Journal of Technology & Information

Blockchain e a Saúde: A Segurança de Dados Sensíveis

Blockchain and Health: The Security of Sensitive Data

Recebido: 21/12/2022 | Revisado: 23/12/2022 | Aceito: 24/09/2023 | Publicado: 25/09/2023

https://www.doi.org/10.5281/zenodo.8376820

Fernando Henrique Felix de Siqueira
Faculdade de Tecnologia de Santana de Parnaíba - CEETEPS
https://orcid.org/0000-0003-2389-3019
fernando.siqueira3@fatec.sp.gov.br

Michelle Santos Nascimento
Faculdade de Tecnologia de Santana de Parnaíba - CEETEPS
https://orcid.org/0000-0002-8635-7515
michelle.nascimento@fatec.sp.gov.br

Renato Moraes de Menezes
Faculdade de Tecnologia de Santana de Parnaíba - CEETEPS
https://orcid.org/0000-0003-3141-5180
renato.menezes@fatec.sp.gov.br

Wiliam Carlos Galvão
Faculdade de Tecnologia de Santana de Parnaíba - CEETEPS
https://orcid.org/0000-0003-3171-1721
wiliam.galvao@fatec.sp.gov.br

Resumo

O uso cada vez maior de meios tecnológicos para processamento e tratamento das informações pessoais na área da saúde demanda uma preocupação por mitigar os riscos e proteção dos dados. Além do fator reputação, as empresas que coletam e tratam os dados devem estar atentas às possíveis sanções respaldadas pelas leis vigentes que garantem, dentre outros direitos, o de privacidade. Para isso, a tecnologia *Blockchain* vem sendo utilizada como ferramenta de proteção dos dados sensíveis na área da saúde, uma vez que funciona de forma descentralizada e permite o rastreamento das operações. O *Blockchain* é um "livro digital" imutável que registra todas as transações realizadas, onde as informações são compartilhadas entre os membros da rede e qualquer tentativa de adulteração num determinado ponto gera um erro, pois os demais pontos possuem um resumo da operação original realizada. No Brasil, os dados sensíveis são regulados pela Lei Geral de Proteção dos Dados e por outras leis mais antigas, que dispõem sobre a coleta e uso das informações. Utilizando a metodologia *Design Science Research*, este artigo procura verificar como o *Blockchain* é utilizado nesse contexto e assim criar *frameworks* reutilizáveis. O objetivo é analisar a viabilidade e efetividade do uso da tecnologia na saúde quando se trata de privacidade das informações de natureza médica.

Palavras-chave: Saúde. *Blockchain*. LGPD. DATASUS.

Journal of Technology & Information

Abstract

The increasing use of technological means for processing and processing personal information in the health area demands a concern for mitigating risks and protecting data. In addition to the reputation factor, companies that collect and process data must be aware of possible sanctions supported by current laws that guarantee, among other rights, privacy. For this, Blockchain technology has been used as a tool to protect sensitive data in the health area, since it works in a decentralized way and allows the tracking of operations. Blockchain is an immutable "digital ledger" that records all transactions carried out, where information is shared between network members and any attempt to tamper with a given point generates an error, as the other points have a summary of the original operation performed. In Brazil, sensitive data is regulated by the General Data Protection Law and other older laws, which provide for the collection and use of information. Using the Design Science Research methodology, this article seeks to verify how Blockchain is used in this context and thus create reusable frameworks. The objective is to analyze the feasibility and effectiveness of the use of technology in health when it comes to the privacy of medical information.

Keywords: Health. Blockchain. GDPR. DATASUS.

1. Introdução

Esta pesquisa teve por objetivo elucidar como a tecnologia *Blockchain* pode ser utilizada na área da saúde para proteger e facilitar o transporte dos dados sensíveis. Conforme a Lei Geral de Proteção de Dados Pessoais (LGPD), os dados sensíveis requerem um cuidado maior dos envolvidos no processo de coleta, armazenamento e tratamento de dados, pois caso ocorra algum vazamento, além disso significar uma infração com relação à privacidade, por exemplo, pode causar um transtorno enorme para o usuário que teve seus dados sensíveis expostos, mas estes podem ser utilizados como formas de discriminação (NUNES *et al.*, 2021)

Camara *et al*. (2021) menciona que o Brasil por sua vez está adotando no Governo projetos de *Blockchain* voltado para políticas governamentais e sociais. O projeto que mais chama a atenção é sem dúvidas a utilização da tecnologia *Blockchain* no Sistema Único de Saúde (SUS), com a ideia de melhorar o cenário de armazenamento dos dados em hospitais e também laboratórios, para evitar os problemas com vazamentos de dados sensíveis dos pacientes.

A tecnologia *Blockchain* desponta como um grande divisor de águas para resolução de problemas relacionados à integridade e segurança dos dados, seja na área da saúde como em outros cenários cuja proteção dos dados é o ponto principal, visto que é uma tecnologia baseada em redes de cadeia de blocos de dados descentralizados e

assinados digitalmente, impedindo que os dados sejam roubados por cibercriminosos, dificultando o trabalho dos *hackers*, trazendo conceitos e tecnologias cada vez mais inovadoras e avançadas, evitando que dados sejam alterados em qualquer um dos pontos, seja na origem ou no destino (NUNES *et al.*, 2021).

É neste contexto que entra o *Blockchain*, pois conforme Nunes *et al.* (2021) com essa tecnologia é possível garantir que os dados médicos, que compreendem: exames, laudos, históricos de consultas, receituário e todos os documentos referente à saúde do paciente, não sejam visualizados por terceiros que não estão autorizados.

Diante deste contexto, emerge a seguinte Questão de Pesquisa: Quais os benefícios de se utilizar o *Blockchain* na área da saúde?

A fim de responder esta questão, tem-se por objetivo principal pesquisar em artigos científicos quais os principais avanços tecnológicos estão em desenvolvimento nesta área. Para atingir esse objetivo principal, faz-se necessário que sejam atingidos os seguintes objetivos específicos: (1) Entender o funcionamento da *Blockchain* na Saúde; (2) Analisar a eficiência das soluções implantadas e o grau de *compliance*.

2. Referencial Teórico

2.1. Blockchain

Blockchain é uma tecnologia que permite o rastreamento do envio e recebimento de informações ou transações financeiras, dependendo de qual seu uso.

Segundo Lago (2017) funciona como o livro-razão utilizado na contabilidade clássica, mas na *Blockchain* os registos das operações estão dispostos na internet de forma descentralizada – não havendo assim uma pessoa ou instituição específica responsável por fazer esses controles ou permitir essas operações -seguras, pois podem garantir a integridade dos dados armazenados na cadeia (transações e blocos).

