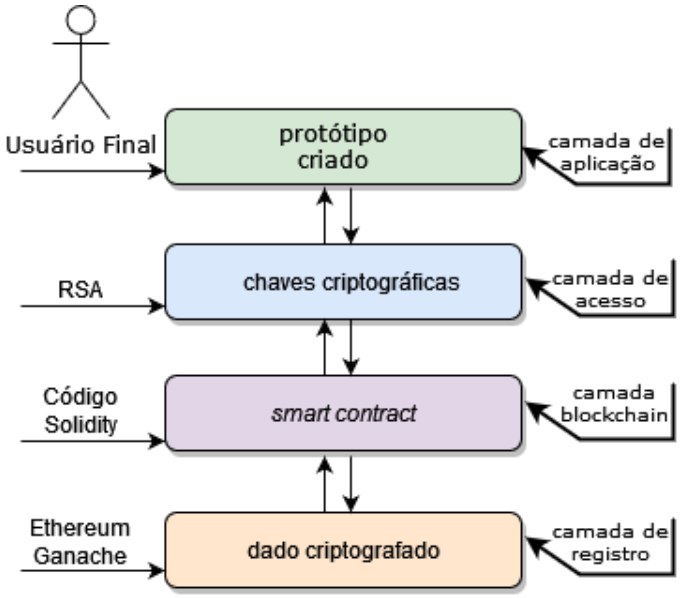
5.5.2 Resultados Alcançados

Conforme proposta deste trabalho, foi apresentado um modelo, com quatro (4) **Camadas** oferecidas, **Mapa Estrutural** integrado entre os usuários e possíveis sistemas e o **Barramento de Dados** para as interações. Tal abordagem, direcionada à privacidade, permite relacionar as etapas de interação, armazenamento e recuperação dos dados. Na perspectiva de segurança, ainda são relacionadas a estrutura utilizada para o processo criptográfico, formato de liberação da informação pelo paciente a específico medico a partir da carteira digital deste profissional junto a Blockhain, e perfis de acesso disponíveis junto ao *smart contract*, para relacionar o vínculo de cada usuário ao acesso de cada informação.

Nas **Camadas** descritas o modelo conseguiu refletir a divisão oferecida dos serviços compreendendo o espaço de cada tecnologia, suas limitações de uso, dependências técnicas e relacionamentos, recursos a oferecer e sequência lógica de acessos, ou seja, as camadas permitiram entender o encapsulamento para que uma informação seja disponível, montando a pilha de tecnologias ou técnicas necessárias em cada momento de interação entre os usuários e o meio que o cerca, estabelecendo uma relação de confiança importante e definindo o conjunto de tecnologias para o acesso ao dado. Na Figura 26 são representadas as camadas conforme a

prática implementada, ou seja refletindo as tecnologias e modo de operação utilizado no ambiente controlado e simulado.

Figura 26 – Exemplo de pilha de acesso ao dado.



Fonte: Elaborada pelo autor.

É possível perceber a idealização das camadas entendendo o funcionamento da prática do modelo, que inicia a sua concepção com um pedido ao protótipo criado podendo ser uma consulta ou inserção de dados, sendo este o primeiro componente tecnológico da pilha, o próprio sistema. Após isto ocorre a troca de chaves no serviço de criptografia para estabelecer a relação de confiança no acesso à informação, requisito mínimo para a interação do protótipo criado com o ambiente Blockchain, sendo este o segundo componente tecnológico da pilha, as chaves geradas. Por sua vez, as transações precisam de regras para existirem e essas são estabelecidas no *smart contract* que estabelece quem tem acesso aos dados, provendo a informação para somente a origem que teve a carteira digital informada, sendo este o terceiro componente tecnológico da pilha, o *smart contract*. Partindo da abstração *top-down*, definida no trabalho, a ação final é entregar o dado que está contido na Blockchain (Ethereum/Ganache), está informação contida é criptografada e precisa de todas as etapas anteriores para o usuário final receber o dado corretamente no sistema, sendo este dado o quarto componente tecnológico da pilha.

O **Mapa Estrutural** definido serviu como arquitetura de negócio indicando os relacionamentos e serviços providos para os diferentes tipos de usuários, a organização foi

representada pelo próprio sistema e a partir disso o protótipo criado definiu as comunicações entre os demais usuários. Foi possível perceber na prática a teoria do modelo, por intermédio dos serviços oferecidos e providos, como o sistema sendo utilizado por usuários (paciente e médico), seja na liberação da carteira ou na consulta ao dado, por exemplo. Continuando, também foi permitido entender a interação do protótipo com o serviço criptográfico e como as informações e transações eram inseridas no Ganache, onde toda a recuperação de informação criptografada era retornada ao sistema finalizando toda o ciclo de acesso ao dado que tem por protagonista neste caso o paciente.

A última visão, denominada **Barramento de Dados**, estabeleceu o relacionamento entre médico e paciente a partir do acesso por estes dois usuários, onde o dono do dado (paciente) pode definir quem iria interagir com seu prontuário. Junto ao protótipo criado foi possível entender este momento de atuação do modelo, em que o médico era liberado junto as suas credenciais de acesso (carteira digital), para a recuperação do dado, caso contrário está informação ficava criptografada para o profissional, por sua vez, o médico poderia até requisitar ações sobre um dado, mas sempre teria vinculada a decisão do paciente. Então, as quatro interações foram possíveis de identificar, desde a solicitação ao registro eletrônico (1ª), conferência das regras de acesso (2ª), lógica de regras para acesso ao dado (3ª) e entrega do dado (4ª).

Vale entender que o propósito não foi criar burocracias em torno de um dado dando ao paciente controle total sobre a informação, mas sim, beneficiar e indicar uma melhor conduta no acessos a dados sensíveis, melhorando a prática da privacidade. Em um contexto geral o modelo deste trabalho, comparando aos existentes que propuseram o conceito de privacidade a partir de um propósito estabelecido entre paciente e médico, conseguiu estruturar um ambiente controlado e simulado para manipulação de informações. A teoria estabelecida fomentou os resultados do modelo e encontrou na prática uma das formas de evidenciar todas as convicções desenvolvidas.

5.5.3 Replicações

Diante da implementação deste projeto é possível colocar que tanto o modelo proposto, assim bem como, as tecnologias escolhidas permitem a replicação em outros ambientes de saúde. Também é capaz a implantação em demais ambientes que desejarem aplicar o conceito de privacidade, acolhendo o usuário como detentor do dado e gestor da forma de

compartilhamento deste, salvo particularidades no modo de gestão do fluxo da informação. Com a aplicação deste modelo, é possível a absorção das **Camadas** por outros ambientes de saúde, pois é uma forma genérica de prover informação independente do sistema de informação a ser utilizado, com ressalvas para os legados que possivelmente poderiam ter restrições na camada de acesso dependendo das tecnologias herdadas.

Já o **Mapa Estrutural** e o **Barramento de Dados** podem ser adaptados a quaisquer ambientes, visto a forma como foram construídos, a partir de usuários e estruturas de acesso praticadas e passíveis de serem implementadas sobre serviços e interações do cotidiano da maioria dos negócios. Isso presume ambientes que possuem interações entre usuários e precisam de serviços e de lógicas de negócio para existir com um mínimo de organização. As regras para proteger o dado pode apresentar restrições devido à especificidade em que o usuário paciente é dono da informação, todavia vale lembrar que sistemas com privilégios, tais como perfis de acesso e módulos para separar serviços também possuem formas particulares de limitar permissões.

A tecnologia Blockchain está a cada momento sendo implantada em diversos ambientes. Complementarmente, a criptografia é também uma ferramenta computacional cada vez mais imprescindível em estruturas que carecem de proteções e garantias de proteção a informação. O conceito de privacidade a informação remete ao uso de tecnologias e práticas operacionais que foram tratadas neste trabalho, sendo evidente que adaptações precisam ser realizadas nas formas de implantação dependendo o negócio, mas também é elucidativo a possibilidade de reproduzir o mesmo modelo em outros tipos de cenários, visto a proposta baseada nos conceitos que envolvem a tecnologia Blockchain.

5.5.4 Discussões

Para suportar a arquitetura implantada, descrita no projeto, foram examinados 3 (três) ambientes antes de chegar a proposta ideal que suportou o modelo e as necessidades das tecnologias escolhidas. Em um primeiro momento a expectativa apontou para uma solução de funcionamento em nuvem, com alocação de recursos educacionais em um ambiente gratuito fornecido pela AWS (Amazon Web Services), na instância Amazon Elastic Compute Cloud (Amazon EC2), com 1 GB de memória primária, 1 CPU para processamento e 20 GB de disco. Foi instalado neste ambiente um sistema operacional Linux (distribuição Debian) e a Máquina Virtual Ethereum para prover o local de armazenamento dos *smarts contracts* e transações, no

entanto, devido a custos de *hardware* adicionais para execução e manutenção esta alocação de recursos na nuvem foi suprimida logo em seguida.

Uma segunda abordagem foi construída com recursos próprios do autor, a partir de um sistema computacional, com características para prover a tecnologia Blockchain, a rede de acesso Ethereum e as interações que esta precisa para o funcionamento das transações e armazenamento, com 4 GB de memória primária, processador com arquitetura de 64 *bits* com dois núcleos (*dual-core*) e 250 GB de disco (HDD). Diante disso foram instalados e configurados o sistema operacional Linux (distribuição Debian) e a Máquina Virtual Ethereum, logo após foi ajustado o ambiente Ethereum com a introdução do Genesis Block (Bloco Zero) e iniciada a rede Blockchain. Com o processo inicial estabelecido foram realizadas ações nas contas para simulação do ambiente controlado e simulado com a constatação de dificuldade inicial com o *hardware* escolhido perante as transações e gravação na Blockchain, as adversidades continuaram mesmo acrescentando mais 4 GB de memória primária, com totalidade de 8 GB.

Os dois ambientes inicialmente experimentados tiveram dificuldades de implantação devido as configurações de *hardware* possíveis alcançadas. No primeiro ambiente, os testes iniciais de execução da Blockchain já apresentavam problemas de desempenho na execução da Máquina Virtual Ethereum e apesar de parametrizações adicionais, este não se apresentou adequado devido à demora excessiva nas ações mínimas já na operação da tecnologia. Com relação ao segundo ambiente apesar de ter tido uma melhora significativa ao executar a Máquina Virtual Ethereum, as transações, gravações das carteiras e até mesmo a troca de chaves criptográficas ficaram prejudicadas, ficando evidenciado a espera elevada no armazenamento dos dados.

Como forma de solucionar a questão de *hardware* o terceiro ambiente foi elaborado a partir de um *notebook* de uso pessoal com memória primária, processamento e armazenamento superiores as características das tentativas anteriores, como apontado na seção de detalhamento do Estudo de Caso. A alteração que mais contribuiu foi o quesito armazenamento, que a partir de uma unidade de estado sólido (SSD) impactou positivamente no funcionamento do Ganache que simulou a gravação e transação dentro da Blockchain, além do processo de troca de chaves e leitura dos registros das ações entre as contas. A utilização da ferramenta Ganache também melhorou o formato de experimento já que simula e controla as varáveis de um modo mais facilitado e com possibilidade no detalhamento de ações e possíveis erros.

