CENTRO UNIVERSITÁRIO CARIOCA - UNICARIOCA

LUCCAS PESSOA AGUIAR
VICTOR REIS FERREIRA

SISB (SISTEMAS DE INFORMAÇÃO DA SAÚDE EM BLOCKCHAIN)

RIO DE JANEIRO
2021

LUCCAS PESSOA AGUIAR
VICTOR REIS FERREIRA

SISB (SISTEMAS DE INFORMAÇÃO DA SAÚDE EM BLOCKCHAIN)

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Carioca, como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Fabio Henrique Silva

RIO DE JANEIRO
2021

A668d Aguiar, Luccas Pessoa
SISB - Sistemas de informação de saúde em Blockchain / Luccas Pessoa Aguiar e Victor Reis Ferreira.- Rio de Janeiro, 2021.
49 f.

Orientador: Fábio Henrique Silva
Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro Universitário UniCarioca - Rio de Janeiro, 2021.

1. Aplicativo, Saúde, Blockchain.. I. Ferreira, Victor Reis. II. Silva, Fábio Henrique prof. orient. III. Titulo.

CDD 005

LUCCAS PESSOA AGUIAR
VICTOR REIS FERREIRA

SISB (SISTEMAS DE INFORMAÇÃO DA SAÚDE EM BLOCKCHAIN)

Trabalho de conclusão de curso apresentado ao Centro Universitário Carioca, como requisito do grau de Bacharel em Ciência da Computação.

Rio de Janeiro, 14 de Junho de 2021.

Banca Examinadora

_____

Prof. Fabio Henrique Silva, M.Sc. - Orientador
Centro Universitário Carioca

_____

Prof. André Luiz Avelino Sobral, M.Sc. - Coordenador
Centro Universitário Carioca

_____

Prof. Lincoln Faria da Silva, D.Sc. - Convidado
Centro Universitário Carioca

“É fazendo que se aprende a fazer aquilo que se deve aprender a fazer”
Aristóteles

AGRADECIMENTOS

Primeiramente, agradecemos a Deus por abençoar nossas vidas, por ter nos guiados por toda a nossa existência, por ser o apoio e a força nesses momentos de dificuldade e fraqueza.

Também agradecendo à nossas famílias, por serem as principais motivadoras dos nossos sonhos, por acreditarem e confiarem nas nossas ideias, pelos conselhos, valores e princípios que eles infundiram em nós.

Agradecemos aos professores do Centro Universitário Carioca - Unicarioca, por compartilharem seus conhecimentos durante todo o nosso curso, de maneira especial, ao professor Fábio Henrique Silva, orientador do nosso projeto que nos guiou com seu conhecimento, permitindo a elaboração deste trabalho.

RESUMO

O objetivo para este trabalho é implementar uma ferramenta que permite a troca eficiente e segura de informações médicas entre setores hospitalares e hospitais de uma mesma rede, possibilitando que seja possível agrupar dados confidencias, assegurar a confiabilidade das informações, transparências nos processos internos da Rede. Portanto, este trabalho propõe a implementação de um sistema que utiliza BlockChain como base, integração com uma base de dados administrada pelo MongoDB, disponibilizando de maneira segura, ordenada e concisa das informações. Tal ferramenta pretende minimizar os riscos operacionais dentro do sistema de saúde, simplificando a comunicação de dados dentro da rede.

Palavras-chave: BlockChain, MongoDB, Rede e Segurança.

ABSTRACT

The goal for this work is to implement a tool that enables the efficient exchange and secure medical information between hospital departments and hospitals of the same network, allowing it to be possible to group confidential data, ensure the reliability of information, transparency in the internal processes of the network. Therefore, this work proposes the implementation of a system that uses BlockChain as a base, integration with a database administered by MongoDB, providing a secure, orderly and concise information. This tool aims to minimize operational risks within the health system, simplifying data communication within the network.

Keyword: BlockChain, MongoDB, Network and Security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

P2P – Peer-to-Peer
TTP – Third Trusted Party
HIPAA – Health insurance portability and accountability act
ERP – Enterprise Resource Planning
JS – Javascript
NPM – Node Package Manager
RSA – Rivest-Shamir-Adleman
SHA256 – Secure Hash Algorithm
POW – Proof of Work
MD5 – Message-Digest Algorithm
ODM – Object Data Modeling
SI – Sistema de Informação
NAFTA – North American Free Trade Agreement (Tratado Norte-Americano de Livre-Comércio)
CAFTA – Central America Free Trade Agreement and Dominican Republic (Tratado de Livre-Comércio entre Estados Unidos, América Central e República Dominicana)
UE – União Europeia
AUSFTA – Australia–United States Free Trade Agreement (Tratado de Livre-Comércio entre Estados Unidos e Australia)
KORUS-FTA – United States–Korea Free Trade Agreement (Tratado de Livre-Comércio entre Estados Unidos e Coréia)
LGPD – Lei Geral de Proteção de Dados
SP – São Paulo
ANPD – Autoridade Nacional de Proteção de Dados
ACM – Association for Computing Machinery (Associação para Maquinas de Computação)
HMAC – Keyed-Hash Message Authentication Code
TLS – Transport Layer Security
HTTPS – Hyper Text Transfer Protocol Secure
EUA – Estados Unidos da América
CDC – (Centro de Controle e Prevenção)

TI – Tecnologia da Informação

RME – Registros médicos eletrônico

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais, a informação é considerada o principal ativo da sociedade moderna. Ter os dados corretos em um certo momento pode representar a diferença entre lucro e prejuízo, entre a decisão correta e a errada e entre o sucesso e fracasso. Portanto a segurança computacional tornou-se a grande preocupação das empresas, motivado pelo aumento significativo nas ocorrências de ciberataques, os criminosos cibernéticos estão evoluindo de maneira exponencial. Porém, essa importância com relação a informações não é uma consequência da evolução dos computadores, antes esta foi se consolidando ao longo dos anos (PLANEZ, 2015).

Por exemplo, a Informação na Saúde se inicia com Hipócrates (460-350 a.C.) que registrava suas observações em relação aos sinais e sintomas durante uma análise do paciente, pois acreditava que tais doenças não eram algo sobrenatural, mas sim a inter-relação do ser humano em seu meio ambiente (FRANCO, 2015). Com a evolução da sociedade, os sistemas de informações também evoluem, além das mudanças tecnológicas, os conceitos e métodos para armazenar, tratar e disseminar informações para que seja utilizada da melhor maneira possível por diferentes públicos (gestores, acadêmicos e sociedade em geral) têm se desenvolvido rapidamente.

Segundo uma publicação no blog Certisign (2018), no contexto comercial, existe a necessidade de permitir transações de informações utilizando métodos criptográficos modernos. Com o surgimento do Certificado Digital Eletrônico, que possibilita o envio de informações criptografadas, permitindo que usuários troquem dados de maneira segura. A Figura 1, apresenta um exemplo do uso de um modelo criptográfico para o envio de um texto.

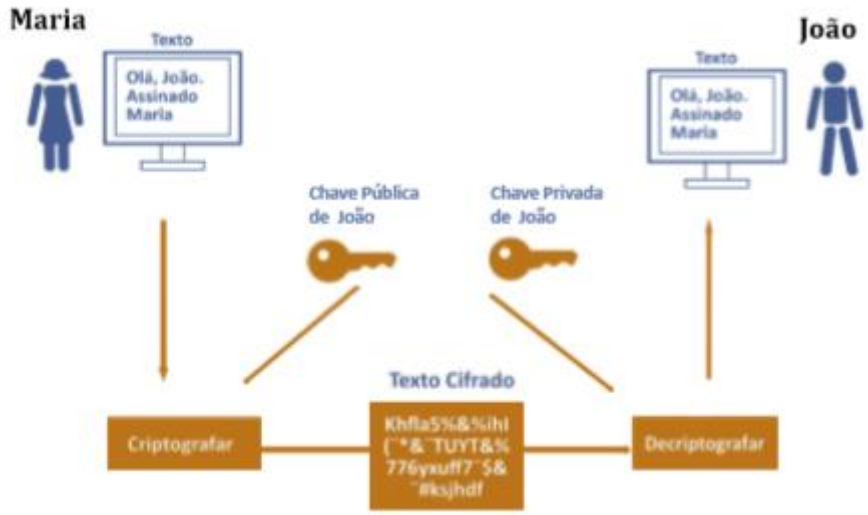

Figura 1: Como a criptografia funciona no Certificado Digital? Fonte: Blog Certisign (2018)

1.1 Motivação e justificativa

A motivação para a realização deste trabalho, surgiu ao identificarmos a necessidade e dificuldade que as empresas de saúde devem enfrentar sempre que é preciso buscar informações históricas de um paciente, de maneira segura e estável. Tendo em vista a baixa disponibilidade de recursos físicos e computacionais, os horários específicos do plantão médico e o quesito de linearidade no histórico do paciente, entre outros.