Surgiu em meados de 1991, mas foi em 2008 - devido à uma grande crise financeira que a princípio atingiu os Estados Unidos e na sequência espalhou-se pelo mundo – que houve a popularização do conhecimento da tecnologia (LAGO, 2017),

mediante disseminação de um documento que circulava pela internet com o título de "*Bitcoin: A Peer-to-Peer Electronic Cash System*", com a assinatura "Satoshi Nakamoto". Esse documento trazia a ideia de criar um sistema financeiro, com métodos alternativos ao atual sistema financeiro que começou a perder credibilidade a partir da crise de 2008 (NAKAMOTO, 2008).

A definição de *Blockchain*, segundo Nakamoto (2008, p.1) é "Uma versão puramente *peer-to-peer* de dinheiro eletrônico permitiria que pagamentos on-line fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira".

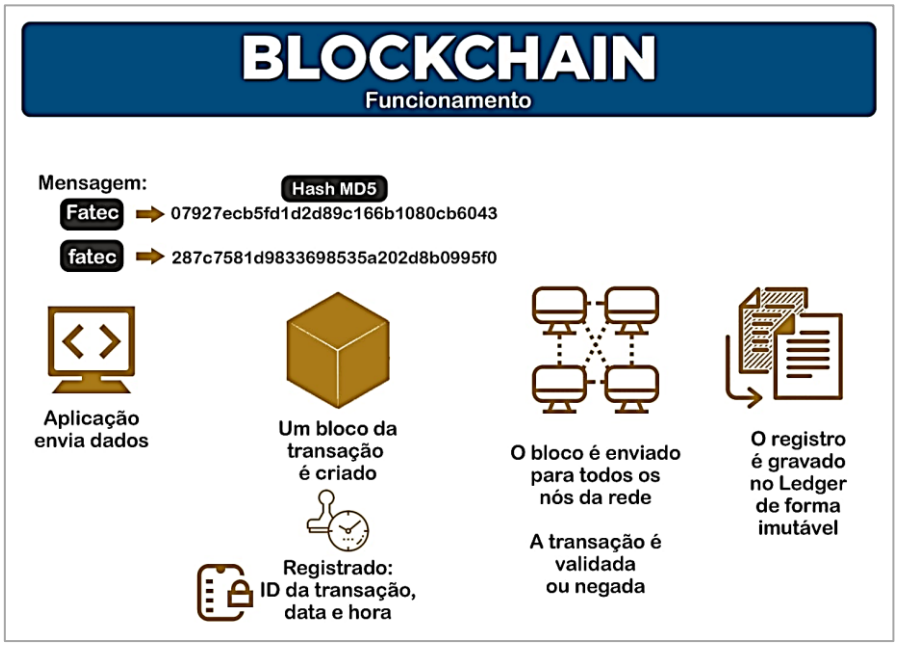
Satoshi Nakamoto é um pseudônimo, tendo em vista que até os dias atuais ainda não é possível saber quem é a real pessoa por trás dessa tecnologia que está revolucionando o mundo com extrema segurança e confiança (CERNEV & MORAES, 2021).

Hash é um algoritmo matemático utilizado na criptografia que transforma um arquivo, senha ou qualquer outra informação em um conjunto alfanumérico com comprimento fixo, que é determinado conforme o algoritmo utilizado.

Conforme De Lucena e Henriques (2018) seu objetivo é garantir a integridade e confiabilidade do dado, uma vez que a cada inclusão, exclusão ou alteração irá gerar um *hash* totalmente distinto.

O *Blockchain* utiliza funções de *hash* e assinatura digital em sua estrutura. Enquanto a função *hash* irá garantir que o dado não foi adulterado, conforme demonstrado na (**Figura 1**), onde qualquer alteração no conteúdo de um arquivo gerará um *hash* totalmente diferente, a assinatura digital autenticará a sua origem.

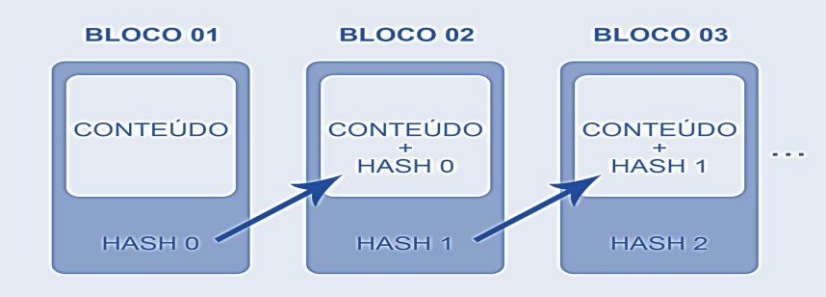
Figura 1- Funcionamento da *Blockchain.*



Fonte: Baseado em Nakamoto (2008) e Lucena & Henriques (2018).

A *Blockchain* funciona como uma rede de blocos encadeados. O bloco 1 irá gerar um *hash* do conteúdo que será transmitido (**Figura 2**), que funcionará como uma assinatura digital; o bloco 2 irá conter o *hash* anterior e mais conteúdo e partir disso um novo *hash* será gerado que será inserido do bloco 3, ocorrendo este processo reiteradas vezes a cada novo bloco (DE LUCENA & HENRIQUES, 2018).

Figura 2 - Blocos de *hash* – *Blockchain.*



Fonte: Baseado em Nakamoto (2008) e Lucena & Henriques (2018).

O sistema do *Blockchain* gera um *hash* – que é um algoritmo matemático para criptografia – para cada bloco e agrega o *hash* do bloco anterior neste novo bloco e gera um novo *hash*, interligando assim as cadeias de blocos, em ordem cronológica. O único bloco diferente é o "Bloco 0", pois é o único que não tem a informação de *hash* anterior dentro dele (LAGO, 2017).

2.2. Blockchain na Saúde

Na prática, significa que *Blockchain* pode ser aproveitado para proteger o armazenamento e transporte de informações médicas de uma pessoa, pois as informações armazenadas em uma plataforma que utiliza a tecnologia *Blockchain* só podem ser acessadas e visualizadas por pessoas que detêm a chave-pública do prontuário.