6 CONCLUSÕES E TRABALHOS FUTUROS

Esta dissertação expôs um modelo para a criação de um projeto mínimo e operacional que estabelece critérios com vistas da implantação do conceito de privacidade, aliado à tecnologia Blockchain em ambientes de Saúde 4.0. O modelo em questão foi criado com base em projetos similares sobre privacidade em ambientes de saúde digital, com o objetivo de estabelecer critérios claros e operacionais para a implantação desse conceito em Saúde 4.0. Por precisar de requisitos tecnológicos específicos e complexos o ambiente foi simulado e controlado localmente a partir de um sistema computacional.

A partir do BIMHE os dados pessoais sensíveis foram utilizados com o intuito de entender o comportamento do modelo, representando assim as possíveis interações com as informações, forma de armazenamento e preservação dos dados e melhor forma para conduzir o sentido do tráfego de dados, com relação aos aspectos de privacidade. Foi constatado a relevância da tecnologia Blockchain na prática do conceito de privacidade e a consciência crítica sob os efeitos de abordagens e implementação não planejadas que disseminam massa de dados consideráveis sob ambientes de saúde sem o cuidado necessário ao proprietário da informação.

Outro ponto a se comentar foi a padronização do formato de comunicação atrelado a aplicação do modelo. A intenção foi propagar o conjunto de passos para validação de acesso ao dado tornando assim o negócio mais propício a segurança da informação. O entendimento dos fluxos de processamento possibilitou uma melhor disponibilidade de todos os recursos funcionais envolvidos. Fica evidente que as situações de favorecimento no acesso aos dados também devem ser extintas com o formato de apuração de registros padrão da Blockchain que permite rastreamento confiável até a origem de cada solicitação em um ambiente.

A concepção do modelo foi fundamentada a partir de autores que trataram e discutiram conceitos relacionados a Blockchain, criptografia, privacidade, registros eletrônicos de saúde, *smart contracts* e DLTs. Assim, o modelo, as visões construídas sobre as Camadas, Mapa Estrutural e Barramento de Dados, aliado ao ambiente simulado e controlado que foi implementado são as principais contribuições deste trabalho. Estas e demais colaborações são mais bem especificadas nos parágrafos seguintes.

O primeiro objetivo requereu a busca por trabalhos em mecanismos de buscas acadêmicos que desenvolveram modelos, a partir de tecnologias Blockchain (privadas ou públicas), aplicadas a cenários de saúde que mostravam como ocorria o tratamento do dado

privado do paciente. Sobre o modelo, a busca foi refinada a partir de projetos similares que implantavam métodos com o estudo prático de alguma maneira caracterizando a preocupação com os perfis de acesso ao dado. Por intermédio da Revisão Sistemática de Literatura, se verificou o estado da arte sobre Blockchain na Saúde 4.0, identificando as principais modelagens atualmente utilizadas e as ferramentas tecnológicas aplicadas aos cenários descritos.

As modelagens levantadas em conjunto com o referencial teórico sobre criptografia e privacidade estruturaram e forneceram conceitos elementares para a elaboração de um modelo conceitual, segundo objetivo específico, conseguindo para o paciente a gestão de suas informações. Com o modelo conceitual proposto foi possível identificar: as Camadas estruturantes do modelo, que delimitaram a atuação tecnológica; o Mapa Estrutural que elucidou a forma de como usar e como se relacionam os serviços e; o Barramentos de Dados com caminhos e conexões para a liberação do dado. Também foi apresentado uma sequência lógica no modelo para o compartilhamento de dados e definidas as terminologias utilizadas para o entendimento deste modelo.

Com a lógica de atender o terceiro objetivo específico foi desenvolvido um protótipo construído a partir da tecnologia Ethereum (Ganache), com dados privados a partir da criptografia assimétrica (RSA). Esta condução prática cobriu a execução das etapas e visões do modelo, como a liberação da informação atrelado a carteira digital do requerente, as interações entre os usuários, o provimento dos serviços a partir das tecnologias implantadas, a criptografia dos dados, a entrega da informação ao solicitante e a sequência das interações do ciclo correto para a liberação de um dado. O protótipo com a interface desenvolvida foi importante para atender os requisitos da atuação do modelo teórico que buscava a privacidade ao dado, sendo demonstrado durante a execução em cada momento de atuação dos usuários.

Já o quarto objetivo específico surge da obrigatoriedade em avaliar o modelo construído no ambiente simulado e controlado pelo autor, entendendo as variáveis, observando o comportamento do protótipo e registrando as ações resultantes dos usuários. O ambiente simulado e controlado foi essencial para mostrar os resultados de controle do dado pelo usuário não se preocupando com influências externas para a avaliação final do conceito de privacidade e também foi crítico para compreender a interação entre os usuários e estabelecer o funcionamento correto do protótipo que possuía uma finalidade limitada as ações do modelo. Foram realizadas comparações de características com os outros trabalhos levantados onde se

percebeu o impacto positivo do formato de construção da estrutura deste modelo produzindo avaliações positivas sobre os resultados.

O resultado obtido neste documento indicou então uma proposta inicial para implementar o conceito de privacidade em ambientes com a temática Saúde 4.0. Em se tratando de manipulação da informação existe a preocupação em compreender as variáveis e possíveis problemas que surgem das interações obrigatórias entre os usuários, mas sempre com a preocupação sobre o dado compartilhado. Na visão geral do modelo os dados pessoais sensíveis são entregues mediante validação. Foram realizados experimentos com o propósito de simular interações reais, induzindo para situações de acesso considerados autênticos por meio das validações de chave e perfil do usuário (carteira digital), sem o propósito de esgotar todas as possibilidades de conjunturas ao solicitar os dados pessoais sensíveis, visto as inúmeras variações de interações tecnológicas que poderão existir na busca por tais informações.

É válido afirmar que o objetivo geral do modelo foi alcançado e concluir também que os aspectos levantados neste trabalho de pesquisa podem ser adaptados com a realidade das aplicações que buscam modos de tratar dados pessoais sensíveis. Julga-se ainda que a tecnologia Blockchain é aliada importante para a busca de privacidade das informações, mas precisa de entendimento de suas propriedades com boas práticas nas configurações de ambiente, com métodos e técnicas, como a criptografia, no intuito de dominar a melhor forma do uso da tecnologia e expor de forma correta o dado.

6.1 TRABALHOS FUTUROS

O modelo proposto (BIMHE) neste trabalho, é constituído de 3 visões que sugerem o comportamento dos serviços, tecnologias e usuários. Este consegue indicar um caminho na tentativa de sistemas informatizados obterem uma melhor conduta, respeitando o usuário proprietário do dado. Contudo, ainda é preciso entender alguns pontos de melhorias necessárias para melhor escalonar a informação a ser armazenada no ambiente Blockchain diante de alguns aspectos, a saber.

Como sugestão de trabalhos futuros é desafiador pensar o modelo com a autenticação de dois fatores, adicionando assim mais uma validação para o usuário requisitante obter acesso a informação e melhorando com isso a proteção sobre o dado. Neste sentido as três visões criadas, sofreriam alterações, pois seria estabelecido um novo desenho da integração entre os serviços oferecidos, assim bem como mudanças quanto a sequência das interações que

precisariam ocorrer devido a este acréscimo de validação. Em suma, esta característica é bem vinda para complementar o modelo e adicionar mais uma técnica que acionaria mais um estado de verificação sobre o compartilhamento de informação.

Outro ponto a ser entendido como melhora não explorado no trabalho é a escalabilidade que não foi propósito do modelo diante dos objetivos estabelecidos sobre privacidade, mas necessário se existirem cenários com montante de dados elevado. A possibilidade de trabalhar este tipo de situação também condicionaria mudanças no comportamento e escrita do modelo que necessitaria de uma interpretação diferente da atual e testes das tecnologias para abrigar uma massa de dados maior que a utilizada em se tratando de origens diversas de alimentação dos dados a serem inseridos no ambiente Blockchain. Os dados precisariam não só de tratamento da informação, mas também serem analisados para uma possível área de transição antes de serem inseridos no ambiente Blockchain obrigando uma abordagem mais precisa de como armazenar estes dados temporariamente e com segurança.

Em se tratando do protótipo utilizado no estudo de caso é interessante perceber que melhorias poderiam ser implementadas em todos os sentidos, como a interface gráfica melhorando a usabilidade, funções para carregamento de arquivos, relatórios sobre problemas entre outras funcionalidades possíveis em um sistema de informação, mas este trabalho não possuiu o intuito em trabalhar estes aspectos devido à especificidade do tema que buscava provar conceitos sem envolvimento de outras características operacionais. O estudo de caso poderia sofrer também, melhorias abrigando novas tecnologias como Blockchains do tipo privada conduzindo a outros testes e outras conexões entre ferramentas de diferentes desenvolvedores, ou até mesmo, sendo aplicada em um cenário real o que poderia trazer experiências significativas devido a diversos pontos de vista a serem contemplados conformes o biótipo organizacional abordado e as situações inesperadas, no qual sempre acontecem.

Outro aspecto importante a ser explorado são as 3 visões que foram elementares para o modelo, pois estas podem avançar com relação a tratamento de erros nas camadas, adição de serviços oferecido por cada camada e até a inclusão de conceitos de modelos de referência consagrados, com intenção de tornar este modelo desenvolvido mais genérico e com possibilidade de reutilização mais apurada e precisa. A proposição do modelo foi realizada com apoio no ambiente simulado e controlado e isto pode ter invariavelmente de uma forma involuntária e automática ter inserido aspectos na construção do modelo que não reflete outros ambientes e temáticas que precisam aplicar a tecnologia Blockchain. Posto isto, vale representar

e contemplar outras demandas de aplicação que também possui o intuito em minimizar aspectos hostis no compartilhamento de informações tendo como base tecnológica o Blockchain.

REFERÊNCIAS

AGBO, C. C.; MAHMOUD, Q. H. Design and Implementation of a Blockchain-Based E-Health Consent Management Framework. In: 2020. **IEEE Transactions on Systems, Man, and Cybernetics**: Systems. [S. l.]: Institute of Electrical and Electronics Engineers Inc., p. 812–817, 2020. Disponível em: https://doi.org/10.1109/smc42975.2020.9283203. Acesso em: 17 fev., 2021.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANSS). **Nota Técnica n.º 3/2019/gepin/dirad-dides/dides**. Nota Técnica 3 (14815937). Processo n.º 33910.029786/2019-51, Rio de Janeiro, dez., 2019. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/nota-te%cc%81cnica-sobre-lgpd.pdf. Acesso em: 6 fev., 2021.