A maneira de organizar tais informações de forma, que represente um quadro evolutivo, é o início para o processo de diagnóstico e tratamento de um paciente. Qualquer atividade a ser realizada pelo mesmo, por quesitos ou necessidades médicas, deve ser registrada e adicionada à base de dados, possibilitando que outros usuários (laboratórios, médicos, enfermeiros e etc.) que venham a ter contato com o paciente, possam fazer seu trabalho de maneira íntegra.

1.2 Objetivos

O objetivo deste trabalho é desenvolver uma ferramenta, mediante ao uso de conceitos de programação e sistemas de informações operacionais, para que seja possível transitar informações de maneira segura e eficiente entre setores

hospitalares ou até mesmo entre hospitais de uma mesma rede. Sendo possível agrupar os dados confidenciais, garantir a confiabilidade das informações e transparência nos processos internos.

Para alcançar tal objetivo, é proposto uma ferramenta que utiliza o BlockChain como base para a transação dos dados, fazendo o registro do envio de dados e armazenando as informações de maneira ordenada em blocos. Para que sejam analisados posteriormente pelos médicos e enfermeiros.

Basicamente a aplicação, vai administrar as transações de informações, usando a criptografia como ferramenta para garantir a segurança dos dados que serão transitados dentro da rede.

1.3 Metodologia

Identificando os principais requisitos e necessidades que os médicos e enfermeiros enfrentam ao buscar e administrar as informações de múltiplos pacientes no hospital, tendo em vista os seus respectivos, históricos pessoais e familiares, identificaram-se as principais funcionalidades a serem cumpridas pela aplicação proposta.

As principais funcionalidades são:

- Custos operacionais e curva de aprendizado dos usuários;
- Garantir a segurança das transações dos dados;
- Permitir a visualização da linearidade dos pacientes;

Para atender a tais necessidades básicas, decidimos trabalhar com a ferramenta Node.js que permite escrever programas com JavaScript que serão compilados e interpretados. Possibilitando criarmos uma aplicação End-to-End utilizando a mesma linguagem de programação.

Essa ferramenta é extremamente leve e multiplataforma, permitindo que seja possível rodar em servidores abertos e em qualquer Sistema Operacional, diminuindo bastante seu custo de hardware (em comparação com um programa em Java) e software (licenças de servidores).

1.4 Organização do Trabalho

Este trabalho está organizado da seguinte forma:

O Capítulo 2 introduz os principais conceitos sobre Sistemas de Informação Operacionais, Sistemas de Gerência de Informações, segurança em rede de computadores e segurança da informação. O foco principal deste capítulo é apresentar uma fundamentação teórica dos principais conceitos desenvolvidos neste trabalho.

O Capítulo 3 descreve o desenvolvimento da ferramenta proposta no trabalho, apresenta os principais desafios na construção do software, as etapas da construção, os conceitos importantes sobre o funcionamento e métodos utilizados na implementação.

O Capítulo 4 trata o teste da aplicação, considerando um ambiente estável e múltiplas ocorrências de rotinas do dia-a-dia em uma rede hospitalar. Apresentando uma breve análise do funcionamento da aplicação e avaliação dos resultados obtidos.

Finalmente, o Capítulo 5 descreve as conclusões alcançadas, indicações de possíveis pontos de evolução de escalabilidade e aperfeiçoamento da aplicação proposta.

2 FUNDAMENTAÇÃO TEÓRICA.

Neste capítulo serão apresentados os fundamentos teóricos utilizados, pois tais tópicos são necessários para o entendimento do problema e da solução proposta.

Os seguintes tópicos têm como propósito embasar a pesquisa, usando como fundamento alguns conceitos referentes a Sistemas de Informação, BlockChain e Criptografia.

2.1 Sistemas de Informação

Sistema de Informação é um conjunto de componentes inter-relacionados que coletam, manipulam, armazenam, e disseminam dados e informações, e fornecem um mecanismo de feedback para atender um objetivo (STAIR; REYNOLDS, 2009).

A Figura 2 apresenta os componentes principais de um Sistema de Informação.

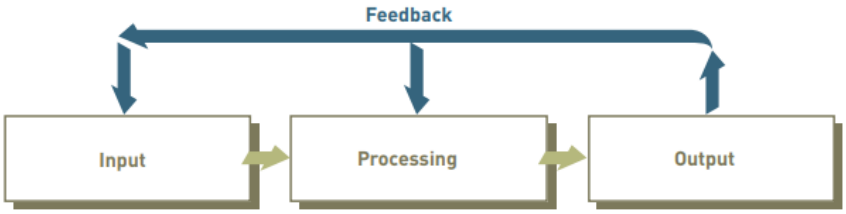

Figura 2: Os componentes de um sistema de informações. Fonte: STAIR; REYNOLDS (2009)

Os componentes principais são: entradas (inputs) [1], processamento (processing) [2], saídas (output) [3] e Feedback [4].

1. A entrada para um Sistema de Informação é a atividade de colheita e captura de dados não tratados. Por exemplo, o processo de produção de contracheques, o número de horas que os colaboradores trabalham devem ser coletados antes do cálculo e da emissão dos contracheques (STAIR; REYNOLDS, 2011).

2. O processamento significa converter e transformar as informações em resultados úteis. Esse processo envolve a realização de cálculos, comparação de dados e tomada de ações alternativas, e armazenamento das informações para que sejam usadas futuramente. O processamento de dados em informações úteis é crítico para as configurações de negócios. O processo pode ser realizado manualmente ou com assistência de um computador. Uma aplicação de folha de pagamento, o número de horas trabalhadas por cada colaborador deve ser convertido em um valor líquido (STAIR; REYNOLDS, 2011).

3. Segundo (STAIR; REYNOLDS, 2011), a saída envolve a produção de informações úteis, normalmente em forma de documentos e relatórios. Para Taylor (1894), o objetivo e direção de um output são básicos, pois estabelecem o contexto de acompanhamento para um cliente individual, para uma classe de usuários ou para uma organização. A saída de informação tem direção, ou seja, ela é enviada ou usada, ora por alguém, ora por um grupo. Possui um propósito. Isto é a intenção daqueles que iniciam e transmitem a saída é ter um efeito sobre algum ato futuro, decisão ou mudança.

4. O feedback é a informação sobre a lacuna entre o nível real e o nível de referência de um parâmetro do sistema que é usado para alterar a lacuna de alguma forma. Por exemplo, informações sobre gastos excessivos com viagens realizadas por um vendedor, usadas para cortar seus gastos no futuro são feedback (RAMAPRASAD, 1983).

O desenvolvimento de sistemas de informações para atender às necessidades de negócios é altamente complexo e difícil, tanto que é comum que os projetos de SI ultrapassem os orçamentos e excedam datas de conclusão programadas. Uma estratégia para melhorar os resultados de um projeto de desenvolvimento de sistemas é dividi-lo em várias etapas, cada uma com um objetivo bem definido e um conjunto de tarefas para realizar (STAIR; REYNOLDS, 2009). Essas etapas são resumidas a seguir (Consulte a figura 3):

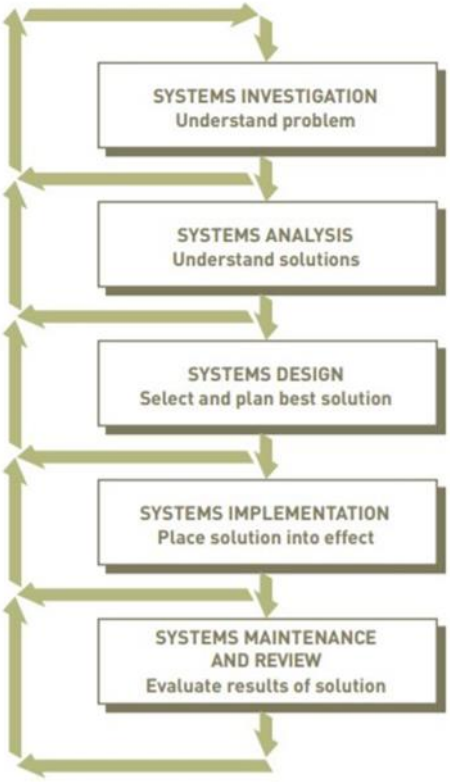

Figura 3: As etapas de um desenvolvimento de sistema de informações. Fonte: Stair; Reynolds (2009)

Stair e Reynolds (2009) estabelece que as duas primeiras etapas do desenvolvimento, são investigação e análise de sistemas. O objetivo da investigação de sistemas é obter uma compreensão clara do problema a ser resolvido ou oportunidade de ser abordada. Depois que entende o problema, a próxima pergunta é: "Vale a pena resolver o problema?" Dado que os recursos são limitados: pessoas e dinheiro. Se a decisão é continuar, a próxima etapa e a análise de sistemas, define os problemas e oportunidades de sistema existente. Durante a investigação e análise de sistemas, bem como a manutenção e revisão do projeto, discutido a seguir, o projeto deve ter o suporte completo dos gerentes de nível superior e foco no desenvolvimento de sistemas que atinjam os objetivos de negócios.