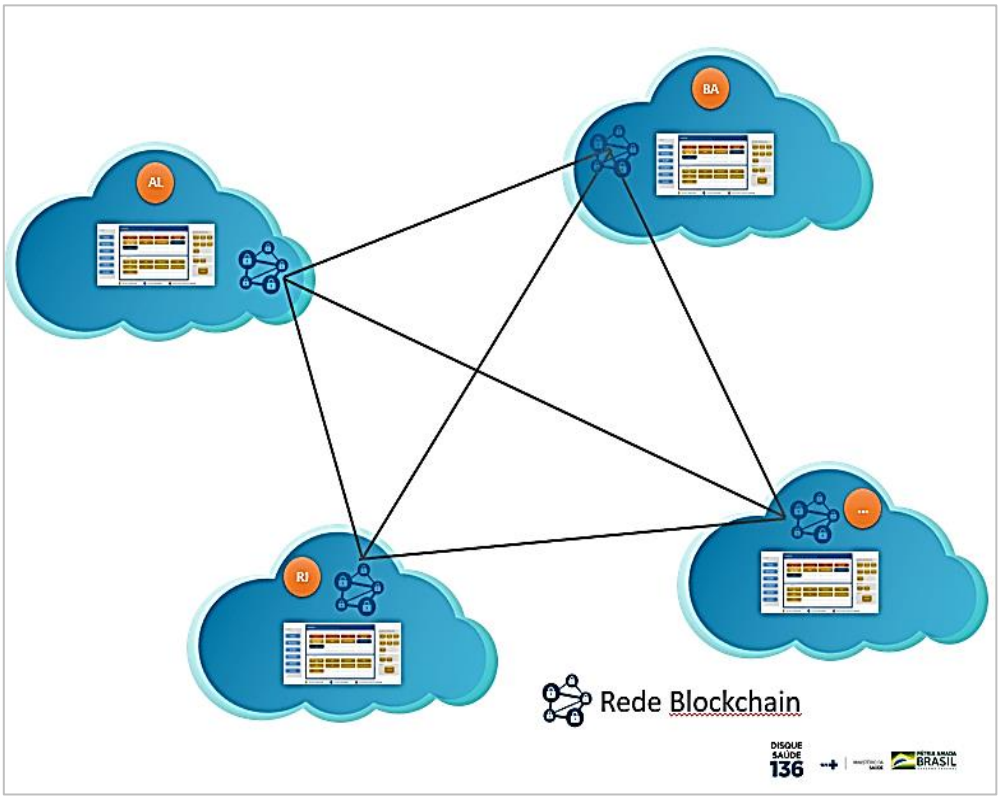
O uso de tecnologias com a finalidade de otimizar e automatizar os serviços públicos, segundo Lallana (2007), pode ajudar o País a economizar dinheiro público com gastos operacionais, por exemplo, permitindo que os cidadãos acessem com mais facilidades os serviços e seus dados médicos.

A facilidade de acesso a consultas médicas remotas beneficia pacientes com dificuldades de locomoção, permitindo atendimento em suas residências. O gerenciamento da rede e dos recursos web torna-se mais complexo devido ao aumento do tráfego de dados. Questões legais estão se expandindo para se adequar ao cenário em constante evolução.

Algumas normas são utilizadas para facilitar a gestão dos processos na área, assim como em uma empresa que utiliza o modelo ágil, por exemplo, ou está sob os preceitos da ISO 27000.

Segundo Ministério da Saúde (2019) o SUS armazena as informações de saúde dos cidadãos, por meio da Rede Nacional de Dados em Saúde (RNDS) e utiliza da tecnologia *Blockchain* por apresentar a solução mais adequada para garantir a segurança, performance, escalabilidade e acesso, além de garantir a disponibilidade do serviço (**Figura 3**).

Figura 3 - A rede *Blockchain* da RNDS.



Fonte: Ministério da Saúde (2019).

2.3. DATASUS

O Departamento de Informática do Sistema Único de Saúde (DATASUS), fundado em 1991, tem como atividade principal oferecer suporte de tecnologia aos órgãos do Sistema Único de Saúde (SUS).

Atua no desenvolvimento de sistemas para o Governo Federal, esferas Estaduais e Municipais, com servidores de dados e armazenamento com informações da população e de usuários do sistema de saúde público e privado, seja em hospital, clínica, vacina, exame ou qualquer outro procedimento no âmbito da saúde (MINISTÉRIO DA SAÚDE, 2022).

Segundo dados do Tribunal de Contas da União (Tribunal de Contas da União, 2020a), o sistema de *Blockchain* atual apresentou uma performance de até 1800 transações por segundo nos testes de prova de conceito. É uma ferramenta de gestão de interoperabilidade em saúde onde trata os dados como prontuários de pacientes, documentos clínicos e uma *timeline* do paciente na plataforma *Hyperledger Fabric*, aplicando os conceitos de *Blockchain* como Serviço (BaaS) e para isso utiliza os recursos tecnológicos da Rede Nacional de Dados em Saúde – RNDS que tem como objetivo gerenciar as informações, além de prover integridade dos dados e segurança.

São integradas diversas informações, como dados de atendimentos, exames, altas médicas, prontuários, farmácias e medicamentos, conectando a União, estados, municípios, sistema gov, Receita Federal, e sistemas de terceiros, utilizando *Blockchain* como ferramenta de segurança e atendendo os requisitos da LGPD (Tribunal de Contas da União, 2020b).

Utiliza o padrão FHIR (HL7) como recurso rápido de interoperabilidade em saúde, proporcionando troca de informações de dados. A plataforma armazena registros chamados de Conjunto Mínimo de Dados - CMD, que contém informações como resumo dos atendimentos, sumário de alta, imunização, medicamentos dispensados e exames realizados (Tribunal de Contas da União, 2020b).

2.4. Estrutura da *Blockchain* RNDS

Os dados apresentados na (

Tabela *1*), conforme verificado nas pesquisas, demonstram algumas soluções provenientes da problemática em torno da implantação da estrutura *Blockchain* no âmbito da saúde, organizando as respostas aos problemas investigados conforme o ciclo regulador de Wieringa (2009), onde é possível obter uma ideia das ações necessárias em caso de instalação de outra instância ou aplicação em diferentes áreas ou segmentos.

Tabela 1 - Estrutura *Blockchain* RNDS.

Artefato/Problema	Respostas/Soluções
Abrangência do Projeto	Federal, gerenciado pelo Ministério da Saúde.
Distribuição do banco de dados	Distribuído entre os Estados (nós da rede) Projeto piloto: Alagoas
Serviço disponível	Prontuário eletrônico dos pacientes *Timeline* dos pacientes Documentos clínicos *Smart Contracts*
Segurança	Integridade e imutabilidade dos dados
Tipo *Blockchain*	Privada. O acesso somente é permitido mediante autenticação dos usuários autorizados por *smart contracts.*
Demanda	1,2 milhões de registros / ano Capacidade: 5bi registros / ano
Plataforma	Hyperledger Fabric
Padrão de interoperabilidade	HL7 FHIR – *Fast Healthcare Interoperability Resources*. Padrão de formato de dados em linguagem de programação para troca de informações de saúde.
Data início das operações	1º semestre de 2020
Linguagem de programação	Golang
Prova de conceito	1800 transações por segundo
BaaS	*Blockchain* como serviço (BaaS). Conceito de soluções em tecnologia de serviços e infraestrutura em nuvem para desenvolvimento, implantação e hospedagem de aplicações baseadas em *Blockchain*.