AHMAD, K. A. B.; KHUJAMATOV, H.; AKHMEDOV, N.; BAJURI, M. Y.; AHMAD, M. N.; AHMADIAN, A. Emerging trends and evolutions for smart city healthcare systems. **Sustainable Cities And Society**, [S.L.], v. 80, p. 103695 -103711, mai., 2022. Elsevier BV. Disponível em: https://dx.doi.org/10.1016/j.scs.2022.103695. Acesso em: 22 dez., 2022.

AKBAR, I. M.; BHAWIYUGA, A.; SIREGAR, R. An Ethereum Blockchain Based Electronic Health Record System for Inter-Hospital Secure Data Sharing. **6Th International Conference On Sustainable Information Engineering And Technology 2021**, [S.L.], p. 226-230, 13 set., 2021. ACM. Disponível em: https://dx.doi.org/10.1145/3479645.3479699. Acesso em: 20 dez., 2021.

AL-JAROODI, J.; MOHAMED, N.; ABUKHOUSA, E. Health 4.0: On the Way to Realizing the Healthcare of the Future. **IEEE Access**, [*s. l.*], v. 8, p. 211189–211210, 2020. Disponível em: https://doi.org/10.1109/access.2020.3038858. Acesso em: 4 fev., 2021.

AL-ZAHRANI, F. A. Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service. **IEEE Access**, 8, 115966–115981, 2020. Disponível em: https://doi.org/10.1109/access.2020.3002823. Acesso em: 22 set., 2021.

ALBANESE, G.; CALBIMONTE, J.; SCHUMACHER, M.; CALVARESI, D. Dynamic consent management for clinical trials via private blockchain technology. **Journal of Ambient Intelligence and Humanized Computing**, [*s. l.*], v. 11, n. 11, p. 4909–4926, 2020. Disponível em: https://doi.org/10.1007/s12652-020-01761-1. Acesso em: 12 fev., 2021.

ALLEN, D.; BERG, C.; MARKEY-TOWLER, B.; NOVAK, M.; POTTS, J. Blockchain and the evolution of institutional technologies: implications for innovation policy. **Research Policy**. v. 49, p. 103865, february 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0048733319301842. Acesso em: 5 abr., 2021.

AMOFA, S.; SIFAH, E.; AGYEKUM, K. O.-B. O.; ABLA, S.; XIA, Q.; GEE, J. C.; GAO, J. A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data. **2018 Ieee 20Th International Conference On E-Health Networking, Applications And**

Services (Healthcom), [S.L.], p. 1-6, set. 2018. Disponível em: http://dx.doi.org/10.1109/healthcom.2018.8531160. Acesso em: 11 fev., 2021.

ANTONOPOULOS, A. M. **Mastering bitcoin**: unlocking digital cryptocurrencies. [S.l.]: O'Reilly Media, Inc., 2014.

ANTONOPOULOS, A. M.; WOOD, G. **Mastering Ethereum**. 1. ed. O'Reilly, 2018.

ARMKNECHT, F.; KARAME, G. O.; MANDAL, A.; YOUSSEF, F.; ZENNER, E. Ripple: overview and outlook**. Trust And Trustworthy Computing**, [S.L.], p. 163-180, 2015. Springer International Publishing.

ATTARAN, M.; GUNASEKARAN, A. **Applications of Blockchain Technology in Business**: challenges and opportunities. Cham: Springer, 2019. 112 p. Disponível em: https://doi.org/10.1007/978-3-030-27798-7. Acesso em: 19 abr., 2020.

AZARIA, A.; EKBLAW, A.; VIEIRA, T.; LIPPMAN, A. MedRec: Using blockchain for medical data access and permission management. **Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016**, p. 25–30, 2016.

BALIGA, A.; I. S.; KAMAT, P.; CHATTERJEE, S. Performance Evaluation of the Quorum Blockchain Platform. 2018. **ArXiv**. Disponível em: https://arxiv.org/pdf/1809.03421.pdf. Acesso em: 25 abr., 2020.

BAMBARA, J. J.; ALLEN, P. R. **Blockchain**: A Practical Guide to Developing Business, Law, and Technology Solutions. New York, N.Y.: McGraw-Hill Education, 2018.

BAN, T. Q.; ANH, B. N.; SON, N. T.; DINH, T. V. Survey of Hyperledger Blockchain Frameworks. **Proceedings Of The 2019 8th International Conference On Software And Computer Applications - Icsca '19**, [s.l.], p. 472-480, 2019. Disponível em: https://dl.acm.org/doi/abs/10.1145/3316615.3316671. Acesso em: 20 jun., 2020.

BARROWS, R. C.; CLAYTON, P. D. Privacy, Confidentiality, and Electronic Medical Records. **Journal Of The American Medical Informatics Association**, [S.L.], v. 3, n. 2, p. 139-148, 1 mar., 1996. Disponível em: http://dx.doi.org/10.1136/jamia.1996.96236282. Acesso em: 12 jan., 2021.

BAUSE, M.; ESFAHANI, B. K.; FORBES, H.; SCHAEFER, D. Design for Health 4.0: exploration of a new area, **Proceedings of the International Conference on Engineering Design, ICED, 2019**-August, p. 887–896, 2019.

BERG, A.; BERG, C.; NOVAK, M. Blockchains and constitutional catallaxy. **Constitutional Political Economy,** v. 31, n. 2, p. 188-204, 2020. Disponível em: https://link.springer.com/article/10.1007%2fs10602-020-09303-9. Acesso em: 1 jul., 2021.

BERNABE, J. B.; CANOVAS, J. L.; HERNANDEZ-RAMOS, J. L.; MORENO, R. T.; SKARMETA, A. Privacy-Preserving Solutions for Blockchain: review and challenges. **Ieee Access**, [S.L.], v. 7, p. 164908-164940, 2019. Disponível em: http://dx.doi.org/10.1109/access.2019.2950872. Acesso em: 23 fev., 2021.

BHUIYAN, M. Z. A.; ZAMAN, A.; WANG, T.; WANG, G.; TAO, H.; HASSAN, M. M. Blockchain and Big Data to Transform the Healthcare. **Proceedings Of The International Conference On Data Processing And Applications**, [S.L.], p. 62-68, 12 maio 2018. ACM. Disponível em: http://dx.doi.org/10.1145/3224207.3224220. Acesso em: 20 fev., 2021.

BIRMAN, K. P. **Building Secure and Reliable Network Applications**. New York: Manning Publications, 1996. 591 p.

BLOCK.ONE. **EOSIO overview,** v. 2.1, 2020. Disponível em: https://developers.eos.io/manuals/eos/v2.1/index. Acesso em: 3 jun., 2020.

BORKO, H. **Information science**: what is it? American Documentation, v. 19, n. 1, p. 3-5, jan., 1968.

BROWN, R. G. **The Corda Platform**: an introduction. 2018. Disponível em: https://www.corda.net/content/corda-platform-whitepaper.pdf. Acesso em: 1 jun., 2020.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Lei n.º13.709/2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 mai., 2021.

BRASIL. Imprensa Nacional. **Decreto n.º 10.332, de 28 de abril de 2020.** Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, DF, 28 abr., 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm. Acesso em: 30 nov., 2021.

BUCHINGER, D.; CAVALCANTI, G. A. S.; HOUNSELL, M. S. Mecanismos de busca acadêmica: uma análise quantitativa. **Revista Brasileira de Computação Aplicada**, [*s. l.*], v. 6, n. 1, p. 108–120, 2014. Disponível em: https://doi.org/10.5335/rbca.2014.3452. Acesso em: 25 fev., 2021.

BUTERIN, V. **A next-generation smart contract and decentralized application platform**. White paper, 2014. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 4 jul., 2020.

CAMPBELL-VERDUYN, M. **Bitcoin and Beyond**: cryptocurrencies, blockchains and global governance. Routledge, 2018. 212 p. (RIPE Series in Global Political Economy).

CERT.BR. **Incidentes notificados ao cert.br**. Incidentes notificados voluntariamente ao CERT.br por CSIRTs, administradores de redes e usuários finais [atualização mensal]. 2019. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 11 set, 2020.

CHAN, K. Y.; ABDULLAH, J.; KHAN, A. S. A Framework for Traceable and Transparent Supply Chain Management for Agri-food Sector in Malaysia using Blockchain Technology. **International Journal of Advanced Computer Science and Applications** (IJACSA), v. 10,

n. 11, p. 149-156, 2019. Disponível em: https://pdfs.semanticscholar.org/a82a/a77d59c0f313508abdd77468a88e4c6ef6cf.pdf. Acesso em: 29 jun., 2020.

CHANG, Y.; WONG, S. F.; LIBAQUE-SAENZ, C. F.; LEE, H. The role of privacy policy on consumers' perceived privacy. **Government Information Quarterly**, [S.L.], v. 35, n. 3, p. 445-459, set., 2018. Disponível em: http://dx.doi.org/10.1016/j.giq.2018.04.002. Acesso em: 22 mar., 2021.

CHANCHAICHUJIT, J.; TAN, A.; MENG, F.; EAIMKHONG, S. **Healthcare 4.0**. Next Generation Processes with the Latest Technologies. 1 ed., 202 p., 2019. Disponível em: https://link.springer.com/book/10.1007/978-981-13-8114-0. Acesso em: 12 jul., 2020.

CHANDWANI, R.; KUMAR, N. Stitching infrastructures to facilitate Telemedicine for low-resource environments, Conference on Human Factors in Computing Systems - **Proceedings**, p. 1–12, abr., 2018. Disponível em: 10.1145/3173574.3173958, 2018. Acesso em: 12 jul., 2021.

CHASE, B.; MACBROUGH, E. Analysis of the XRP Ledger Consensus Protocol. **ArXiv**. 2018. Disponível em: https://arxiv.org/pdf/1802.07242.pdf. Acesso em: 12 jul., 2020.

CHAUM, D. Untraceable electronic main, return addresses, and digital pseudonyms, in **Communications of the ACM**, v. 24, n. 2, p. 84-88, fev., 1981.

CHEN, C.; LOH, E.-W.; KUO, K. N.; TAM, K.-W. The Times they Are a-Changin' – Healthcare 4.0 Is Coming! **Journal Of Medical Systems**, [S.L.], v. 44, n. 2, p. 40-44, 23 dez. 2019. Disponível em: http://dx.doi.org/10.1007/s10916-019-1513-0. Acesso em: 16 jul., 2021.

CHEN, X.; ZHOU, X.; LI, H.; LI, J.; JIANG, H. The value of WeChat application in chronic diseases management in China. **Comput Methods Programs Biomed,** nov., 2020. Disponível em: https://doi.org/10.1016/j.cmpb.2020.105710. Acesso em: 12 jul., 2021.

CHERVINSKI, J.; KREUTZ, D. Introdução às tecnologias dos blockchains e das criptomoedas. **Revista Brasileira de Computação Aplicada**, [s.l.], v. 11, n. 3, p. 12-27, 25 set., 2019. Disponível em: http://seer.upf.br/index.php/rbca/article/view/9394. Acesso em: 14 abr., 2020.