Para Stair e Reynolds (2009) o design de sistemas determina como o novo sistema funcionará para atender às necessidades de negócios definidas durante a análise de sistemas. A implementação de sistemas envolve a criação ou aquisição de vários componentes do sistema (hardware, software, bancos de dados, etc.) definidos na etapa de design, montá-los e colocar o novo sistema em operação. O objetivo da

manutenção e revisão de sistemas é verificar e modificar o sistema para que continue a atender às mudanças necessidades de negócios.

Segundo (STAIR; REYNOLDS, 2009), os sistemas de informação de hoje levaram a uma maior globalização. Porém, introduz vários obstáculos e problemas, incluindo desafios envolvendo cultura, idioma e muitos outros.

- **Desafios culturais** – Países e áreas regionais têm suas próprias culturas e costumes que podem afetar significativamente os indivíduos e organizações envolvidas no comércio global (STAIR; REYNOLDS, 2009).

- **Desafios de linguagem** – Diferenças de idioma podem dificultar a tradução exata significados de uma língua para outra (STAIR; REYNOLDS, 2009).

- **Desafios de tempo e distância** – Problemas de tempo e distância podem ser difíceis de superar para indivíduos e organizações envolvidos com o comércio global em locais remotos. Muito tempo as diferenças tornam difícil falar com as pessoas do outro lado do mundo. Com longa distância, pode levar dias para obter um produto, uma peça crítica ou um equipamento de um local para outro local (STAIR; REYNOLDS, 2009).

- **Desafios de infraestrutura** – Eletricidade e água de alta qualidade podem não estar disponíveis em certas partes do mundo. Serviços telefônicos, conexões de Internet e profissionais os funcionários podem ser caros ou não estar prontamente disponíveis (STAIR; REYNOLDS, 2009).

- **Desafios de moeda** – O valor de diferentes moedas pode variar significativamente ao longo do tempo, tornando o comércio internacional mais difícil e complexo (STAIR; REYNOLDS, 2009).

- **Desafios de produtos e serviços** – Produtos tradicionais físicos ou tangíveis, como um automóvel ou bicicleta, pode ser difícil de entregar ao mercado global. Contudo, produtos eletrônicos (e-products) e serviços eletrônicos (e-services) podem ser entregues a clientes eletronicamente,

por telefone, por meio de redes, por meio da Internet ou por outros meios eletrônicos. Software, música, livros, manuais e conselhos podem ser entregues globalmente e pela Internet (STAIR; REYNOLDS, 2009).

- **Problemas de transferência de tecnologia** – A maioria dos governos não permite certos assuntos militares equipamentos e sistemas a serem vendidos para alguns países. Mesmo assim, alguns acreditam que empresas estrangeiras estão roubando propriedade intelectual, segredos comerciais e materiais protegidos por direitos autorais e falsificação de produtos e serviços (STAIR; REYNOLDS, 2009).

- **Leis estaduais, regionais e nacionais** – Cada estado, região e país tem um conjunto de leis que deve ser obedecido pelos cidadãos e organizações que operam no país. Essas leis podem lidar com uma variedade de questões, incluindo segredos comerciais, patentes, direitos autorais, proteção de dados pessoais ou financeiros, privacidade e muito mais. Leis que restringem como os dados entram ou as saídas de um país são frequentemente chamadas de leis de fluxo de dados transfronteiriças. Acompanhar essas leis e incorporando-os aos procedimentos e sistemas informáticos de multinacionais e organizações transnacionais podem ser muito difíceis e demoradas, exigindo especialistas aconselhamento jurídico (STAIR; REYNOLDS, 2009).

- **Acordos comerciais** – Os países frequentemente celebram acordos comerciais entre si. O Tratado Norte-Americano de Livre-Comércio (NAFTA) e o Tratado de Livre-Comércio entre Estados Unidos, América Central e República Dominicana (CAFTA) são exemplos. A União Europeia (UE) é outro exemplo de um grupo de países com um acordo de comércio internacional. A UE é uma coleção, principalmente, de países europeus que se uniram para a paz e a prosperidade. Acordos comerciais adicionais incluem o Tratado de Livre-Comércio entre Estados Unidos e Australia (AUSFTA), sancionada em 2005, e o Tratado de Livre-Comércio entre Estados Unidos e Coréia (KORUS-FTA), assinado em lei em 2007. Acordos

> de livre comércio também foram estabelecidos entre Bolívia e México, Canadá e Costa Rica, Canadá e Israel, Chile e Coréia, México e Japão, Estados Unidos e Jordânia e muitos outros (STAIR; REYNOLDS, 2009).

Recentemente, no Brasil, foi aprovada a LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, a chamada Lei Geral de Proteção de Dados (LGPD) que vem para atualizar as diretrizes do Marco Civil da Internet, aprovado em 2014. Segundo uma publicação da FECOMERCIO SP (2020), a Lei, editada em agosto de 2018, estava prevista para entrar em vigor em 16 de agosto de 2020. No entanto, devido ao cenário de crise gerado pela pandemia, algumas iniciativas legislativas e do Poder Executivo surgiram visando a prorrogação da lei, as sanções administrativas da LGPD passam a valer em 1º de agosto de 2021. A mudança na data da imposição de sanções no âmbito da LGPD tem o objetivo de não onerar as empresas, que já enfrentam enormes dificuldades técnicas e econômicas por causa da pandemia.

O objetivo da nova lei é tornar mais rigorosa a proteção de nossos dados pessoais em quaisquer canais (físicos ou digitais), afetando setores importantes como o da saúde. Na prática, as novas medidas colocam em xeque a prática de comercialização e/ou uso de informações pessoais sem o consentimento do consumidor. Além disso, passa a existir a ANPD (Autoridade Nacional de Proteção de Dados), órgão responsável por fiscalizar as empresas quanto ao cumprimento da lei de proteção e privacidade de dados (ALMEIDA, 2019).

Para Almeida (2019), a LGPD impactará diretamente o setor de saúde, uma vez que paciente passa a ter direito sobre os dados fornecidos às instituições de saúde. Atualmente, o uso do blockchain na saúde aparece como grande aliado de gestores e profissionais da área, percebendo a importância dessa tecnologia e os benefícios para o setor, o mercado de healthtech não ficou alheio às vantagens de inserir o blockchain no setor de saúde e algumas empresas já oferecem soluções a partir de sistemas de armazenamento de dados, onde médicos podem manter seu portfólio profissional e acadêmico, ou para que hospitais manejem dados de pacientes e da equipe de colaboradores com total segurança.

2.2 O que é BlockChain?

Blockchain pode ser definido como um livro-razão digital resistente à violação, implementadas em um sistema distribuído e geralmente sem uma autoridade central (ou seja, um banco, empresa ou governo). Em seu nível mais básico, eles permitem que uma comunidade de usuários registre transações em um livro-razão compartilhado dentro desse agrupamento, de modo que sob a operação normal da rede blockchain, nenhuma transação pode ser alterada depois de publicada. Em 2008, a ideia do blockchain foi combinado com várias outras tecnologias e conceitos de computação para criar criptomoedas: dinheiro eletrônico protegido por mecanismos criptográficos em vez de um repositório central ou autoridade (YAGA; MELL; ROBY; SCARFONE, 2018). Veja a diferença de uma estrutura centralizada e não centralizada na figura 4.