Fonte: Baseado em Tribunal de Contas da União (2020a).

3. Metodologia

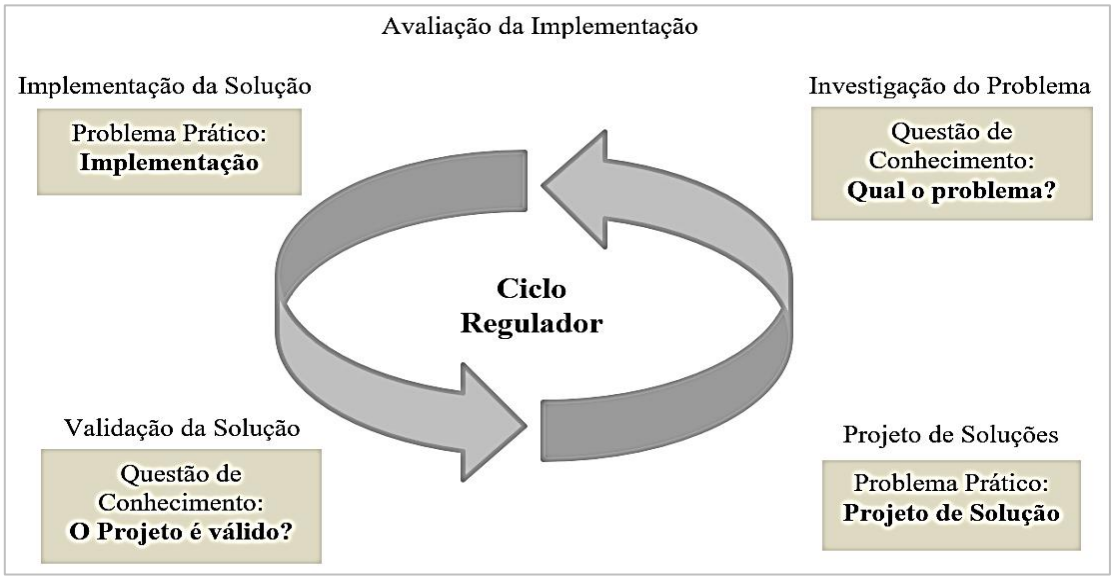
Em meados da década de sessenta surgiu o termo *Design Science*. Fuller (1965) e Gregory (1966), foram os primeiros autores a utilizá-la e concordavam que era necessário ter uma forma mais organizada e sistemática para projetar e melhorar artefatos, e a partir disso a pesquisa baseada em *Design Science Research* surgiu.

A metodologia Design Science Research (DSR), de acordo com Dresch et al. (2015), envolve a construção, investigação, validação e análise de artefatos e sistemas para resolver problemas práticos de forma prática. Simon (1996) define artefato como uma interface entre o ambiente interno e externo de um sistema. Wieringa (2009) afirma que a DSR busca soluções para problemas práticos e de conhecimento. Problemas práticos visam melhorar o mundo e atender aos objetivos dos tomadores de decisão, enquanto problemas de conhecimento buscam adquirir informações. Ambos os tipos de problemas coexistem na DSR, mas exigem abordagens e métodos diferentes para suas soluções.

Na *Design Science Research* um problema prático é o guia da pesquisa, e partir deste problema outros surgirão, inclusive de conhecimento. Este encadeamento é o que Wieringa (2009) chama de "Ciclo Regulador" demonstrado na (**Figura 4**) que é composto pelas seguintes etapas:

a. **Investigação do problema:** (*problem investigation*), conforme a figura, note que é uma "Questão de Conhecimento", sendo fortemente pautada pela teoria, como forma de buscar informações para entender o problema, sem ainda pretender e ter condições de mudá-lo;
b. **Projeto de Soluções:** (*solution design*), é parte do enfrentamento e elaboração do projeto com as possíveis soluções para o problema;
c. **Validação da Solução:** (*design validation*), é quando o pesquisador avalia os potenciais resultados caso o projeto seja bem-sucedido, e pautada na construção de conhecimento também. Eventuais ajustes do projeto podem ocorrer nesta fase;
d. **Implementação da Solução:** (*solution implementation*), esta fase é totalmente prática, que é quando o projeto será posto em uso.
e. **Avaliação da Implementação:** (*implementation evaluation),* como o nome já indica, nesta fase o pesquisador irá avaliar o resultado da implementação e estes dados irão gerar mais conhecimento científico a respeito do objeto/questão de problema.

Figura 4 - Ciclo Regulador.



Fonte: Baseado em Wieringa (2009).