CHOWDHURY, M. J. M.; FERDOUS, S.; BISWAS, K.; CHOWDHURY, N.; KAYES, A. S. M.; ALAZAB, M.; WATTERS, P. A Comparative Analysis of Distributed Ledger Technology Platforms. in **IEEE Access**, v. 7, p. 167930-167943, 2019. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8902067. Acesso em: 11 jul., 2020.

CHOWDHURY, N. **Inside Blockchain, Bitcoin and Cryptocurrencies**. Auerbach, 2019.

COHEN, B. **The Future of Money.** Princeton University Press, 2004.

COINMARKETCAP. **Top 100 Cryptocurrencies by Market Capitalization.** 2023. Disponível em: https://coinmarketcap.com. Acesso em: 9 jan., 2023.

CROSBY, M.; NACHIAPPAN; PATTANAYAK, P.; VERMA, S.; KALYANARAMAN, V. BlockChain technology: beyond bitcoin, **Applied Innovation Review**, v. 2, Pantas and Ting Sutardja Center for Entrepeneurship & Technology, Berkeley Engineering, UC Berkeley, 2016. Disponível em: https://j2-capital.com/wp-content/uploads/2017/11/air-2016-blockchain.pdf. Acesso em: 6 abr., 2020.

COULOURIS, G.; DOLLIMORE, J.; KINDBERG, T; BLAIR, G. **Distributed systems**: concepts and design. 5 ed. Boston: Addison-Wesley, 2012.

COUTINHO, E. F.; MOREIRA NETO, Maurício; ABREU, A. W.; MOREIRA, L. O.; BEZERRA, C. I. M.; PAILLARD, G.; SOUZA, J. N. Modeling blockchain e-health systems. **Proceedings Of The 10Th Euro-American Conference On Telematics And Information Systems**, [S.L.], p. 1-8, 25, nov., 2020. Disponível em: http://dx.doi.org/10.1145/3401895.3401917. Acesso em: 10 jul., 2021.

ĆWIKLICKI, M., J. KLICH; CHEN, J. The adaptiveness of the healthcare system to the fourth industrial revolution: A preliminary analysis, **Futures**, v. 122, oct., 2020.

DELGADO-MOHATAR, O.; FIERREZ, J.; TOLOSANA, R.; VERA-RODRIGUEZ, R. Blockchain meets biometrics: concepts, application to template protection, and trends. Computer Science. Computer Vision and Pattern Recognition. **ArXiv**. School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain, 2020. Disponível em: https://arxiv.org/abs/2003.09262. Acesso em: 5 jan., 2021.

DHILLON, V.; METCALF, D.; HOOPER, M.: **Blockchain Enabled Applications**: understand the blockchain ecosystem and how to make it work for you. New York: Apress, 2017.

DONEDA, D.; MENDES, L. S. Data Protection in Brazil: new developments and current challenges. **Reloading Data Protection**, [S.L.], p. 3-20, out., 2013. Disponível em: http://dx.doi.org/10.1007/978-94-007-7540-4_1. Acesso em: 18 jul., 2020.

DOOLEY, J. F. **History of Cryptography and Cryptanalysis**: Codes, Ciphers, and Their Algorithms. History of Computing. Springer Cham: Springer International Publishing AG, part of Springer Nature 2018, 2018.

DROLET, B. C.; MARWAHA, J. S.; HYATT, B.; BLAZAR, P. E.; LIFCHEZ, S. D. Electronic Communication of Protected Health Information: privacy, security, and hipaa compliance. **The Journal Of Hand Surgery**, [S.L.], v. 42, n. 6, p. 411-416, jun., 2017. Disponível em: http://dx.doi.org/10.1016/j.jhsa.2017.03.023. Acesso em: 12 nov., 2021.

DUBOVITSKAYA, A.; XU, Z.; RYU, S.; SCHUMACHER, M.; WANG, F. How Blockchain Could Empower eHealth: an application for radiation oncology**. Data Management And Analytics For Medicine And Healthcare**, [S.L.], p. 3-6, 2017. Disponível em: http://dx.doi.org/10.1007/978-3-319-67186-4_1. Acesso em: 19 jul., 2020.

EASLEY, D.; O'HARA, M.; BASU, S. From mining to markets: the evolution of bitcoin transaction fees. **Journal Of Financial Economics**, [S.L.], v. 134, n. 1, p. 91-109, out., 2019. Disponível em: http://dx.doi.org/10.1016/j.jfineco.2019.03.004. Acesso em: 14 jul., 2020.

EFANOV, D.; ROSCHIN, P. The All-Pervasiveness of the Blockchain Technology. **Procedia Computer Science**, [S.L.], v. 123, p. 116-121, 2018. Disponível em: http://dx.doi.org/10.1016/j.procs.2018.01.019. Acesso em: 18 jul., 2021.

EPIPHANIOU, G.; DALY, H.; AL-KHATEEB, H. **Blockchain and healthcare**. [*S. l.*]: Springer, 2019. Disponível em: https://doi.org/10.1007/978-3-030-11289-9_1. Acesso em: 12 jul., 2020.

ESPEL, T.; KATZ, L.; ROBIN, G. Proposal for Protocol on a Quorum Blockchainwith Zero Knowledge. LeLab Banque de France, Paris, 2017. **IACR**. Disponível em: https://eprint.iacr.org/2017/1093.pdf. Acesso em: 29 abr., 2020.

FARIA, P. M. **Revisão Sistemática da Literatura:** contributo para um novo paradigma investigativo. Metodologia e Procedimentos na área das Ciências da Educação. Aplicação prática aos temas desenvolvimento profissional docente e inovação educativa com tecnologias digitais. 2. ed. Santo Tirso: Whitebooks, 2019.

GALVÃO, M. C. B.; RICARTE, I. L. M. Systematic literature review: concept, production and publication. **Logeion: Filosofia da Informação**, [*s. l.*], v. 6, n. 1, p. 57–73, 2019.

GIARDELLI, G. **Você é o que você compartilha**: e-agora: como aproveitar as oportunidades de vida e trabalho na sociedade em rede. São Paulo: Editora Gente, 2012.

GIBBS, T.; YORDCHIM, S. Thai perception on Litecoin value. **World Academy of Science, Engineering and Technology**: International Journal of Economics and Management Engineering, 8, 2634-2636, 2014. Disponível em: https://waset.org/publications/9999129/thai-perception-on-litecoin-value. Acesso em: 18 jul., de 2020.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6a. ed. [s.l.] São Paulo: Atlas, 2017.

GOVERNMENT OFFICE FOR SCIENCE. Distributed Ledger Technology: beyond block chain. London: **Government Office for Science**. v. 3, 2016. UK Government Chief Scientific Adviser. WordLink. Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Acesso em: 10 abr., 2020.

GRIGGS, K.; OSSIPOVA, O.; KOHLIOS, C.; BACCARINI1, A.; HOWSON, E. · HAYAJNEH, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. **Journal Of Medical Systems**. Mobile & wireless health. Med Syst (2018), [s.l.], v. 42, n. 7, p. 129-136, 6 jun., 2018. Springer Science and Business Media LLC. Disponível em: https://link.springer.com/article/10.1007%2fs10916-018-0982-x. Acesso em: 10 abr., 2020.

GRIGORIADIS, N. C.; BAKIRTZIS, C.; POLITIS, K.; DANAS, K.; THUEMMLER, C. Health 4.0: The case of multiple sclerosis, **2016 IEEE 18th International Conference on e-Health Networking**, Applications and Services, Healthcom, p. 14–18, 2016. Disponível em: 10.1109/healthcom.2016.7749437. Acesso em: 18 jul., 2020.

GRISOTO, A. P.; SANT'ANA, R. C. G.; SANTAREM SEGUNDO, J. E. A questão da privacidade no contexto da Ciência da Informação: uma análise das teses e dissertações do programa de pós graduação em ciência da informação da unesp campus de marília. **Revista Ibero-Americana de Ciência da Informação**, [S.L.], v. 8, n. 2, p. 165-181, 2015. Biblioteca Central da UNB. Disponível em: http://dx.doi.org/10.26512/rici.v8.n2.2015.2066. Acesso em: 12 ago, 2021.

HASAN, H. R.; SALAH, K. Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts. **Ieee Access**, [s.l.], v. 6, p. 65439-65448, 2018. Disponível em: http://dx.doi.org/10.1109/access.2018.2876971. Acesso em: 12 abr., 2020.

HASAN, H. R.; SALAH, K.; JAYARAMAN, R.; OMAR, M.; YAQOOB, I.; PESIC, S.; TAYLOR, T.; BOSCOVIC, A. D.; A Blockchain-Based Approach for the Creation of Digital Twins. **IEEE Access**, v. 8, p. 34113-34126, 2020. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9001017. Acesso em: 2 de jul., 2021.

HASSANI, H.; HUANG, X.; SILVA, E. S. **Fusing Big Data, Blockchain and Cryptocurrency.** Their Individual and Combined Importance in the Digital Economy. Palgrave Pivot, 2019. Disponível em: http://dx.doi.org/10.1007/978-3-030-31391-3. Acesso em: 1 jan., 2021.

HATHALIYA, J. J.; TANWAR, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. **Computer Communications**, [S.L.], v. 153, p. 311-335, mar., 2020. Disponível em: http://dx.doi.org/10.1016/j.comcom.2020.02.018. Acesso em: 12 jan., 2021.

HATHALIYA, J.; SHARMA, P.; TANWAR, S.; GUPTA, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. **2019 Ieee 9Th International Conference On Advanced Computing (Iacc)**, [S.L.], p. 87-91, dez., 2019. Disponível em: http://dx.doi.org/10.1109/iacc48062.2019.8971593. Acesso em: 12 jun., 2020.

HEARN, M.; BROWN, R. G. **Corda**: a distributed ledger. 2019. Disponível em: https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf. Acesso em: 1 jun., 2020.

HEWA, T.; BRAEKEN, A.; YLIANTTILA, M.; LIYANAGE, M. Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. **Globecom 2020 - 2020 Ieee Global Communications Conference**, [S.L.], p. 1-6, dez.. 2020. Disponível em: http://dx.doi.org/10.1109/globecom42002.2020.9348125. Acesso em: 17 jul., 2021.

HIMSS HEALTH INFORMATION STANDARDS WORK GROUP. **Evaluating HIT standards**: Key principlies to support healthcare IT interoperability in the United States. HIMSS Interoperability & Standards, [s. l.], n. July, p. 23, 2013. Disponível em:

https://www.himss.org/sites/hde/files/d7/filedownloads/2013-09-23-evaluatinghitstandards-final.pdf. Acesso em: 21 ago., 2021.

HOLBROOK, J. **Architecting Enterprise Blockchain Solutions**. Indianápolis: Sybex, 2020. 400 p.

HYPERLEDGER 2019. **Hyperledger Indy**. 2019. Disponível em: https://www.hyperledger.org/use/hyperledger-indy. Acesso em: 29 de jun., 2020.