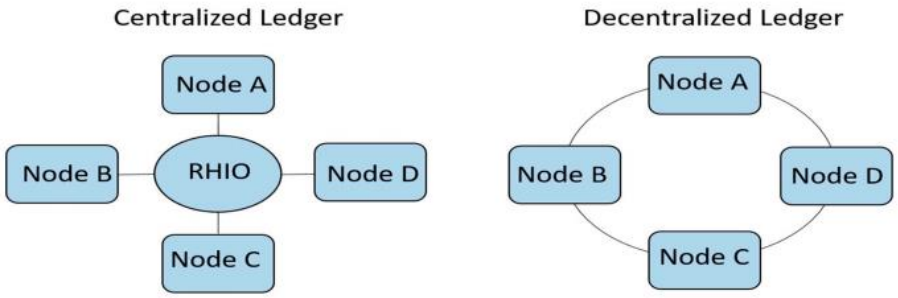

Figura 4: Exemplo de uma estrutura centralizada e de uma estrutura não centralizada. Fonte: Agbo; Mahmoud; Eklund (2019)

A principal utilidade do blockchain é a possibilidade de efetuar transações entre participantes de uma rede distribuída, sem a necessidade de uma entidade central para atual como autoridade no modelo TTP. O modelo de Sistema de confiança tripla não é considerado como desejável por conta de uma série de razões, por exemplo, mau funcionamento dos sistemas computadorizados, falhas ou comprometimento de dados causados por eventos maliciosos impossibilitando a ação de processamento de transações financeiras. Outros quesitos levados em consideração para a crítica do modelo TTP, seriam o excesso de taxas nas transações e o próprio das transações por conta da análise (AGBO; MAHMOUND; EKLUND, 2019).

Após o lançamento do famigerado artigo Bitcoin: A Peer to Peer Electronic Cash System, publicado pelo pseudônimo Satoshi Nakamoto, foi possível implementar com

sucesso a criptomoeda Bitcoin. Em sua pesquisa, Nakamoto (2008), define a Bitcoin como uma versão de dinheiro eletrônico que faz uso de uma rede P2P, sem a necessidade do uso de um sistema de confiança tripla para averiguar a ocorrência de gastos duplos. Sua proposta consiste da utilização de registros de marca temporal nas transações, criptografando-as em uma cadeia contínua baseado no modelo de proof-of-work, a longa corrente de dados não só serve como prova da sequência dos eventos testemunhados, como também a prova de que existe um grande poder computacional por trás desses registros.

De acordo com Swan (2015), a primeira geração de criptomoedas baseadas em blockchain, como a Bitcoin, Dash e LiteCoin constituem a primeira geração da tecnologia blockchain, que também é conhecido como blockchain 1.0.

A segunda geração da tecnologia blockchain, referenciada como blockchain 2.0, está relacionado a contratos, que englobam toda a economia, mercado de finanças e aplicações financeiras, como exemplo: ações, debêntures, empréstimos, títulos, propriedades inteligentes e contratos inteligentes (SWAN, 2015).

No blockchain 3.0, são aplicações blockchain que vão além de moedas, finanças e mercado, particularmente usada em áreas governamentais, de saúde, ciência, artes e etc (SWAN, 2015).

2.2.1 História do Blockchain

O primórdio das principais ideias que constituem o blockchain surgiram no final dos anos 80s e no começo dos anos 90s. Em 1989, Leslie Lamport desenvolveu o protocolo Paxos e em 1990 enviou o artigo The Part Time Part-Time Parliament para a revista ACM Transactions on Computer Systems. Segundo (LAMPORT,1998), é descrito como um modelo de consenso que possui como finalidade, chegar a um acordo levando em consideração os resultados encontrados em uma rede de computadores, onde os computadores ou até mesmo a própria rede podem não ser confiáveis. Tais conceitos foram combinados e aplicados no desenvolvimento de um sistema de dinheiro eletrônico em 2009, descrita previamente por Nakamoto (2008).

Existiam diversos sistemas de dinheiro eletrônico antes do Bitcoin (por exemplo, ecash e NetCash), mas nenhum deles conseguiu alcançar o uso generalizado. A utilização do blockchain permitiu ao Bitcoin que fosse implementado

de forma distribuída, sem que nenhum usuário controlasse o dinheiro eletrônico e nenhum ponto único de falha existia, com isso foi possível promover seu uso. Seu principal benefício era permitir transações diretas entre usuários sem a necessidade de um TTP. Também possibilitou a emissão de novas criptomoedas de maneira definida para aqueles usuários que conseguem publicar novos blocos e mantém cópias do livro-razão, esses usuários são chamados de mineiros no Bitcoin. O pagamento automatizado definido aos mineiros garante uma administração distribuída do sistema sem a necessidade de uma organização para controle. Com o uso do blockchain e uma manutenção baseada em consenso, foi criado um mecanismo de autopoliciamento, que garantiu que apenas transações e blocos válidos sejam adicionados ao blockchain (YAGA; MELL; ROBY; SCARFONE, 2018).

2.3 Componentes básicos de um blockchain

A tecnologia blockchain pode parecer complexa, no entanto, é possível criar uma visão simplificada se examinarmos cada componente individualmente.

2.3.1 Crypto

No blog do Node.js, o módulo crypto é um pacote de funções criptográficas para OpenSSL. Ele suporta cálculos de hashes, autenticação com HMAC, cifras e entre outros. O módulo crypto é principalmente útil como uma ferramenta para implementar protocolos criptográficos, como TLS e HTTPS. Para a maioria dos usuários, o módulo TLS integrado e o módulo HTTPS devem ser mais do que suficientes.

O blog do Node.js continua dizendo que os hashes que funcionam com crypto, dependem, de qual versão do OpenSSL está usando e se ela suporta. Se você tiver uma versão nova o suficiente do OpenSSL, poderá obter uma lista de tipos de hash que seu OpenSSL suporta digitando na sua linha de comando: – *openssl list-message-digest-algorithms* – Um dos algoritmos de hash mais comuns é o SHA-256. Tipos populares mais antigos, como SHA-1 ou MD5, não são mais seguros e não devem ser usados. A figura 5 é um exemplo de entrada e saída de texto em SHA-256.

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Figura 5: Exemplo de entradas de texto e suas respectivas saídas em SHA-256. Fonte: Yaga; Mell; Roby; Scarfone (2018)

2.3.2 Funções de Hash Criptográficas

Segundo (YAGA; MELL; ROBY; SCARFONE, 2018), um importante componente da tecnologia blockchain é o uso de funções hash criptográficas em diversas operações. Hashing é um método que aplica uma função de hash criptográfica aos dados, que calcula uma saída relativamente única (conhecida como resumo de mensagem ou apenas resumo) para uma entrada de quase qualquer tamanho (por exemplo, um arquivo, texto ou imagem). Permite que os indivíduos capturem dados de entrada de forma independente, hashing esses dados e obter o mesmo resultado, provando que não houve alteração nos dados.

As principais propriedades de segurança das funções de hash criptográficas:

- **Determinismo** – Significa que independentemente de quantas vezes uma determinada entrada seja convertida através de uma função hash, sempre alcançara o mesmo resultado (ROSIC, 2020).

- **Função Unidirecional (Pre-image Resistance)** – Isso significa que é computacionalmente inviável calcular o valor de uma entrada dado algum valor de saída (ROSIC, 2020).

- **Resistencia a colisão** – Significa que duas entradas de dados aleatórias e distintas não podem obter o mesmo valor de saída. Cada entrada terá seu próprio hash único.

2.3.3 Blocos

Os usuários da rede Blockchain enviam transações candidatas à rede blockchain via software (aplicativos de desktop, aplicativos de smartphones, carteiras digitais, serviço da Web, etc.). O software envia essas transações para um nó ou nós dentro da rede blockchain, os nós escolhidos podem ser nós completos de não publicação, bem como nós de publicação. Em seguida, as transações são propagadas para os outros nós da rede, mas isso por si só não coloca a transação no blockchain. Para muitas implementações dessa tecnologia, uma vez que uma transação pendente foi distribuída aos nós, ela deve então esperar em uma fila até que seja adicionado ao blockchain por um nó de publicação (YAGA; MELL; ROBY; SCARFONE, 2018).