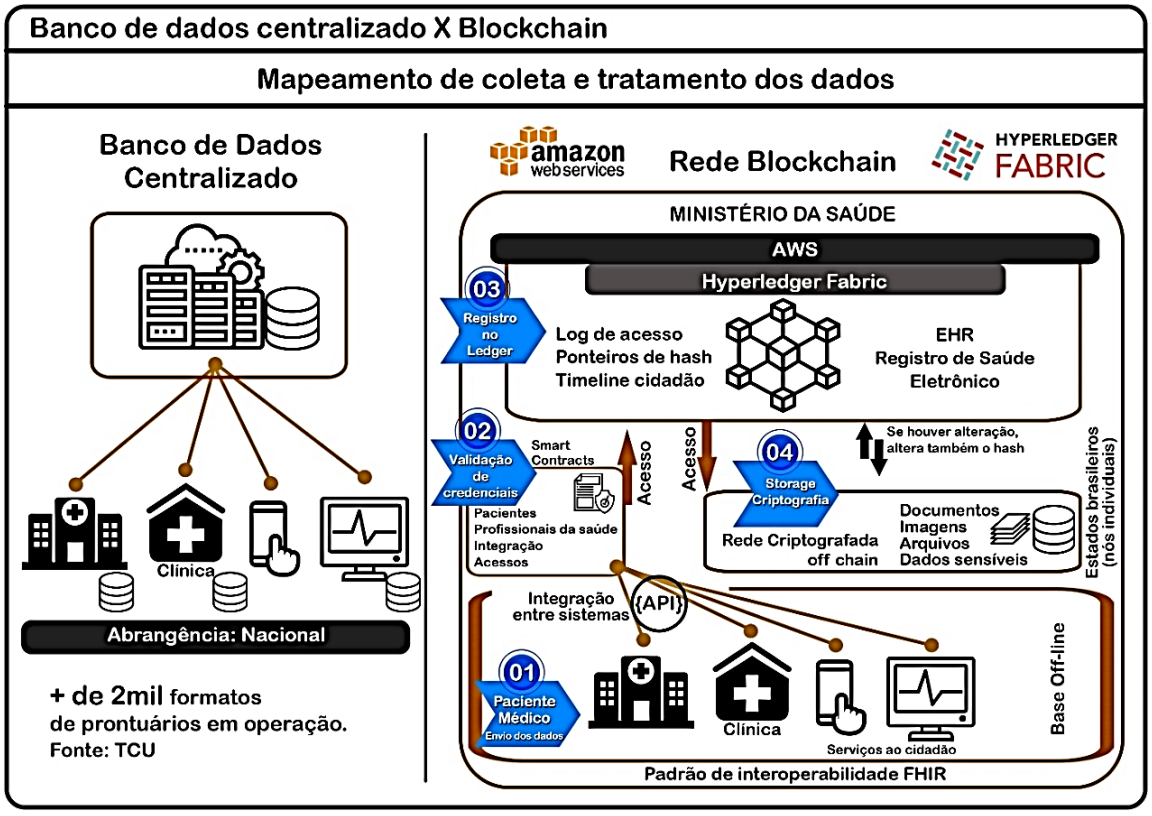
Diante do exposto e baseados em Wieringa (2009), podemos afirmar que a metodologia de *Design Science Research* é composta por cinco etapas que compreendem: pesquisa, implementação, avaliação e elaboração de propostas de solução para problemas práticos, a partir de um design bem definido, mas que pode ser mutável ao longo do processo, a fim de se adequar às necessidades que forem surgindo.

4. Análise e interpretação dos resultados

Para a análise e interpretação dos resultados o processo de instalação contribui para o entendimento do ecossistema envolvido no estudo.

Para implantação do sistema de interoperabilidade operando com a estrutura do *Blockchain* foi utilizada a plataforma da Amazon Cloud (AWS), a partir da criação de uma conta para testes e validação do processo, com uma amostragem de menor amplitude em relação à modelagem do sistema da RNDS. Com base nas informações, foi gerado um mapeamento dos processos (**Figura 5**) do ciclo de alimentação dos dados em saúde no âmbito nacional, apresentando também questões sobre os requisitos prévios para início e viabilidade do projeto, evitando transtornos durante a execução.

Figura 5 - Mapeamento da rede *Blockchain* na saúde.



Fonte: Baseado em TCU (2020).

O modelo de armazenamento centralizado (**Figura 5**) não proporciona integração entre as aplicações, pois o sistema de saúde atual possui mais de 2 (dois) mil formatos de prontuários médicos em operação, não permitindo implementar o histórico de consultas dos pacientes. Assim, a confiabilidade dos dados apresenta vulnerabilidades, pois as informações podem ser alteradas ou excluídas das bases de dados descentralizadas.

A implantação de um sistema de interoperabilidade em saúde, utilizando como ferramenta o *Blockchain* em nuvem (**Figura 5**), apresenta robustez no processo de validação de credenciais e imutabilidade dos dados. As informações são alimentadas ou consultadas na aplicação (passo 1), onde são validadas as devidas permissões no *Smart Contract*, e caso seja autorizado (passo 2), a transação é registrada de forma irreversível na rede *Blockchain* (passo 3). Os resumos das transações são armazenados na *Blockchain*, e os arquivos em uma base *off chain* criptografada de cada Estado brasileiro, de acordo com o local da consulta ou inserção (passo 4). Toda operação é registrada na rede, e em caso de tentativa de alteração indevida nos dados, o sistema faz a verificação do *hash* gerado no processo original e identifica como fraude, bloqueando a transação ilegal.

4.1. Etapas de Implementação

Antes da implantação é fundamental realizar o levantamento dos requisitos técnicos e operacionais necessários para garantir a estruturação adequada, assim como analisar a viabilidade econômica do uso da tecnologia. Algumas questões são apresentadas na (**Tabela 2**), bem como seus respectivos resultados, baseado na metodologia de Wieringa (2009), contendo ainda as soluções que serão utilizadas na implementação que será efetuada pelos autores.

Tabela 2 - Requisitos para implantação de uma *Blockchain*.

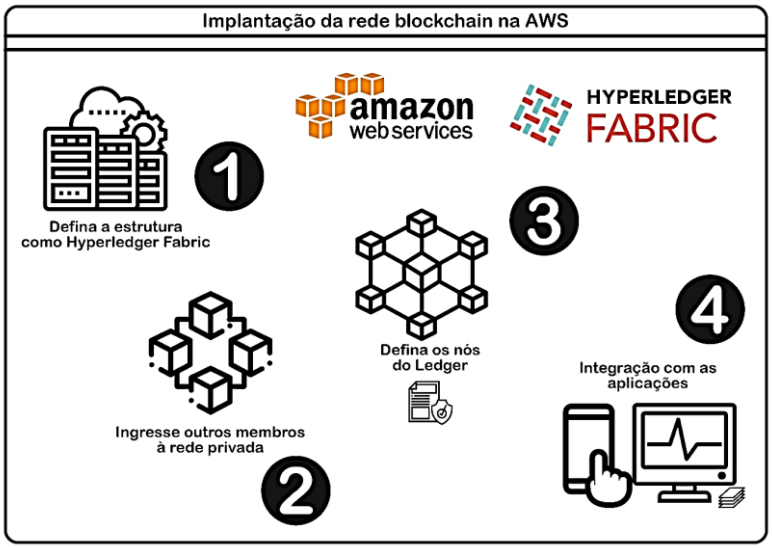
Questão/Problema	Resposta/Solução
Como proteger os dados sensíveis dos usuários do DATASUS?	A partir de bases de dados criptografadas distribuídas entre os Estados brasileiros, acessadas somente mediante validação no *Smart Contract*, onde cada operação gera um *hash* armazenado na *Blockchain*. Assim as informações não podem ser alteradas, nem acessadas indevidamente.
Como atender o titular que não quer ceder acesso aos dados?	A rede *Blockchain* não permite a exclusão de dados. O acesso aos dados é excluído, porém os dados permanecem na *Blockchain*. Obtêm-se respaldo jurídico para esta ação, conforme LGPD: • Art. 7 inciso VII: Para proteção da vida; dispensa consentimento do titular. • Art. 7 inciso VIII: Tutela da saúde; dispensa consentimento do titular. • Art. 11 inciso II alínea "e": Para proteção da vida; dispensa consentimento do titular. • Art. 11 inciso II alínea "f": Tutela da saúde; dispensa consentimento do titular.
Distribuição do banco de dados	Rede *Blockchain* Privada com *backup* e *restore* gerenciado pela plataforma *Amazon Cloud*
Restrições técnicas	Muitas regiões ainda utilizam somente documentos impressos. A internet não chega a todas as unidades de saúde.
Estrutura	*HyperLedger Fabric* de código aberto
Tipo de rede *Blockchain*	Privada. O acesso somente é permitido mediante autenticação dos usuários autorizados por *smart contracts*.
Segurança	Integridade, autenticidade, imutabilidade e combate à fraude. Elimina os nós que apresentam desempenho baixo ou suspeito.
Ambiente de nuvem	*Amazon Cloud* – AWS

Fonte: Baseado em TCU (2020) e Brasil (2019).