HYPERLEDGER BESU. **Announcing Hyperledger Besu**. 2019. Disponível em: https://www.hyperledger.org/blog/2019/08/29/announcing-hyperledger-besu. Acesso em: 1 jul., 2020.

HONGWEI, L.; XINHUI, W.; SANYANG, L. Feasible direction algorithm for solving the SDP relaxations of quadratic {-1, 1} programming problems. **Optimization Methods and Software**, v. 19, n. 2, p. 125–136, 2004.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 1. ed. Brasport, 2018.

HIRTAN, L.; KRAWIEC, P.; DOBRE, C.; BATALLA, J. M. Blockchain-based approach for e-health data access management with privacy protection. *In*: , 2019. **IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD**. [*S. l.*]: Institute of Electrical and Electronics Engineers Inc., 2019. Disponível em: https://doi.org/10.1109/camad.2019.8858469. Acesso em: 12 jul., 2021.

HUANG, A.; KANDULA, A.; WANG, X. A Differential-Privacy-Based Blockchain Architecture to Secure and Store Electronic Health Records. **2021 The 3Rd International Conference On Blockchain Technology**, [S.L.], p. 189-194, 26 mar., 2021. Disponível em: http://dx.doi.org/10.1145/3460537.3460555. Acesso em: 14 nov., 2021.

HUANG, Y.; WANG, H.; WU, L.; TYSON, G.; LUO, X.; ZHANG, R.; LIU, X.; HUANG, G.; JIANG, X. Characterizing EOSIO Blockchain. **Computer Science**: Cryptography and Security, [S.L.], p. 1-14, 2020. ArXiv. Disponível em: http://dx.doi.org/10.48550/arxiv.2002.05369. Acesso em: 23 jan., 2021.

ISHANI, A.; CHRISTOPHER, J.; PALMER, D.; OTTERNESS, S.; CLOTHIER, B.; NUGENT, S.; NELSON, D.; ROSENBERG, M. E.; ATWOOD, M.; BANGERTER, A. Telehealth by an Interprofessional Team in Patients With CKD: a randomized controlled trial. **American Journal Of Kidney Diseases,** [S.L.], v. 68, n. 1, p. 41-49, jul. 2016. Disponível em: http://dx.doi.org/10.1053/j.ajkd.2016.01.018. Acesso em: 21 jul., 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. **ISO/TR 20514:2005**, Health Informatics—Electronic Health Record—Definition, Scope and Context, 2005.

ISTEPANIAN, R. S. H.; WOODWARD, B. **Introduction to m-Health**, p. 1–22, 2017.

JALALI, M. S.; LANDMAN, A.; GORDON, W. J. Telemedicine, privacy, and information security in the age of COVID-19. **Journal of the American Medical Informatics Association**, [s. l.], v. 28, n. 3, p. 671–672, 2020. Disponível em: https://doi.org/10.1093/jamia/ocaa310. Acesso em: 28 jan., 2021.

JAIN, R.; GUPTA, M.; NAYYAR, A.; SHARMA, N. Adoption of Fog Computing in Healthcare 4.0. **Fog Computing For Healthcare 4.0 Environments**, [S.L.], p. 3-36, 3 ago., 2020. Disponível em: http://dx.doi.org/10.1007/978-3-030-46197-3_1. Acesso em: 18 jul., 2021.

KAUARK, F. S.; MANHÃES, F. C.; MEDEIROS, C. H. **Metodologia da Pesquisa: um guia prático.** 1a. ed. Itabuna: Via Litterarum, 2010.

KESSLER, A. **The End of Medicine**: how silicon valley (and naked mice) will reboot your doctor. Collins: Nova York, 2007.

KHAN, A. A.; LAGHARI, A. A.; SHAIKH, A. A.; BOUROUIS, S.; MAMLOUK, A. M.; ALSHAZLY, H. Educational Blockchain: a secure degree attestation and verification traceability architecture for higher education commission. **Applied Sciences**, [S.L.], v. 11, n. 22, p. 755-763, nov., 2021. Disponível em: http://dx.doi.org/10.3390/app112210917. Acesso em: 12 fev., 2022.

KIMBLE, C. Electronic Health Records: Cure-all or Chronic Condition?. **Global Business and Organizational Excellence**, Wiley, v. 34, v. 4, p. 63-74, 2014.

KIRTAVA, Z.; SHULAIA, T.; KILADZE, N.; KORSANTIA, N.; GOGITIDZE, T.; JORJOLIANI, D. E-Health/mHealth services for dermatology outpatients screening for skin cancer and follow-up, **2016 IEEE 18th International Conference on e-Health Networking, Applications and Services**, Healthcom, 2016.

KITCHENHAM, B. **Procedures for Performing Systematic Reviews**. [*s. l.*], v. 33, p. 1–26, 2004.

KORDESTANI, H.; BARKAOUI, K.; ZAHRAN, W. Hapichain: A blockchain-based framework for patientcentric telemedicine, in **2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH)**, p. 1–6, 2020.

KOREN, I.; KRISHNA, C. M. **Fault-Tolerant Systems**. 2. ed. [s.l.] Morgan Kaufmann Publishers, 2020.

KOTSIUBA, I.; VELVKZHANIN, A.; YANOVICH, Y.; BANDUROVA, I. S.; DYACHENKO, Y.; ZHYGULIN, V. Decentralized e-Health Architecture for Boosting Healthcare Analytics. **2018 Second World Conference On Smart Trends In Systems, Security And Sustainability (Worlds4)**, [S.L.], p. 113-118, out., 2018. IEEE. Disponível em: http://dx.doi.org/10.1109/worlds4.2018.8611621. Acesso em: 15 jul., 2020.

KUMARI, A.; TANWAR, S.; TYAGI, S.; KUMAR, N. Fog computing for Healthcare 4.0 environment: opportunities and challenges. **Computers & Electrical Engineering**, [S.L.], v.

72, p. 1-13, nov., 2018. Disponível em: http://dx.doi.org/10.1016/j.compeleceng.2018.08.015. Acesso em: 12 jul., 2021.

KUO, T. T.; KIM, H. E.; OHNO-MACHADO, L. Blockchain distributed ledger technologies for biomedical and health care applications. **Journal of the American Medical Informatics Association**, v. 24, n. 6, p. 1211–1220, 2017.

LAI, Y. The latent class analysis in telemedicine user in taiwan, in 2016 **International Conference on Applied System Innovation (ICASI)**, p. 1–3, 2016.

LANGLEY, D. J.; VAN DOORN, J.; NG, I. C. L.; STIEGLITZ, S.; LAZOVIK, A.; BOONSTRA, A. The Internet of Everything: smart things and their impact on business models. **Journal Of Business Research**, [S.L.], v. 122, p. 853-863, jan. ,2021. Disponível em: http://dx.doi.org/10.1016/j.jbusres.2019.12.035. Acesso em: 2 nov., 2021.

LAUSLAHTI, K.; MATTILA, J.; SEPPALA, T. Smart Contracts How Will Blockchain Technology Affect Contractual Practices? **ETLA Reports.** n.68. Research Institute of the Finnish Economy. 2017. Disponível em: https://pub.etla.fi/ETLA-Raportit-Reports-68.pdf. Acesso em: 9 abr., 2020.

LEE, A. R; KIM, M. G.; KIM, I. K. SHAREChain: healthcare data sharing framework using blockchain-registry and fhir. **2019 Ieee International Conference On Bioinformatics And Biomedicine (Bibm)**, [S.L.], p. 1087-1090, nov., 2019. Disponível em: http://dx.doi.org/10.1109/bibm47256.2019.8983415. Acesso em: 12 mar., 2020.

LEE, H. Home IoT resistance: Extended privacy and vulnerability perspective. **Telematics and Informatics**, [*s. l.*], v. 49, n. February, p. 101377, 2020. Disponível em: https://doi.org/10.1016/j.tele.2020.101377. Acesso em: 29 fev., 2021.

LÉVY, P. **O Que é o Virtual?** São Paulo: Editora 34, 1996.

_____. **Cibercultura**. São Paulo: Editora 34, 1999.

LIU, W.; PARK, E.K.; ZHU, S.s.; KRIEGER, U. Smart and Connected e-Health R&D platform. **2015 17Th International Conference On E-Health Networking, Application & Services (Healthcom)**, [S.L.], p. 677-679, out., 2015. Disponível em: http://dx.doi.org/10.1109/healthcom.2015.7454591. Acesso em: 15 jan., 2021.

LU, Y. F.; CHEN, H. M.; KUO, C. F.; CHEN, B. T.; DAI, Z. Y. Enhanced Privacy with Blockchain-based Storage for Data Sharing. **Proceedings Of The International Conference On Research In Adaptive And Convergent Systems**, [S.L.], p. 124-129, 13 out., 2020. Disponível em: http://dx.doi.org/10.1145/3400286.3418242. Acesso em: 14 jul., 2021.

LOIZOU, C.; KARASTOYANOVA, D.; SCHIZAS, C. N. Measuring the Impact of Blockchain on Healthcare Applications. In: , **2019, New York, NY, USA. Proceedings of the 2nd International Conference on Applications of Intelligent Systems**. New York, NY, USA: Association for Computing Machinery, 2019. Disponível em: https://doi.org/10.1145/3309772.3309806. Acesso em: 1 jul., 2020.

LYRA, J. **Blockchain e Organizações Descentralizadas**. Rio de Janeiro: Brasport, 2019. 135 p.

MAHMUD, H.; RAHMAN, T. An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone. **Peer-To-Peer Networking And Applications**, [S.L.], v. 14, n. 6, p. 3758-3777, jul., 2021. Disponível em: http://dx.doi.org/10.1007/s12083-021-01210-6. Acesso em: 22 jul., 2022.

MAHORE, V.; AGGARWAL, P.; ANDOLA, N.; RAGHAV, G.; VENKATESAN, S. Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain. **2019 Ieee Conference On Information And Communication Technology**, [S.L.], p. 1-6, dez., 2019. Disponível em: http://dx.doi.org/10.1109/cict48419.2019.9066204. Acesso em: 12 jul., 2020.

MATSUMOTO, Y.; OGAWA, M.; TSUJI, M. Economic evaluation of m-Health: case of e-ambulance in japan. **2016 Ieee 18Th International Conference On E-Health Networking, Applications And Services (Healthcom)**, [S.L.], p. 1-6, set., 2016. Disponível em: http://dx.doi.org/10.1109/healthcom.2016.7749505. Acesso em: 19 jul., 2020.

MAURI, L.; CIMATO, S.; DAMIANI, E. A Comparative Analysis of Current Cryptocurrencies. **Proceedings Of The 4Th International Conference On Information Systems Security And Privacy**, [S.L.], p. 127-138, 2018. SCITEPRESS - Science and Technology Publications. Disponível em: http://dx.doi.org/10.5220/0006648801270138. Acesso em: 28 nov., 2020.