As transações são adicionadas ao blockchain quando um nó de publicação disponibiliza um novo bloco. Um bloco contém um cabeçalho e os dados desses respectivos blocos. O cabeçalho contém os metadados para este bloco, já os dados do bloco contêm uma lista de transações validadas e autenticas que foram enviadas para a rede blockchain. A validade e autenticidade são garantidas ao verificar se a transação está formatada corretamente e que os fornecedores de ativos digitais em cada transação (listados nos valores de entrada da transação) tem cada transação assinada de maneira criptografada (YAGA; MELL; ROBY; SCARFONE, 2018). Abaixo, na figura 6, um exemplo de um bloco.

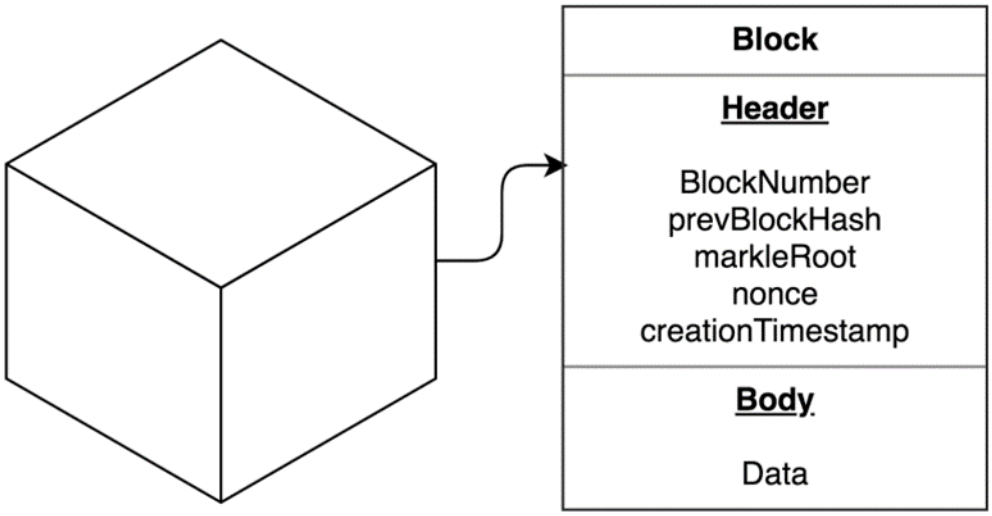

Figura 6: Exemplo de um Bloco. Fonte: Castro (2018)

2.4 Árvore de Merkle

Segundo Antonopoulos (2017), uma árvore de Merkle, também conhecida como árvore de dispersão, é uma estrutura de dados usada para resumir e verificar a integridade de grandes conjuntos de dados. Árvores de Merkle são árvores binárias contendo hashes criptográficos. O termo "árvore" é usado na ciência da computação para descrever uma estrutura de dados ramificada, mas essas árvores geralmente são exibidas de cabeça para baixo com a "raiz" no topo e as "folhas" na parte inferior de um diagrama.

Árvores de Merkle são usadas em bitcoin para resumir todas as transações em um bloco, produzindo uma impressão digital geral de todo o conjunto de transações, proporcionando um processo muito eficiente para verificar se uma transação está incluída em um bloco. Resumindo, cada bloco no blockchain da bitcoin contém um resumo de todas as transações no bloco, usando uma árvore de Merkle (ANTONOPOULOS, 2017). Consulte a figura 7 para um exemplo de árvore de Merkle.

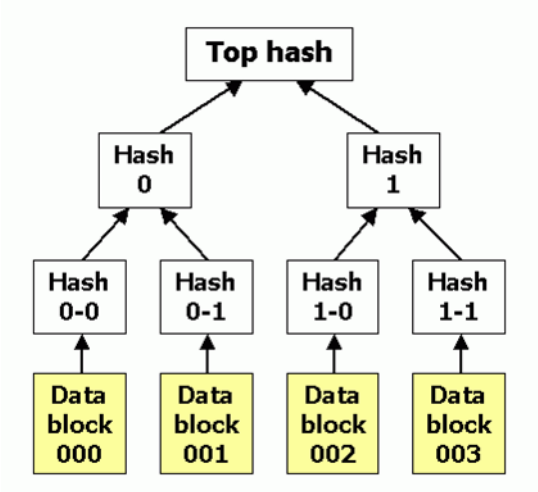

Figura 7: Exemplo de uma árvore de Merkle. Fonte: Wikipédia

A adoção da árvore de Merkle realiza o requisito de escalabilidade e, o mais importante, melhora a eficiência para validar a integridade dos dados. A árvore de Merkle é uma estrutura de árvore binária onde a entrada é uma lista de registros de dados com hash. Esses registros são ordenados no momento em que são gerados. A cada dois registros são agrupados e os hashes dos dois registros de dados tornam-se dois nós de folha da árvore de Merkle e, consequentemente, constituem um nó de

grupo de alto nível com o grupo de hash gerado pela concatenação de dois hashes. Dois nós de grupo seguirão o mesmo caminho para gerar um novo nó de grupo de nível superior com um novo hash. Esta etapa é repetida até que haja um único hash que irá tornar-se a raiz da árvore, ou seja, a raiz de Merkle (LIANG, X.; ZHAO, J.; SHETTY, S.; LIU, J.; & LI, D., 2017).

3 UMA APLICAÇÃO PARA ENVIO DE INFORMAÇÕES MÉDICAS BASEADA EM BLOCKCHAIN

Neste capítulo, será apresentado a descrição da problemática, as justificativas sobre o uso de determinadas ferramentas usadas.

3.1 Problemáticas na área da saúde

O aumento da expectativa de vida da população mundial tem trazido alguns desafios para área da saúde, tais como condições de saúde crônicas e mais complexas. Na medida em que a população envelhece e a demanda por melhores condições de vida continua a aumentar, os custos com a saúde crescem substancialmente (DE NEGRI, 2020).

Um dos maiores problemas na indústria médica é a segurança dos dados e informações. De acordo com estudos realizados pela HIPAA Journal (2021), durante 2009 e 2020, foram reportados nos Estados Unidos, 3.705 violações de dados de saúde, conforme demonstrado na tabela 1 logo abaixo. Essas violações resultaram na perde, roubo, exposição ou divulgação inadmissível de 268.189.693 registros de saúde.

Ano	Prestador de Saúde	Plano de Saúde	Associado de Negócios	Câmara de compensação de Saúde	Total
2009	14	1	3	0	18
2010	134	21	44	0	199
2011	134	19	45	1	199

2012	155	23	40	1	219
2013	191	20	64	2	277
2014	196	41	77	0	314
2015	195	61	14	0	270
2016	256	51	22	0	329
2017	285	52	21	0	358
2018	273	53	42	0	368
2019	398	59	53	2	512
2020	497	70	73	2	642
Total	2,728	471	498	8	3,705

Tabela 1: Violações por tipo de entidade na saúde. Fonte: HIPPA Journal (2020)

De acordo com a pesquisa realizada pela empresa de segurança Comparitech, Bischoff (2021) explica que ataques virtuais a organizações, hospitais e clinicas, custaram em torno de 20 bilhões de dólares. Esse custo surgi por conta do tempo de inatividade causado pelos ataques cibernéticos, os servidores podem ficar offline por horas, semanas ou até mesmo meses. Abaixo, na figura 8, um gráfico de incidentes e cyber-ataques na área de TI.

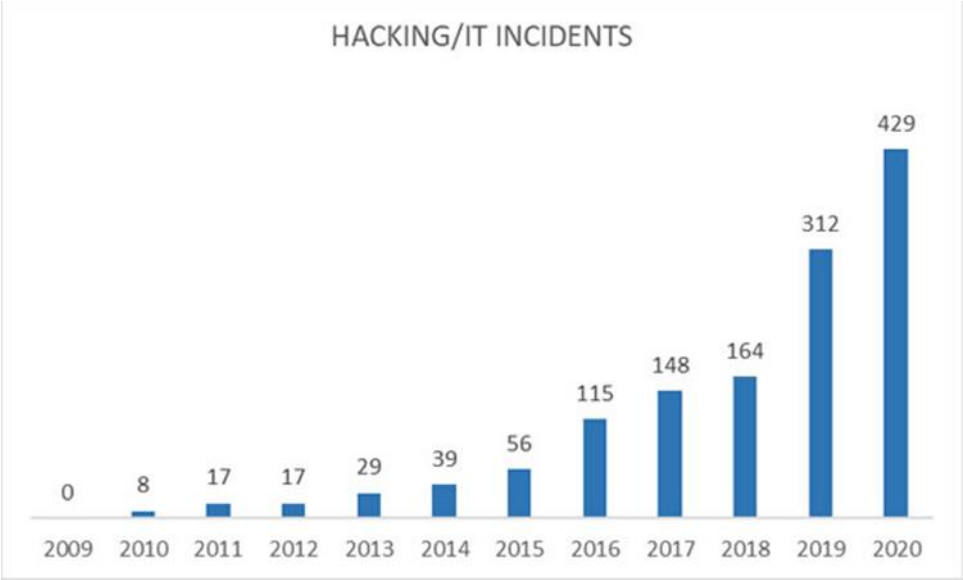

Figura 8: Gráfico de incidentes na área de TI e cyber-ataques. Fonte: HIPPA Journal (2020)

Segundo De Negri (2020), as tecnologias da informação representam uma alternativa promissora para a redução dos custos, para a melhoria dos serviços de saúde e a ampliação do acesso. Muitos gastos com a saúde são ineficientes, provinda da falta de informação e da repetição de exames desnecessários. O acesso total do paciente e a possibilidade do compartilhamento de seus registros médicos com os profissionais de sua confiança tem um enorme potencial de reduzir esses custos.