Após considerar e analisar os requisitos e outros pontos que sejam pertinentes para a finalidade do negócio e aplicação, deve-se iniciar a parametrização da rede no ambiente, e conforme vimos anteriormente, neste estudo será utilizado a *Blockchain* disponibilizada pela a AWS.

A primeira etapa caracteriza-se pela definição do tipo de infraestrutura, conforme (**Figura 6**):

Figura 6 - Etapas para implementação da *Blockchain.*



Fonte: Baseado em AWS (2022).

A plataforma possui duas opções (**Figura 7**): rede pública, utilizando a *Blockchain Ethereum* ou rede privada utilizando a *Hyperledger Fabric*:

Figura 7 – Primeira etapa: definição do tipo de infraestrutura.

Fonte: AWS (2022).

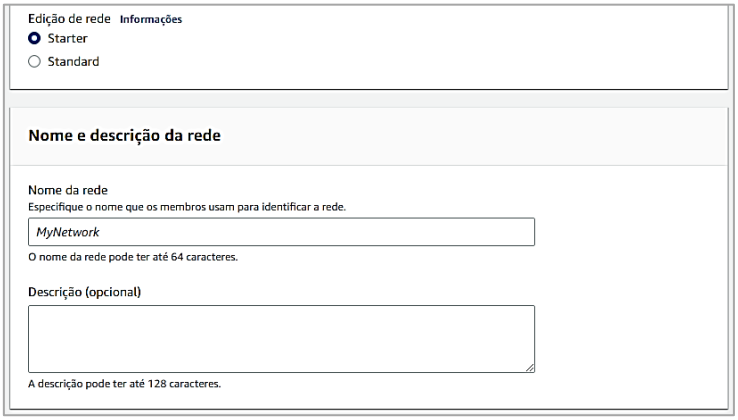
A estrutura *Hyperledger Fabric* é a mais adequada para este cenário e foi a opção escolhida (**Figura 8**), pois esta é uma estrutura de código aberto iniciada pela *Linux Foundation* em meados de 2015 e possui recursos de gerenciamento de identidade e controle de acesso (autenticação), atendendo assim a um dos pilares da segurança da informação de forma sólida e eficiente (AWS-HF, 2022).

Figura 8 - Criação da rede privada.

Fonte: Baseado em AWS-HF (2022).

O próximo passo é a escolha da versão de rede, que pode ser *starter* ou *standard*, dependendo do tipo de robustez necessária, mas para este projeto basta a *starter* (**Figura 9**), bem como definir o seu nome:

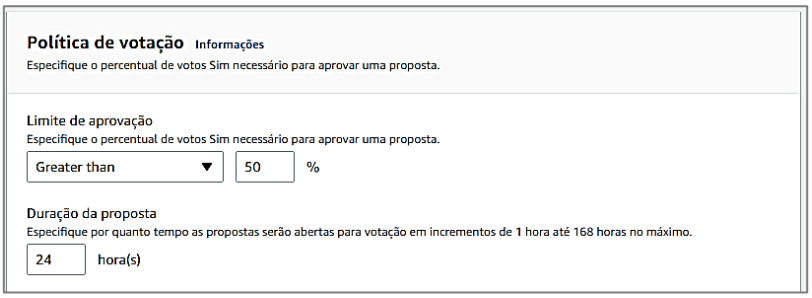
Figura 9 - Definição da rede e nome.



Fonte: Baseado em AWS-HF (2022).

As configurações de segurança são fundamentais para garantir a integridade da rede. O limite de aprovação indica os nós da rede necessários para validar uma transação, enquanto a duração da proposta pode mitigar os riscos de violação por duplo gasto (**Figura 10**).

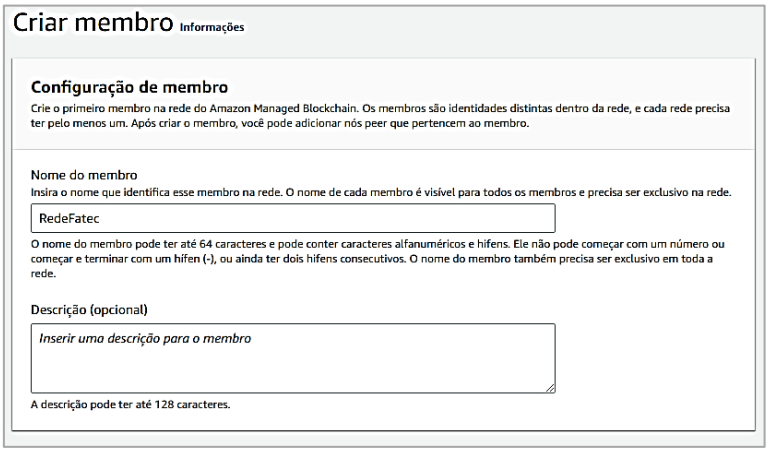
Figura 10 - Fatores de Segurança.



Fonte: Baseado em AWS-HF (2022).

A segunda etapa, conforme (**Figura 6**) é caracterizada pela inserção dos membros à sua rede privada, que deve ser exclusivo e ficará visível para todos os membros da rede, cada membro terá um usuário administrador, o comprovante de Autoridade de Certificação do *Hyperledger Fabric* é emitido.

Figura 11 - Segunda Etapa - Inclusão dos membros à rede.



Fonte: Baseado em AWS-HF,(2022).

A terceira etapa, conforme (**Figura 6**) é caracterizada pela definição dos nós, que é cada máquina ou dispositivo que estará conectado à rede.