MCGARRY, K. **O contexto dinâmico da informação**: uma análise introdutória. Tradução de Helena Vilar de Lemos. 2. ed. Brasília: Briquet de Lemos, 1999.

MIKHAILOV, A. I; CHERNYI, A. I.; GILYAREVSKY, R. S. Informatics: its scope and methods. In: FID/RI- International Federation for Documentation. Study Committee Research on Theoretical Basis of Information. **On theoretical problems of Informatics**, Moscou, ALL-Union for Scientific and Technical Information, 1969.

MILUTINOVIC, M.; HE, W.; WU, H.; KANWAL, M. Proof of Luck: an efficient blockchain consensus protocol. **Proceedings of The 1st Workshop On System Software For Trusted Execution - Systex '16**, [s.l.], p. 1-6, 2016. Disponível em: https://dl.acm.org/doi/abs/10.1145/3007788.3007790. Acesso em: 12 abr., 2020.

MIZRAHI, A. **A blockchain-based property ownership recording system**. 2015. Disponível em: http://tiny.cc/01p35y. Acesso em: 21 jul., 2019.

MOHAMED, W.; ABDELLATIF, M. M. Telemedicine: An IoT Application for Healthcare systems, **ACM International Conference Proceeding Series**, p. 173–177, 2019. Disponível em: 10.1145/3328833.3328881. Acesso em: 12 dez., 2020.

MOREIRA NETO, M.; COUTINHO, E. F.; MOREIRA, L. O.; SOUZA, J. N.; AGOULMINE, N. A Proposal for Monitoring People of Health Risk Group Using IoT Technologies. **2018 Ieee 20Th International Conference On E-Health Networking,**

Applications And Services (Healthcom), [S.L.], p. 20-25, set., 2018. Disponível em: http://dx.doi.org/10.1109/healthcom.2018.8531196. Acesso em: 1 jul., 2021.

MORROW, E.; ROBERT, G.; MABEN, J.; GRIFFITHS, P. Implementing large-scale quality improvement. **International Journal Of Health Care Quality Assurance**, [S.L.], v. 25, n. 4, p. 237-253, 27 abr., 2012. Disponível em: http://dx.doi.org/10.1108/09526861211221464. Acesso em: 12 jul., 2022.

MUKHIYA, S. K.; RABBI, F.; PUN, K. I; LAMO, Y. An Architectural Design for Self-Reporting E-Health Systems. **2019 Ieee/Acm 1St International Workshop On Software Engineering For Healthcare (Seh)**, [S.L.], p. 1-8, mai., 2019. Disponível em: http://dx.doi.org/10.1109/seh.2019.00008. Acesso em: 12 jul., 2021.

NAIR, A. R.; TANWAR, S. Fog Computing Architectures and Frameworks for Healthcare 4.0. **Fog Computing For Healthcare 4.0 Environments**, [S.L.], p. 55-78, 3 ago., 2020. Disponível em: http://dx.doi.org/10.1007/978-3-030-46197-3_3. Acesso em: 22 jul., 2021.

NAKAMOTO, S. **Bitcoin**: a peer-to-peer electronic cash system. 2008. Disponível em https://bitcoin.org/bitcoin.pdf. Acesso em: 28 jun., 2020.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. **Bitcoin and Cryptocurrency Technologies**: a comprehensive introduction. Princeton, New Jersey:: Princeton University Press, 2016.

NARVA, A. S.; ROMANCITO, G. T.; FABER, M. E.; STEELE, M. E.; KEMPNER, K. M. **Managing CKD by Telemedicine**: The Zuni Telenephrology Clinic, Advances in Chronic Kidney Disease, v. 24, n. 1, p. 6–11, 2017. Disponível em: 10.1053/j.ackd.2016.11.019. Acesso em: 12 jul., 2020.

NATSIAVAS, P.; RASMUSSEN, J.; VOSS-KNUDE, M.; VOTIS, K.; COPPOLINO, L.; CAMPEGIANI, P.; CANO, I.; MARÍ, D.; FAIELLA, G.; CLEMENTE, F.; NALIN, M.; GRIVAS, E.; STAN, O.; GELENBE, E.; DUMORTIER, J.; PETERSEN, J.; TZOVARAS, D.; ROMANO, L.; KOMNIOS I.; KOUTKIAS, V. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange 08 Information and Computing Sciences 0806 Information Systems. **BMC Medical Informatics and Decision Making**, v. 18, n. 85, 2018. Disponível em: https://doi.org/10.1186/s12911-018-0664-0. Acesso em: 12 jul., 2021.

NGUYEN, D. C.; PATHIRANA, P. N.; DING, M.; SENEVIRATNE, A. BEdgeHealth: a decentralized architecture for edge-based iomt networks using blockchain. **Ieee Internet Of Things Journal**, [S.L.], v. 8, n. 14, p. 11743-11757, 15 jul., 2021. Disponível em: http://dx.doi.org/10.1109/jiot.2021.3058953. Acesso em: 29 jan., 2022.

NSENGIMANA, J. P. Reflections upon periclitations in privacy: perspectives from Rwanda's digital transformation. **Health and Technology,** v. 7, p. 377–388, 2017. Disponível em: https://doi.org/10.1007/s12553-017-0196-0. Acesso em: 23 jul., 2020.

OLSON, K.; BOWMAN, M.; MITCHELL, J.; AMUNDSON, S.; MIDDLETON, D.; MONTGOMERY, C. **Sawtooth**: An introduction. Hyperledger Sawtooth Whitepaper, p. 1-7,

2018. Disponível em: https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf. Acesso em: 12 jun., 2020.

OBJECT MANAGEMENT GROUP**. Business Process. Model & Notation (BPMN).** 2022. Disponível em: https://www.omg.org/bpmn/index.htm. Acesso em: 18 out., 2022.

PAPPALARDO, G.; DIMATTEO, T.; CALDARELLI, G.; ASTE, T. Blockchain inefficiency in the Bitcoin peers network. **Epj Data Science,** [S.L.], v. 7, n. 1, p. 2-13, 5 set., 2018. Disponível em: http://dx.doi.org/10.1140/epjds/s13688-018-0159-3. Acesso em: 12 set., 2020.

PADMAVATHI, M.; SURESH, R. M. Secure P2P Intelligent Network Transaction using Litecoin. **Mobile Networks And Applications,** [S.L.], v. 24, n. 2, p. 318-326, abr., 2018. Disponível em: https://link.springer.com/article/10.1007%2Fs11036-018-1044-9. Acesso em: 18 jul., 2020.

PANG, Z.; YANG, G.; KHEDRI, R.; ZHANG, Y. T. Introduction to the Special Section: convergence of automation technology, biomedical engineering, and health informatics toward the healthcare 4.0. **Ieee Reviews In Biomedical Engineering**, [S.L.], v. 11, p. 249-259, 2018. Disponível em: http://dx.doi.org/10.1109/rbme.2018.2848518. Acesso em: 12 jul., 2020.

PEREZ-NOBOA, B.; SOLEDISPA-CARRASCO, A.; PADILLA, V. S.; VELASQUEZ, W. Teleconsultation apps in the COVID-19 pandemic: The case of Guayaquil City, Ecuador**. IEEE Engineering Management Review,** v. 49, Issue: 1, Firstquarter, mar., 2021. Disponível em:10.1109/emr.2021.3052928, 2021. Acesso em: 29 dez., 2021.

PODGORELEC, B.; KERSIC, V.; TURKANOVIC, M. Analysis of Fault Tolerance in Permissioned Blockchain Networks. **2019 XXVII International Conference On Information, Communication And Automation Technologies (Icat)**, [S.L.], p. 1-6, out. 2019. Disponível em: http://dx.doi.org/10.1109/icat47117.2019.8938836. Acesso em: 4 set., 2020.

PRESSMAN, R. S.; MAXIM, B. **Engenharia de software**: uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2016.

PRIBERAM. **Dicionário Priberam da Língua Portuguesa** (DPLP). Novo. [Ebook]. Priberam.2011. ISBN:978-989-96820-2-3. Priberam Informática, S. A., 2011.

PUSTIŠEK, M.; ŽIVIĆ, N.; KOS, A. **Blockchain**: technology and applications for Industry 4.0, smart energy, and smart cities. [S.l.] Berlin; Bosten De Gruyter, 2022.

QADRI, Y. A.; NAUMAN, A.; ZIKRIA, Y. B.; VASILAKOS, A. V.; KIM, S. W. The Future of Healthcare Internet of Things: a survey of emerging technologies. **Ieee Communications Surveys & Tutorials**, [S.L.], v. 22, n. 2, p. 1121-1167, 2020. Disponível em: http://dx.doi.org/10.1109/comst.2020.2973314. Acesso em: 19 jul., 2021.

R3. **On-Premises Deployment**. Architecture Overview. 2018. Disponível em: https://solutions.corda.net/deployment/onprem/corda-node-architecture-components.html. Acesso em: 28 mai., 2020.

RAMLI, R; ALI, N. Teleconsultation as Knowledge Management System: recognizing the issues contributing to its underutilization in hospitals. **2018 International Conference On Advanced Computer Science And Information Systems (Icacsis)**, [S.L.], p. 277-282, out., 2018. Disponível em: http://dx.doi.org/10.1109/icacsis.2018.8618203. Acesso em: 2 jun., 2020.

RIBEIRO, R. C.; CANEDO, E. D. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. In: 2020, New York, NY, USA. **The 21st Annual International Conference on Digital Government Research**. New York, NY, USA: Association for Computing Machinery, 2020. p. 175–184. Disponível em: https://doi.org/10.1145/3396956.3398252. Acesso em: 12 jan., 2021.

ROMA, C. A.; HASAN, M. A. Energy Consumption Analysis of XRP Validator. **IEEE International Conference on Blockchain and Cryptocurrency (IEEE ICBC 2020)**. 2020. Disponível em: https://uwspace.uwaterloo.ca/bitstream/handle/10012/15717/romahasan_xrpvalidator.pdf?sequence=1&isallowed=y. Acesso em: 5 nov., 2020.

SAECHOW, S.; KAMOLPHIWONG, S.; CHANDEEYING, V. Web-based teleconsultation for clinical diagnosis. **2014 International Conference On Electronics, Information And Communications (Iceic)**, [S.L.], p. 34-36, jan. 2014.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações**. Perpectivas em Ciência da Informação**, v. 1, n. 1, p. 41-62, jan./jun., 1996.

. Information Science. **Encyclopedia Of Library And Information Sciences, Third Edition**, [s.l.], p. 2570-2585, dez., 2009.

SACKETT, D. L.; STRAUS, S. E.; RICHARDSON, W. S.; ROSENBERG, W.; HAYNES, R. B. **Evidence-based medicine**: how to practice and teach ebm. Edinburgh: Churchill Livingstone; 2000.

SARAF, C.; SABADRA, S. Blockchain Platforms: a compendium**. 2018 IEEE International Conference on Innovative Research and Development (ICIRD)**, Bangkok, p. 1-6, 2018.