Outro problema crucial para De Negri (2020), é a relação entre acesso à informação e privacidade, consequente da utilização massiva de registros médicos de pacientes, seja para pesquisa, prescrições de tratamentos e procedimentos. Um desafio adicional, especialmente no caso dos países em desenvolvimento, é a infraestrutura para a coleta e o armazenamento de informações. O Sistema Único de Saúde (SUS), por exemplo, é o maior sistema público de saúde do mundo, e, por isso, uma fonte gigantesca de informações sobre saúde. No entanto, a implementação de prontuários eletrônicos esbarra em coisas simples, como a disponibilidade de infraestrutura básica na ponta: computadores, sistemas e acesso à banda larga.

3.2 Justificativas do uso do Blockchain

Segundo Almeida (2019), a capacidade de proteger um grande número de dados é um dos principais benefícios de utilizar o blockchain na saúde. Além disso, por possuir uma natureza descentralizada e transparente, essa tecnologia também possibilita o compartilhamento das informações entre profissionais de saúde e pacientes de forma rápida e segura. Abaixo, na tabela 2 demonstra os benefícios de uma aplicação blockchain para o setor de saúde.

Descentralização	A própria natureza dos sistemas de saúde, na qual existem partes interessadas distribuídas, requer um sistema de gestão descentralizado. O *blockchain* pode se tornar um aliado a saúde descentralizada, sendo responsável pelo gerenciamento de dados de onde todas as partes interessadas podem ter acesso controlado aos mesmos registros médicos, sem que ninguém desempenhe o papel de autoridade central sobre os dados globais de saúde.

Disponibilidade / Robustez	Uma vez que os registros no *blockchain* são replicados em vários nós, a disponibilidade dos dados armazenados no *blockchain* são garantidos, pois o sistema é robusto e resiliente contra perdas de dados, corrupção de arquivos e contra ataques de segurança à disponibilidade de dados.
Segurança de dados aprimorada e privacidade	A propriedade de imutabilidade do *blockchain* melhora exponencialmente a segurança dos dados armazenados nele, tendo em vista que os dados, uma vez salvos nos blocos, não podem ser corrompidos, alterados ou recuperados. Todos os dados de saúde no *blockchain* são criptografados, com registro de data e hora e anexados em ordem cronológica. Além disso, os dados de saúde são salvos no *blockchain* usando chaves criptográficas que ajudam a proteger a identidade ou a privacidade dos pacientes.
Posse dos dados de saúde	Os pacientes precisam ser os proprietários de seus dados e controlar como eles deveram ser usados. É necessário garantir que os seus dados não sejam usados indevidamente por outras partes interessadas e devem possuir meios de detectar quando tal uso indevido ocorre. A tecnologia do *Blockchain* ajuda a atender a esses requisitos por meio dos protocolos criptográficos fortes e contratos inteligentes bem definidos.
Transparência e confiança	Por conta de sua natureza aberta e transparente, cria uma atmosfera de confiança em torno de aplicativos de saúde distribuídos. Isso facilita a aceitação de tais aplicações pelas partes interessadas em saúde.
Verificabilidade de dados	Mesmo sem acessar o texto simples dos registros armazenados no *blockchain,* a integridade e a validade desses registros podem ser verificadas. Este recurso é muito útil em áreas de cuidados de saúde onde a verificação de registros é uma exigência, como suprimentos farmacêuticos gestão da cadeia e processamentos de reclamações de seguros.

Tabela 2: Benefícios de uma aplicação blockchain para saúde. Fonte: Elaborado pelos autores

Para Almeida (2019), a partir disso, é possível criar um histórico completo de informações do paciente, que pode ser acessado em situações futuras para realizar diagnósticos mais precisos e até mesmo antecipar o tratamento com base nos registros previamente fornecidos. E apesar da possibilidade de gerenciamento de registros privados por meio digital ser o grande motivador do interesse de médicos e gestores de hospitais e clínicas, existem outras contribuições do blockchain para o setor de saúde, como:

- **Registros médicos eletrônico (RME)** – Almeida (2019) definido como a centralização de informações clinicas de pacientes e de que prestou o atendimento. Para Agbo, Mahmound e Eklund (2019), facilita o compartilhamento de dados centrados no paciente entre diferentes sistemas de saúde e partes interessadas, como fornecedores, pesquisadores e seguradoras. Consistente com a Lei Geral de Proteção de Dados (LGPD) que proíbe o processamento de dados pessoais confidenciais de pacientes, a menos que o consentimento explícito seja dado pelos pacientes, o blockchain é amplamente proposto como uma tecnologia viável para construir a plataforma de saúde que pode capacitar os pacientes a controlar como os seus dados são compartilhados, processados ou usados.

- **Rastreabilidade e controle de suprimentos** – permite o controle e a rastreabilidade de suprimentos hospitalares e farmacêuticos, à medida que armazena dados cronologicamente em uma rede ponto a ponto. Essa capacidade torna a tecnologia adequada para resolver questões relacionadas à rastreabilidade de medicamentos e a redução de problemas relacionados com o fornecimento de remédios falsificados (ALMEIDA, 2019).

- **Controle e prevenção** – ao formar uma espécie de “trilha” de informações, os cientistas podem determinar onde e com quais padrões uma doença se originou para então eliminá-la. Por exemplo, nos EUA, o Centro de Controle e Prevenção (CDC) estão utilizando o blockchain na saúde para monitorar doenças e possíveis epidemias de modo semelhante ao que é feito na cadeia de suprimentos, devido aos recursos de processamento de dados e registros de data e hora do sistema (ALMEIDA, 2019).

- **Pesquisa Biomédica e Educação** – armazenamento e compartilhamento de dados sobre pesquisas e ensaios clínicos. A ideia de que a troca de experiências e informações entre médicos de todo o mundo pode criar um Big Data global com estudos de doenças, formas de diagnóstico e tipos de

tratamento. Compartilhar informação de forma descentralizada sobre as doenças mais comuns em cada região do mundo, os medicamentos mais utilizados e acessíveis, o controle de estoque do material necessário para tratamentos. Tudo isso, pode transitar com máxima segurança através do blockchain (ALMEIDA, 2019).

Um recurso importante do blockchain que é claramente benéfico para aplicativos de saúde é a descentralização, que torna possível implementar aplicativos de saúde distribuídos que não dependem de uma autoridade centralizada. Além disso, o fato de que as informações no blockchain são replicadas entre todos os nós da rede, criando uma atmosfera de transparência e abertura, permitindo as partes interessadas na saúde, e em particular os pacientes, para saber como seus dados são usados, por quem é utilizado, quando e como (AGBO; MAHMOUND; EKLUND, 2019).

A propriedade de imutabilidade do blockchain que torna impossível alterar ou modificar qualquer registro que esteja anexado ao blockchain, se alinha muito bem com os requisitos para armazenamento de registros de saúde. Além disso, o uso de algoritmos criptográficos para criptografar os dados armazenados no blockchain, garante que apenas os usuários com permissões legítimas possam acessar e descriptografar os dados, melhorando assim a segurança e privacidade dos dados (AGBO; MAHMOUND; EKLUND, 2019). Abaixo, a figura 9 exemplifica uma aplicação básica de blockchain na saúde.