A quarta etapa refere-se à integração com outras aplicações. Esta é uma etapa importante para garantir mais camadas de segurança para acessar à rede *Blockchain*, pois pode-se utilizar um meio de autenticação ao invés de oferecer acesso direto à rede. Para tal, pode-se utilizar uma *Application Programming Interface* (API) que fará a comunicação entre a rede privada e seus membros.

Nesta etapa optou-se por criar uma instância EC2, onde a máquina tem o Sistema Operacional Ubuntu 22.04 LTS, processador amd64 bits e 1GB de memória RAM. Ressaltando que, por se tratar de ambiente de testes as configurações são adequadas, mas em um cenário real as configurações da máquina poderão ser mais robustas, que é o mais indicado.

Outra questão que deve ser considerada é o custo de implementação e manutenção de uma rede *Blockchain*.

Por fim, após a realização das etapas indicadas, a sua rede privada *Blockchain* estará disponível para uso.

1.1. Comunicação entre os nós da rede *Blockchain* - API

A comunicação, envio e recebimento de dados entre os membros da rede *Blockchain* é realizada mediante o uso de API.

Segundo Fabro (2022) API são conjuntos de normas que permitem que componentes de diferentes plataformas estabeleçam uma comunicação entre si, por meio de uma série de protocolo, padrões e códigos.

A AWS-API (2022) informa ainda há vários tipos de API, sendo:

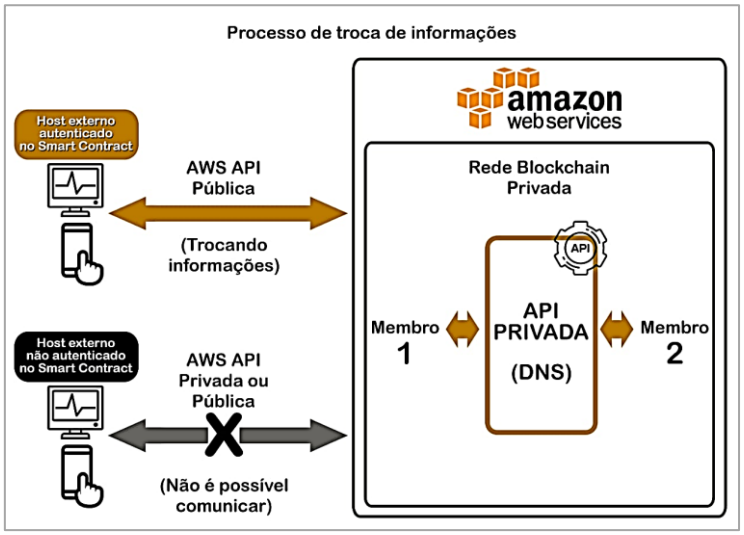
- **APIs privadas**: Como o próprio nome sugere, são de uso interno e exclusivo de uma empresa;
- **APIs públicas**: Podem ser publicadas e disponibilizadas para o público externo da empresa, e são acessíveis de qualquer host, mas podem ser utilizadas em conjunto com algum outro serviço de autenticação;

- **APIs de parceiros**: Podem ser acessadas externamente, mas apenas por desenvolvedores autorizados, geralmente quando estes precisam auxiliar empresas parceiras;
- **APIs compostas**: São utilizadas duas ou mais APIs de tipos distintos para atender às necessidades de negócio e sistema.

Para agregar maior segurança é imprescindível utilizar: uma **API pública** (**Figura 12**, lado superior esquerdo) em conjunto com *smarts contracts* válidos, respeitando quaisquer políticas de recursos que foram criadas e estão em uso para definir opções de leitura e gravação de registros; ou uma **API privada** (**Figura 12**, lado direito), mas somente para os casos onde a troca de informações ocorrerá somente dentro e entre os membros da rede *Blockchain*, pois segundo os requisitos (AWS-API, 2022) este tipo de API somente poderá ser acessada de dentro da própria rede *Blockchain.*

Observa-se ainda na **Figura 12**, há dois casos que não é possível estabelecer comunicação: API privada, mas se a tentativa de acesso for de dispositivo externo; e API Pública, quando realizada por dispositivos sem autenticação aos *smarts contracts*.

Figura 12 - Processo de troca de informações.



Fonte: Baseado em AWS-API (2022).

Ainda com relação à API privada, é possível restringir o acesso por meio do DNS, o qual pode ser público ou privado, ressaltando que o privado acrescenta outra camada de proteção à rede *Blockchain*.

No ambiente de testes não foram habilitados os serviços de DNS e API, pois demanda recurso de desenvolvimento e custo e não é este o foco do projeto. Mas todo o método é possível replicar em ambiente real, e as restrições e políticas devem ser aplicadas.

5. Resultados e Discussões

De acordo com o estudo e a análise dos resultados, alguns pontos fundamentais para serem considerados no levantamento de requisitos para implantação de *Blockchain* como ferramenta de proteção aos dados pessoais e na verificação do grau de maturidade da rede em segurança da informação são:

- Escolha do ambiente de nuvem para armazenamento dos dados, levando também em consideração custo e velocidade de transferência dos dados;
- Qual a previsão de armazenamento no banco de dados, pois isso interfere diretamente na necessidade de as informações ficarem *on chain* ou *off chain;*
- Qual banco de dados utilizar, também em função de velocidade;
- Linguagem de programação da aplicação, pois pode interferir na performance da rede;
- Se os pontos de coleta de dados possuem infraestrutura disponível para realizar as operações de envio e recebimento;
- Treinamento da equipe de colaboradores que alimentarão o sistema, e os demais que terão acesso aos dados de alguma forma, impressos por exemplo;
- Investimento necessário para implantação e manutenção, evitando do projeto ser interrompido antes de sua homologação;
- Provisionamento de instância, com máquinas que possuam configuração adequada para a finalidade.

Após pesquisas e entendimento do funcionamento da *Blockchain* do DATASUS, foi possível obter competência técnica para criar e identificar artefatos, elaborar um modelo de projeto e aplicá-lo, baseando-se no ciclo regulador de Wieringa (2009), verificando a cada etapa se os objetivos iniciais deste trabalho estavam sendo atendidos e, pode-se afirmar que sim, pois houve plena compreensão de como funciona a *Blockchain* de forma prática e, com base nesta constatação, afirma-se que as instituições que aplicarem corretamente o modelo proposto estarão em alto grau de compliance com a Lei Geral de Proteção de Dados, além de ter condições de disponibilizar um serviços de qualidade para os membros da sua rede.