SCHLATT, V.; SEDLMEIR, J.; TRAUE, J.; VÖLTER, F. Harmonizing Sensitive Data Exchange and Double-spending Prevention Through Blockchain and Digital Wallets: the case of e-prescription management. **Distributed Ledger Technologies**: Research and Practice, [S.L.], v. 2, n. 1, p. 1-31, mar., 2023. Disponível em: http://dx.doi.org/10.1145/3571509. Acesso em: 12 abr., 2023.

SENIVONGSE, C.; BENNET, A.; MARIANO, S. Utilizing a systematic literature review to develop an integrated framework for information and knowledge management systems. **VINE Journal of Information and Knowledge Management Systems**, [*s. l.*], v. 47, n. 2, p. 250–264, 2017. Disponível em: https://doi.org/10.1108/vjikms-03-2017-0011. Acesso em: 12 jul., 2020.

SHAIKH, T. A.; ALI, R. Fog-IoT Environment in Smart Healthcare: a case study for student stress monitoring. **Fog Computing For Healthcare 4.0 Environments**, [S.L.], p. 211-250, 3 ago., 2020. Disponível em: http://dx.doi.org/10.1007/978-3-030-46197-3_9. Acesso em: 12 jul., 2021.

SHARMA, D.; AUJLA, G. S.; BAJAJ, R. Evolution from ancient medication to human-centered Healthcare 4.0: a review on health care recommender systems. **International Journal Of Communication Systems**, [S.L.], e4058, 9 set., 2019. Disponível em: http://dx.doi.org/10.1002/dac.4058. Acesso em: 12 jul., 2021.

SHERMIN, V. Disrupting governance with blockchains and smart contracts. **Strategic Change**, [s.l.], v. 26, n. 5, p. 499-509, set. 2017. Wiley. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/jsc.2150. Acesso em: 15 abr., 2020.

SIDDAWAY, A. P.; WOOD, A. M.; HEDGES, L. V. How to Do a Systematic Review: A Best Practice Guide for Conducting and Reporting Narrative Reviews, Meta-Analyses, and Meta-Syntheses. **Annual Review of Psychology**, [*s. l.*], v. 70, n. 1, p. 747–770, 2018.

SILVA, C. A.; AQUINO JUNIOR, G. S.; MELO, S. R. M. A Blockchain-Based Approach for Privacy Control of Patient's Medical Records in the Fog Layer. *In*: , 2019, New York, NY, USA. **Proceedings of the 25th Brazillian Symposium on Multimedia and the Web**. New York, NY, USA: ACM, p. 133–136, 2019. Disponível em: https://doi.org/10.1145/3323503.3360640. Acesso em: 13 abr., 2021.

SITONIO, C.; NUCCIARELLI, A. The Impact of Blockchain on the Music Industry, **29th European Regional Conference of the International TelecommunicationsSociety (ITS)**, 2018. Disponível em: http://hdl.handle.net/10419/184968. Acesso em: 19 abr., 2020.

SMOLIJ, K.; DUN, K. Patient health information management: searching for the right model. **Perspectives in health information management**, [*s. l.*], v. 3, n. 10, p. 10, 2006. Disponível em: http://www.ncbi.nlm.nih.gov/pubmed/18066368. Acesso em: 17 ago., 2021.

SOLTANI, R.; NGUYEN, U. T.; AN, A. A new approach to client onboarding using self-sovereign identity and distributed ledger, in: **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber**, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), p. 1129-1136, mar., 2019.

SOUZA, R. S.; ALMEIDA, M. B.; BARACHO, R. M. A. Ciência da Informação em transformação: big data, nuvens, redes sociais e Web Semântica. **Ciência da Informação**, Brasília, v. 42, n.2, p. 159-173, maio/ago. 2013. Disponível em: https://revista.ibict.br/ciinf/article/view/1379. Acesso em: 09 mar., 2020.

STINSON, D. R.; PATERSON, M. B. **Cryptography** - Theory and Practice. CRC Press, 4. ed. 2019.

SWAN, M. Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. **Advance in Computers**, Blockchain Technology: Platforms, Tools and Use Cases. p. 121-162, 2018. Disponível em:

https://www.sciencedirect.com/science/article/pii/S0065245818300287. Acesso em: 30 jun., de 2020.

_____. **Blockchain**: blueprint for a new economy. Califórnia: O'Reilly Media, 2015.

TANENBAUM, A. S.; STEEN, M. V. **Sistemas distribuídos**: princípios e paradigmas. 2. ed. São Paulo: Pearson Educación, 2008.

TAYLOR, R. S. Professional aspects of information science and technology. In: CUADRA, C.A. (Ed). **Annual Review of Information Science and Technology**. New York: John Wiley, v. 1, 1966, p. 15-40.

THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform**. 2018 IEEE 26th International Symposium On Modeling, Analysis, And Simulation Of Computer And Telecommunication Systems (mascots)**, [s.l.], p. 264-276, set., 2018. Disponível em: https://ieeexplore.ieee.org/document/8526892/. Acesso em: 20 de abr., 2020.

THILAGAVATHY, R.; RENJITH, P. N.; LALITHA, R. V. S.; MURTHY, M. Y. B.; SUCHARITHA, Y.; NARAYANAN, S. L. A novel framework paradigm for EMR management cloud system authentication using blockchain security network. **Soft Computing**, [S.L.], p. 97-105, 3 mar., 2023. Disponível em: http://dx.doi.org/10.1007/s00500-023-07958-8. Acesso em: 12 abr., 2023.

THUEMMLER, C.; BAI, C. **Health 4.0**: How virtualization and big data are revolutionizing healthcare, 1–254 pp., Springer International Publishing, 2017.

ULRICH, F. **Bitcoin** – a moeda na era digital. São Paulo: LVM, 2014. 100 p.

VALENTA, M.; SANDNER, P. Comparison of Ethereum, Hyperledger Fabric and Corda. 2017. **FSBC Working Paper**. Frankfurt School of Finance & Management. Disponível em: https://pdfs.semanticscholar.org/00c7/5699db7c5f2196ab0ae92be0430be4b291b4.pd. Acesso em: 21 abr., 2020.

VENKATAPURAM, S. **Health Justice**. Cambridge: Polity Press, 2011.

VORA, J.; NAYYAR, A.; TANWAR, S.; TYAGI, S.; KUMAR, N.; OBAIDAT, M. S.; RODRIGUES, J. J. P. C.. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. *In*: , 2018. **2018 IEEE Globecom Workshops (GC Wkshps)**. [*S. l.: s. n.*], p. 1–6, 2018. Disponível em: https://doi.org/10.1109/glocomw.2018.8644088. Acesso em: 12 jul., 2020.

XIAO, Y.; WATSON, M. Guidance on Conducting a Systematic Literature Review. **Journal of Planning Education and Research**, [*s. l.*], v. 39, n. 1, p. 93–112, 2019. Disponível em: https://doi.org/10.1177/0739456X17723971. Acesso em: 12 jul., 2021.

XU, L.; BAGULA, A.; ISAFIADE, O.; MA, K.; CHIWEWE, T.. Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform. **2019 Itu Kaleidoscope**: ICT for

Health, [S.L.], p. 1-8, dez., 2019. Disponível em: http://dx.doi.org/10.23919/ituk48006.2019.8995905. Acesso em: 12 set., 2020.

XU, Z. An empirical study of patients' privacy concerns for health informatics as a service. **Technological Forecasting and Social Change**, [s. l.], v. 143, n. January, p. 297–306, 2019. Disponível em: https://doi.org/10.1016/j.techfore.2019.01.018. Acesso em: 20 jul., 2020.

ZALA, K.; THAKKAR, H. K.; JADEJA, R.; SINGH, P.; KOTECHA, K.; SHUKLA, M. PRMS: design and development of patients ⁝ e-healthcare records management system for privacy preservation in third party cloud platforms. **Ieee Access**, [S.L.], v. 10, p. 85777-85791, 2022. Disponível em: http://dx.doi.org/10.1109/access.2022.3198094. Acesso em: 12 jan., 2023.

ZHANG, P.; SCHMIDT, D. C.; WHITE, J.; LENZ, G.. Blockchain Technology Use Cases in Healthcare. **Advances in Computers**, Elsevier, v. 111, p. 1–41, 30, ago. 2018a.

ZHANG, P.; SCHMIDT, D. C.; WHITE, J.; LENZ, G.; ROSENBLOOM, S. T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. **Computational and Structural Biotechnology Journal**, [*s. l.*], v. 16, p. 267–278, 2018b.

ZHANG, A.; LIN, X.. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. **Journal Of Medical Systems**, [S.L.], v. 42, n. 8, p. 1-18, jun., 2018. Disponível em: http://dx.doi.org/10.1007/s10916-018-0995-5. Acesso em: 12 jan., 2021.

ZHENG, X.; MUKKAMALA, R. R.; VATRAPU, R.; ORDIERES-MERE, J. Blockchain-based Personal Health Data Sharing System Using Cloud Storage. **2018 Ieee 20Th International Conference On E-Health Networking, Applications And Services (Healthcom)**, [S.L.], p. 1-6, set. 2018. 2018a. Disponível em: http://dx.doi.org/10.1109/healthcom.2018.8531125. Acesso em: 12 ago., 2020.

ZHENG, Z.; XIE, S.; DAI, H. N.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: a survey. International Journal Of Web And Grid Services, [s.l.], v. 14, n. 4, p. 1-23, 2018b. Disponível em: htttp://dx.doi.org/10.1504/ijwgs.2018.095647. Acesso em: 21 abr., 2020.

ZHOU, J.; TANG, F.; ZHU, H.; NAN, N.; ZHOU, Z. Distributed Data Vending on Blockchain. **2018 Ieee International Conference On Internet Of Things (ithings)** And Ieee Green Computing And Communications (greencom) And Ieee Cyber, Physical And Social Computing (cpscom) And Ieee Smart Data (smartdata)**,** [s.l.], p. 1-10, jul. 2018. IEEE. Disponível em: http://dx.doi.org/10.1109/cybermatics_2018.2018.00201. Acesso em: 13 abr., 2020.

WORLD HEALTH ORGANIZATION, mHealth: New horizons for health through mobile technologies. **Global Observatory for eHealth**, v. 3, 66–71, jun., 2011.

YASSEIN, M. B.; HMEIDI, I.; AL-HARBI, M.; MRAYAN, L.; MARDINI, W.; KHAMAYSEH, Y. IoT-based healthcare systems. **Proceedings Of The Second International Conference On Data Science, E-Learning And Information Systems - Data**

'19, [S.L.], p. 1-9, 2019. Disponível em: http://dx.doi.org/10.1145/3368691.3368721. Acesso em: 12 jul., 2021.

YU, Y.; LI, Q.; ZHANG, Q.; HU, W.; LIU, S. Blockchain-Based Multi-Role Healthcare Data Sharing System. **2020 Ieee International Conference On E-Health Networking, Application & Services (Healthcom)**, [S.L.], p. 1-6, 1 mar., 2021. Disponível em: http://dx.doi.org/10.1109/healthcom49281.2021.9399028. Acesso em: 12 dez., 2021.