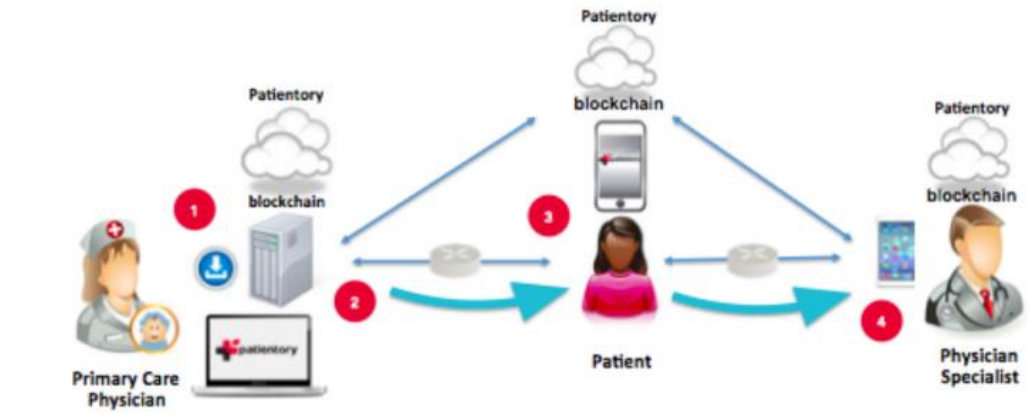

Figura 9: Exemplo básico de uma aplicação blockchain na saúde. Fonte: Fórum Saúde Digital (2018)

4 APRESENTAÇÃO DA PROPOSTA

Durante esse capitulo será apresentado a implementação do protótipo da solução, com o objetivo de descrever o passo-a-passo da construção e uma apresentação de um caso de teste, onde emulamos equipes médicas enviando resultados de exames para pacientes. Será apresentando as ferramentas utilizadas para implementação do protótipo e suas peculiaridades.

Segundo os fundamentos previamente apresentados, desenvolvemos um protótipo de um sistema de envio de informações médicas através do protocolo Blockchain, que faz uso dos benefícios citados e estingue os problemas principais encontrados nos mais populares Sistemas de Informações para saúde (ERP's).

4.1 Ferramentas utilizadas na implementação

Na tabela 3, será apresenta as tecnologias e ferramentas utilizadas no desenvolvimento.

Ferramentas	**Versão Utilizada**	**Referência**
JavaScript	ECMA Script 5	https://www.javascript.com/
TypeScript	4.2.4	https://www.typescriptlang.org/
Node,js	14.17.0	https://nodejs.dev/
NPM	6.14.13	https://www.npmjs.com/
Visual Studio Code	1.56.2	https://code.visualstudio.com/
MongoDB	4.4	https://www.mongodb.com/

Tabela 3: Principais ferramentas utilizadas no desenvolvimento. Fonte: (Elaborado pelos autores)

A implementação foi iniciada através do desenvolvimento de classes utilizando conceitos de Orientação a Objetos com a linguagem de programação JavaScript. Por conta da escolha da linguagem JS, fizemos uso do ambiente Node.js que possibilita a implementação de uma aplicação back-end.

No documento disponibilizado na web pelo Mozilla, JavaScript é uma linguagem leve, interpretável e orientada a objetos, baseada em protótipos, multi-paradigma e dinâmica, suportando estilos de orientação a objeto, imperativos e declarativos.

Para complementar o desenvolvimento e interpretação do código, foi utilizado também a linguagem TypeScript, que, segundo a publicação feita pelo Node.js é basicamente um super conjunto de JavaScript, onde são adicionados novos recursos. A adição mais notável são as definições de tipo estático, algo que não está presente no JS simples. Graças às declarações de tipos, é possível, por exemplo, declarar que tipo de argumentos estamos esperando e o que é retornado exatamente em nossas funções ou qual é a forma exata do objeto que estamos criando.

O Node.js é definido em seu site sendo um ambiente de execução JavaScript de código aberto e plataforma cruzada. Executa o mecanismo V8 JavaScript, o núcleo Google Chrome, fora do navegador. O principal motivo da adoção a essa aplicação é devido a sua alta capacidade de criar aplicações escaláveis. Dentre as suas vantagens são sua arquitetura simples, baixo custo e flexibilidade. A figura 10 mostra a estrutura de uma aplicação moderna.

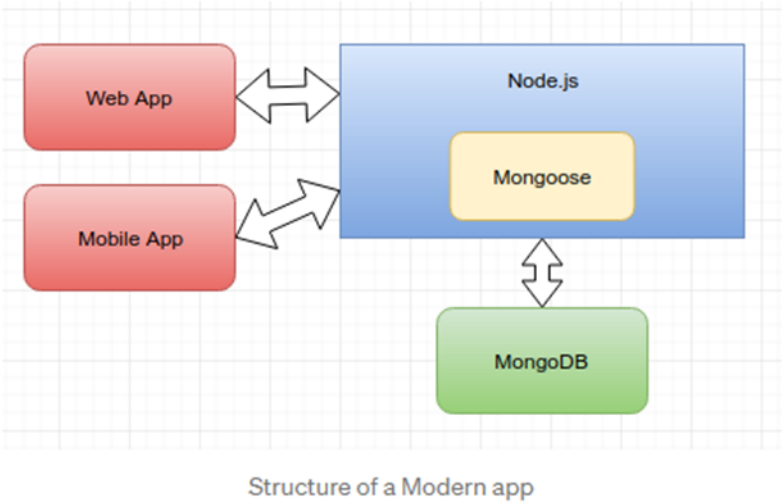

Figura 10: Estrutura de um App Moderno. Fonte: Bits and Pieces (2018)

Outra ferramenta utilizada no projeto de desenvolvimento foi o NPM (Node Package Manager) é um gerenciador de pacote do Node,js. No site do Node.js, o NPM é duas coisas, em primeiro lugar, é um repositório online para publicação de projetos Node.js. A segunda funcionalidade, é um utilitário de linha de comando para interagir

com o referido repositório que ajuda na instalação do pacote, gerenciamento de versão e gerenciamento de dependência. Uma inifinidade de bibliotecas e aplicativos Node.js são publicados no NPM.

A última ferramenta é o MongoDB, que se define em seu site como um sistema de gerenciamento de banco de dados não relacional de código aberto que usa documentos flexíveis em vez de tabelas e linhas para processar e armazenar várias formas de dados.

4.2 Implementação do protocolo Blockchain

A implementação do blockchain foi dividida em algumas classes, onde cada uma é um respectivo ponto essencial para o funcionamento do protótipo, com seus próprios requisitos e funcionalidades.

4.2.1 Classe Wallet

A primeira classe implementada para a realização do protocolo Blockchain, foi a classe Wallet (classe que simula uma carteira de um usuário), que é local onde um usuário guarda sua chave pública e chave privada.

- **Chave Pública:** É uma chave única que permite que o detentor da carteira possa receber documentos, informações e resultados médicos.

- **Chave Privada:** É uma chave única que permite que o detentor da carteira possa transferir dados para outro usuário da rede.

```
class Wallet {
    public publicKey: string;
    public privateKey: string;

    constructor() {
        const keypair = crypto.generateKeyPairSync('rsa', {
            modulusLength: 2048,
            publicKeyEncoding: { type: 'spki', format: 'pem' },
            privateKeyEncoding: { type: 'pkcs8', format: 'pem' },
        });

        this.publicKey = keypair.publicKey;
        this.privateKey = keypair.privateKey;
    }

    sendInfo(information: string, payeePublicKey: string) {
       const transaction = new Transaction(information, this.publicKey, payeePublicKey);
       const sing = crypto.createSign('SHA256');
       sing.update(transaction.toString()).end();

       const signature = sing.sign(this.privateKey);
       Chain.instance.addBlock(transaction, this.publicKey, signature);
    }

}
```

Figura 11: Classe Wallet. Fonte: Desenvolvida pelos Autores

Conforme a Figura 11 é possível visualizar especificações da criação e criptografia das chaves públicas e privadas utilizando o algoritmo RSA, quer permite encriptação e decriptação caso possua essas determinadas chaves. Usamos a chave privada para assinar a Hash da transferência e verificada futuramente pela chave pública, tal funcionalidade impediria que outra pessoa fizesse alterações no bloco, tendo em vista que seria gerado outra hash, essa alteração causaria um erro durante a verificação, impedindo que os dados sejam alterados.

4.2.2 Classe Transaction

A classe Transaction é o proposito fundamental do protocolo Blockchain, transferir informações de um usuário para outro em forma de uma transação. As transações possuem 3 propriedades.