Conclusões

Este estudo apresentou como a tecnologia *Blockchain* é utilizada como ferramenta de segurança da informação, com foco na área da saúde. Os avanços tecnológicos da sociedade, o surgimento de novas leis e a importância dos dados pessoais requerem um grau elevado de proteção às informações, e no caso do sistema de saúde brasileiro - DATASUS, a tecnologia escolhida foi a rede *Blockchain*. Nota-se a partir do estudo que a solução, apesar do fornecedor possuir infraestrutura escalável e robusta, ainda não está implementada a nível nacional devido às limitações das unidades de saúde, principalmente de caráter público, como por exemplo a não padronização e disponibilidade de recursos e *internet*.

De maneira geral, a tecnologia *Blockchain* apresenta um avanço na integração de proteção dos dados pessoais, porquanto provou-se ser útil em mitigar os riscos e vulnerabilidades intrínsecas às operações realizadas em meio à internet, principalmente por causa dos *hashes* gerados em cadeia de blocos interligados.

Após implementação de uma *Blockchain* real, em menor escala, no ambiente de testes disponibilizado pela AWS, constatou-se que a plataforma atende aos requisitos de segurança citados na lei LGPD, com garantias de proteção de dados e mitigação de vulnerabilidades.

Verificou-se ainda que o modelo de implementação analisado pelos autores pode ser reutilizado em outras aplicações e segmentos que necessitem atender aos termos da LGPD e garantir a integridade e disponibilidade dos seus dados.

Observou-se que a solução requer um considerável valor de investimento, com base nas pesquisas e orçamento realizados, mas que são totalmente justificáveis quando comparado ao benefício entregue.

Diante do cenário, constatou-se que o sucesso de um projeto de implementação da tecnologia *Blockchain* dependem de vários fatores, além da plataforma e estrutura em si, tais como: volumetria de dados, infraestrutura dos nós da rede (*internet*, capacidade de processamento dos computadores), banco de dados com capacidade de armazenamento total das informações *on chain*, disponibilidade orçamentária e definição adequada de quais dados são imprescindíveis para serem armazenados na *Blockchain*, uma vez que após enviado para a rede não podem ser deletados.

Como sugestões para pesquisas futuras está a ampliação dos testes, com a inclusão de mais máquinas EC2 na rede *Blockchain* e a realização de testes de intrusão e tentativa de acesso não-autorizado, a fim de validar os níveis de segurança.

Referencial Bibliográfico

AWS. (2022). *Amazon Managed Blockchain*. Recuperado de https://aws.amazon.com/pt/managed-*Blockchain*/.

AWS-API.(2022). O que é uma API?. Recuperado de https://aws.amazon.com/pt/what-is/api/#:~:text=API%20significa%20Application%20Programming%20Interface,de%20servi%C3%A7o%20entre%20duas%20aplica%C3%A7%C3%B5es.

AWS-HF. (2022). *What is Hyperledger Fabric?*. Recuperado de https://aws.amazon.com/pt/*Blockchain*/what-is-hyperledger-fabric/.

Brasil (2019) Lei nº 13.853, de 8 de julho de 2019 que Altera a Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

Camara, M. A. A., Lins, G. H. A., Oliveira, F. H. C. de, Camelo, E. M. A., & Medeiros, N. R. F. C. de. (2021). Internet das Coisas e *blockchain* no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. Cadernos Ibero-Americanos De Direito Sanitário, 10(1), pp. 93–112. Recuperado de https://doi.org/10.17566/ciads.v10i1.657

Cernev, A. K. & Moraes, T. K. L.. (2021). No rastro do *Blockchain*. Gv Executivo. 20(1), pp. 18-21.

Dresch, A; Lacerda, D. P. & Antunes Junior, J. A. V. (2015). *Design Science Research*: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: *Bookman*. Recuperado de https://www.scielo.br/j/gp/a/3CZmL4JJxLmxCv6b3pnQ8pq/?lang=pt.

Fabro, C. (2020, Junho 15). O que é API e para que serve?. Recuperado de https://www.techtudo.com.br/listas/2020/06/o-que-e-api-e-para-que-serve-cinco-perguntas-e-respostas.ghtml.

Fuller, R & Mchale, J. (1965). *World design science decade*, 1965-1975. *World Resources Inventory. Southern Illinois University.*

Gil, A. C. (2008). Métodos e técnicas de pesquisa social. 6. ed. - São Paulo: Atlas.

Gregory, S.A. (1966). *The design method. Butterworths: London*.

Lago, L.. (2017). *Blockchain*: confiança através de algoritmos. Boletim, 2(4). Recuperado de http://www.cest.poli.usp.br/wp-content/uploads/2018/08/V2N4-*Blockchain*-confian%C3%A7a-atrav%C3%A9s-de-algoritmos.pdf.

Lallana, E. C. (2007). *E-Government Interoperability: A Review of Government Interoperability Frameworks in Selected Countries*. *Bangkok, Thailand:* UNDP.

Lisboa, A. & Soares, D.. (2014). *E-Government interoperability frameworks: a worldwide inventory*. *Procedia Technology*, 16, p. 638-648. Recuperado de https://www.sciencedirect.com/science/article/pii/S2212017314002394.

Lucena, A. U. & Henriques, M. A. A.. (2018). Estudo preliminar da adoção de assinaturas baseadas em *hash* no *Blockchain* do Bitcoin. In: Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. SBC. pp. 65-72. Recuperado de https://sol.sbc.org.br/index.php/sbseg/article/view/4271/4202.

Ministério Da Saúde, Datasus. (2019, dezembro 20). Ministério da Saúde, lança a Rede Nacional de dados em Saúde e DATASUS realiza encontro técnico. Recuperado de https://datasus.saude.gov.br/ministerio-da-saude-lanca-a-rede-nacional-de-dados-em-saude-e-datasus-realiza-encontro-tecnico/.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Recuperado de https://bitcoin.org/bitcoin.pdf.

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

Rede Nacional de Dados em Saúde – RNDS. (2022). Solução Tecnológica. Recuperado de https://www.gov.br/saude/pt-br/assuntos/rnds/a-solucao-tecnologica/a-solucao-tecnologica.

Simon, H. (1996). *The sciences of artificial. Cambridge: MIT Press.*

Tribunal de Contas da União (2020a). Aplicações *Blockchain* no setor público no Brasil. Recuperado de https://portal.tcu.gov.br/data/files/58/02/CE/5E/C4854710A7AE4547E18818A8/*Blockchain*_apendice1.pdf.

Tribunal de Contas da União (2020b) Levantamento da Tecnologia *Blockchain*. Recuperado de https://portal.tcu.gov.br/data/files/59/02/40/6E/C4854710A7AE4547E18818A8/*Blockchain*_sumario_executivo.pdf.

Wieringa, R. (2009).*Design science as nested problem solving*, *Proceedings of the 4th int. conf. on design science research in information systems and technology*, ACM, p.8.