YUE, X.; WANG, H.; JIN, D.; LI, M.; JIANG, W. Healthcare Data Gateways: found healthcare intelligence on blockchain with novel privacy risk control. **Journal Of Medical Systems**, [S.L.], v. 40, n. 10, p. 1-8, 26 ago., 2016. Disponível em: http://dx.doi.org/10.1007/s10916-016-0574-6. Acesso em: 12 out., 2020.

YUSOF, M. M.; STERGIOULAS L.; ZUGIC, J. Health information systems adoption: Findings from a systematic review**, Studies in Health Technology and Informatics**, MEDINFO 2007, v. 129, n. 1, p. 262–266, 2007. Disponível em: https://ebooks.iospress.nl/publication/10975. Acesso em: 15 nov., 2020.

APÊNDICE A – CÓDIGO FONTE PRINCIPAL DO SMART CONTRACT

Nos códigos das figuras a seguir estão compostos os principais trechos desenvolvidos. O código completo pode ser encontrado no ambiente https://github.com/patryckrm/.

Figura 27 – Estrutura inicial do código do Smart Contract.

```
pragma solidity >=0.7.0 <0.9.0;

contract Saude {

    address owner = msg.sender;
    uint registroId = 0;

    struct RegistroSaude {
        uint id;
        string descricao;
        address dono;
        uint dataPublicacao;
    }

    struct Liberacao {
        address paciente;
        address medico;
    }

    RegistroSaude[] public registros;

    Liberacao[] public liberacoes;

    function recebeRegistroSaude(string memory descricao) public {
        RegistroSaude memory r;
        r.id = proximoID();
        r.descricao = descricao;
        r.dataPublicacao = block.timestamp;
        r.dono = msg.sender;
        registros.push(r);
    }
```

Fonte: Elaborada pelo autor.

Figura 28 – Parte do código para liberação do médico.

```
function liberarAcesso(address carteira) public {
    Liberacao memory l;
    l.paciente = msg.sender;
    l.medico = carteira;
    liberacoes.push(l);
}

function verificaLiberacao(address paciente) public view returns (int indice) {
    Liberacao memory l;
    l.paciente = paciente;
    l.medico = msg.sender;

    //encontra o indice
    int indice = -1;
    for (uint i=0; i<liberacoes.length; i++) {
        Liberacao memory atual = liberacoes[i];
        if ( atual.paciente == l.paciente && atual.medico == l.medico ){
            indice = int(i);
        }
    }
    return indice;
}
```

Fonte: Elaborada pelo autor.

Figura 29 – Parte 2 do código para liberação do médico.

```
function verificaLiberacao(address paciente) public view returns (int indice) {
    Liberacao memory l;
    l.paciente = paciente;
    l.medico = msg.sender;

    //encontra o indice
    int indice = -1;
    for (uint i=0; i<liberacoes.length; i++) {
        Liberacao memory atual = liberacoes[i];
        if ( atual.paciente == l.paciente && atual.medico == l.medico ){
            indice = int(i);
        }
    }
    return indice;
}

function revogarAcesso(address carteira) public {
    Liberacao memory l;
    l.paciente = msg.sender;
    l.medico = carteira;

    //encontra o indice
    int indice = -1;
    uint indiceU = 0;
    for (uint i=0; i<liberacoes.length; i++) {
        Liberacao memory atual = liberacoes[i];
        if ( atual.paciente == msg.sender && atual.medico == carteira ){
            indice = int(i);
            indiceU = i;
        }
    }
    if (indice > -1){
        //move o ultimo item para o indice atual e faz um pop
        liberacoes[indiceU] = liberacoes[liberacoes.length - 1];
        liberacoes.pop();
    }
}
```

Fonte: Elaborada pelo autor.

Figura 30 – Funções de consulta (parte 1).

```
function consultarRegistroSaude( uint index ) public view returns (RegistroSaude memory r) {
    if ( registros.length >= index ) {
        r = registros[index];
    }
    //address solicitante = msg.sender;
    //address paciente = r.dono;
    return r;
}

function consultar( uint index ) public view returns (uint, string memory, address, uint) {
    RegistroSaude storage r;
    if ( registros.length >= index ) {
        r = registros[index];
        return (r.id, r.descricao, r.dono, r.dataPublicacao);
    }
    return null;
}

function consultarLiberacao( uint index ) public view returns (address, address) {
    Liberacao storage l;
    if ( liberacoes.length >= index ) {
        l = liberacoes[index];
        return (l.paciente, l.medico);
    }
    return null;
}

function consultarTotalDeRegistros() public view returns (uint) {
    if (registros.length > 0) {
        return registros.length;
    }
    return 0;
}
```

Fonte: Elaborada pelo autor.

Figura 31 – Funções de consulta (parte 2).

```
    function consultarTotalDeLiberacoes() public view returns (uint) {
        if (liberacoes.length > 0) {
            return liberacoes.length;
        }
        return 0;
    }

    function proximoID() private returns (uint) {
        return registroId++;
    }

}
```

Fonte: Elaborada pelo autor.

APÊNDICE B – CÓDIGOS RELACIONADOS AO BACK-END

Nos códigos das figuras a seguir estão partes da lógica desenvolvida no *back-end*. O código completo com maiores detalhes também pode ser encontrado no ambiente https://github.com/patryckrm/.

Figura 32 – Novo registro de saude (busca a chave privada e chama o smart contract).

```
@POST
@Consumes(MediaType.APPLICATION_JSON)
@Produces(MediaType.APPLICATION_JSON)
public String novoRegistro(@HeaderParam("private-key")String privateKey, RegistroSaudeModel registroSaudeModel) throws Exception {

    Saude saude = saudeRepository.getFrom(privateKey);
    LOGGER.info( String.format("novo registro a ser inserido em [%s] ", saude.getContractAddress()));

    //json
    String dados = new ObjectMapper().writeValueAsString(registroSaudeModel);

    //criptografa com a chave privada
    String assinado = this.chavesRepository.assinar(privateKey,dados);
    LOGGER.info( String.format("Registro [%s] ", dados));
    LOGGER.info( String.format("Registro criptografado [%s] ", assinado));

    TransactionReceipt receipt = saude.recebeRegistroSaude( assinado )
                                      .send();

    return receipt.getBlockHash();
}
```

Fonte: Elaborada pelo autor.

Figura 33 – Lógica de decriptografia (dono ou liberado pelo dono do registro)

```
public RegistroSaudeModel tentaDescriptografarRegistro(String chavePrivada, String dono, String conteudo ){
    try{
        Credentials credentials = Credentials.create(chavePrivada);
        if (credentials.getAddress().equalsIgnoreCase(dono)) {
            LOGGER.info(String.format("Consulta pelo dono do registro [%s] ", dono));
            LOGGER.info(String.format("Registro criptografado [%s] ", conteudo));
            String descStr = chavesRepository.ler(chavePrivada, conteudo);

            LOGGER.info(String.format("Registro criptografado [%s] ", conteudo));
            LOGGER.info(String.format("Registro descriptografado [%s] ", descStr));
            RegistroSaudeModel descriptografado = new ObjectMapper().readValue(descStr, RegistroSaudeModel.class);
            return descriptografado;
        }
        else{
            //verifica se esta liberado
            LOGGER.info(String.format("Verificando se [%s] foi liberado por [%s]", credentials.getAddress(), dono));
            Saude saude = saudeRepository.getFrom(chavePrivada);
            BigInteger indice = saude.verificaLiberacao(dono)
                    .send();
            LOGGER.info(String.format("Liberado? [%s]", indice.toString()));
            if (indice.intValue() > -1){
                //descriptografa (com a chave publica do dono)
                LOGGER.info(String.format("Buscando a chave publica de [%s] ", dono));
                String descStr = chavesRepository.lerDoEndereco(dono, conteudo);
                LOGGER.info(String.format("Registro criptografado [%s] ", conteudo));
                LOGGER.info(String.format("Registro descriptografado [%s] ", descStr));
                RegistroSaudeModel descriptografado = new ObjectMapper().readValue(descStr, RegistroSaudeModel.class);
                return descriptografado;
            }
            return null;
        }
    }
    catch (Exception ex){
        ex.printStackTrace();
        LOGGER.severe(ex.getMessage());
    }
```

Fonte: Elaborada pelo autor.

Figura 34 – Lógica que busca a chave privada no diretorio de chaves (parte 1).

```
public PrivateKey carregarChavePrivada(String chavePrivadaCarteira) throws Exception {
    this.verificaParametros(chavePrivadaCarteira);
    this.verificarChave(chavePrivadaCarteira);

    Credentials c = Credentials.create(chavePrivadaCarteira);
    String diretorio = this.diretorioChaves + File.separator + c.getAddress();
    File f = new File( pathname: diretorio + File.separator + NOME_CHAVE_PRIVADA);

    try(FileInputStream fis = new FileInputStream(f);
        DataInputStream dis = new DataInputStream(fis) ) {
        byte[] keyBytes = new byte[(int) f.length()];
        dis.readFully(keyBytes);
        byte[] decoded = Base64.getDecoder().decode(keyBytes);
        PKCS8EncodedKeySpec spec = new PKCS8EncodedKeySpec(decoded);
        KeyFactory kf = KeyFactory.getInstance(ALGORITMO);
        return kf.generatePrivate(spec);
    } catch (Exception e) {
        throw new Exception(e);
    }
}
```

Fonte: Elaborada pelo autor.

Figura 35 – Lógica que busca a chave privada no diretorio de chaves (parte 2).

```
private void verificaParametros(String chavePrivadaCarteira) throws Exception {
    if (chavePrivadaCarteira == null || chavePrivadaCarteira.trim().length() < 1){
        throw new Exception("Chave privada da carteira é obrigatória");
    }
    if ( this.diretorioChaves == null || chavePrivadaCarteira.trim().length() < 1){
        throw new Exception("Diretório de chaves é obrigatório na config");
    }
    else{
        File f = new File(this.diretorioChaves);
        if (!f.exists() || !f.isDirectory()){
            throw new Exception("Diretório de chaves não existe: " + this.diretorioChaves);
        }
    }
}
```

Fonte: Elaborada pelo autor.

Figura 36 – Lógica que busca a chave privada no diretorio de chaves (parte 3).

```
public void verificarChave(String chavePrivadaCarteira) throws Exception {
    this.verificaParametros(chavePrivadaCarteira);
    Credentials c = Credentials.create(chavePrivadaCarteira);
    String diretorio = this.diretorioChaves + File.separator + c.getAddress();
    File f = new File(diretorio);
    if (!f.exists()){
        f.mkdir();
        KeyPair pair = this.salvarEmDiscoNovoKeypair(f);
    }
    else{
        LOGGER.info( msg: "Par de Chaves Encontrado");
    }
}
```

Fonte: Elaborada pelo autor.