1. **Information** – Propriedade designada para conter o endereço/caminho de um determinado arquivo, contendo informações como resultado de exames e relatórios médicos.

2. **Sender** - Usuário que faz a transferência dessa informação através do protocolo.
3. **Receiver** - Usuário que será o receptor dessa transferência.

```
class Transaction {
    constructor(
        public information: string,
        public sender: string,
        public receiver: string,
    ){}

    toString(){
        return JSON.stringify(this);
    }

}
```

Figura 12: Classe Transaction. Fonte: Desenvolvido pelos Autores.

Como demonstrado na figura 12, a classe possui um método para converter o objeto para String, para tornar os objetos criptografados mais fáceis de interagir e tratar.

4.2.3 Classe Block

É um container para a transação, ele funciona como uma lista encadeada, pois carrega a referência (hash) do bloco anterior. Agregando ao protocolo a propriedade de imutabilidade aos blocos.

Conforme a Figura 13, utilizando a função createHash() da biblioteca Crypto podemos criptografar o bloco através do algoritmo SHA256, que possui um tamanho de 256 bits. Após criptografia, essa hash é retornada como uma string em Hexadecimal.

```
class Block {

    public nonce = Math.round(Math.random() * 99999999);

    constructor(
        public prevHash: string,
        public transaction: Transaction,
        public ts = Date.now(),

    ) {}

    get hash() {
        const str = JSON.stringify(this);
        const hash = crypto.createHash('SHA256');
        hash.update(str).end();
        return hash.digest('hex');
    }
}
```

Figura 13: Classe Block. Fonte: Desenvolvido pelos Autores.

4.2.4 Classe Chain

Nessa classe, foi implementado o conceito da corrente que conecta os blocos. Para impossibilitar a criação de múltiplas instancias do blockchain, foi criado um Singleton Instance (garantindo que exista apenas uma instancias dessa classe). Como protótipo, definimos a primeiro bloco (Genesis) diretamente nessa classe.

```
class Chain {
    public static instance = new Chain();
    chain: Block[];
    constructor() {
        this.chain = [ new Block("", new Transaction('10201202201', 'genesis', 'arthur'))];
    }
    get lastBlock() {
        return this.chain[this.chain.length - 1];
    }
    mine(nonce: number) {
        let solution = 1;
        while (true) {
            const hash = crypto.createHash('MD5');
            hash.update((nonce + solution).toString()).end();
            const attempt = hash.digest('hex');
            if(attempt.substr(0,4) === '0000') {
                return solution;
            }
            solution += 1;
         }
    }
    addBlock (transaction: Transaction, senderPublicKey: string, signature: Buffer) {
        const verifier = crypto.createVerify('SHA256');
        verifier.update(transaction.toString());
        const isValid = verifier.verify(senderPublicKey, signature);
        if (isValid) {
            const newBlock = new Block(this.lastBlock.hash, transaction);
            this.mine(newBlock.nonce);
            this.chain.push(newBlock);
            let newInstance = new blockChainModel(newBlock);
            newInstance.save((err) => {
                if (err) return console.log("Erro ao salvar", err.message);
                console.log("Foi possível salvar o block no BD");
            });
        }
    }
```

Figura 14: Classe Chain**.** Fonte: Desenvolvido pelos Autores.

Conforme a Figura 14, utilizando a biblioteca Crypto para criar uma verificação de assinatura, na qual todas os dados das transações precisam passar nesse verificador, onde podemos validar que a transação não foi alterada (antes de chegar nessa etapa) usando a chave pública do usuário que envia as informações e a própria assinatura que consta na transação. Garantindo que esse usuário está ciente e deseja efetuar essa transferência.

Para impedir que um usuário faça a transferência de dados para dois usuários diferentes ao mesmo tempo, foi necessário implementar POW (Proof of Work). Portanto criamos um método chamado Mine, que recebera um número e tentará encontrar um valor que somando ao número de entrada, criara uma hash que começa com 4 zeros. Essa hash é criada usando o algoritmo MD5 com tamanho 128.

Caso o bloco seja adicionado ao Blockchain, salvamos o mesmo dentro da base da dados que foi criado no MongoDB.

4.3 Integração com o MongoDB

Após um bloco ser instanciado no blockchain é necessário salva-lo em uma base de dados linear. Com suporte da Mongoose (uma Modelagem de Dados de Objetos - ODM) é possível relacionar dados, fornecendo validação de esquemas.

No arquivo Model.js, onde é criado o Schema, cada um desses esquema é mapeado para uma coleção MongoDB e define a forma dos documentos dessa coleção.

```
"use strict";
let mongoose = require("mongoose");
let Schema = mongoose.Schema;
let BlockChainSchema = new Schema({
    ts: {
        required: true,
        type: Schema.Types.Date,
        default: Date.now()
    },
    transactions: {
        required: true,
        type: Schema.Types.String,
    },
    previousHash: {
        required: true,
        type: Schema.Types.String,
    },
    hash: {
        required: true,
        type: Schema.Types.String,
    }
});
module.exports = mongoose.model("BlockChain", BlockChainSchema);
```

Figura 15: Model.js. Fonte: Desenvolvido pelos Autores.

Conforme a figura 15, definimos como é a estrutura que será indexada ao banco de dados, o protótipo vai armazenar um bloco, utilizando o Timestamp, transação, hash do bloco anterior e a hash do próprio bloco.

O último componente da integração com o MongoDB é o arquivo Main.js, nele é especificado a conexão ao banco de dados. Com o método CallBack() o mongoose executa uma query assíncrona e depois passa a resposta de volta para o método. Na

figura 16, é possivel verificar a conexão a base a dados, pelo endereço localhost e porta 27017.

```
let mongoosedb = require("mongoose");

let BlockChainModel = requise("./model");


mongoosedb.connect("mongodb://localhost:27017/BlockChain", (err) => {
    if (err)
        return console.log("Error on the DB");
    console.log("DB connected");
    connectionCallBack();

});

let connectionCallBack = () => {};

module.exports.onConnect = (callBack) => {
    connectionCallBack = callBack;
}
```

Figura 16: Main.js. Fonte: Desenvolvida pelos Autores.

4.4 Resultados dos Testes

Aplicando um simples cenário de teste, onde um usuário fará a transferência de um arquivo para um paciente. Na Figura 17, é possível verificar as chaves públicas do usuário que envia e a do receptor e também o endereço do arquivo com as informações do paciente (relatório/resultado de exames/aprovação para procedimento).

Figura 17: Resultado de um Transação. Fonte: Desenvolvido pelos Autores

Após o POW dessa transação, o bloco é adicionado a instancia do Blockchain onde poderá ser distribuído por todos os nós da rede. O protótipo salva esses blocos de forma linear no banco de dados para uso futuro.

Figura 18: Instancia do Blockchain. Fonte: Desenvolvido pelos Autores.

Na figura 18 é apresentado uma instancia do blockchain, o primeiro bloco (Genesis) não possui prevHash, porém os demais blocos adicionando apontam para o antecessor corretamente.

5 CONCLUSÃO

Esta pesquisa teve como objetivo de esclarecer os conceitos relacionados à tecnologia do Blockchain, assim como seus impactos e cenários de aplicação, principalmente, no setor de saúde. Com base em tudo em que foi discutido, o uso de Blockchain na área da saúde seria a forma mais possível de garantir a capacidade de proteger uma massiva quantidade de dados sensíveis, essa teoria foi provada com um simples protótipo funcional, que revitaliza a área da tecnologia em um dos pontos mais precários do Brasil.

O principal benefício encontrado na implementação do blockchain, é a descentralização. Ao descentralizarmos os dados, o gerenciamento e o acesso aos recursos do aplicativo, é possível alcançar um serviço maior e mais justo. Outras vantagens da descentralização são: melhora na reconciliação de dados, redução de pontos de fraqueza, otimiza a distribuição de recursos e um ambiente sem um TTP.

As evidências de testes demonstram que, o protótipo conseguiu alcançar resultados positivos e com um custo computacional baixo. Dentro os pontos positivos do protótipo de Blockchain, é possivel destacar o aproveitamento dos recursos de criptografia nativos do Node.js em conjunto com o uso do TypeScript para garantir uma adequação no processo de desenvolvimento.

Segundo Almeida (2019), podemos afirmar que o futuro de ferramentas como o blockchain para a área de saúde é bastante promissor, uma vez que essa estrutura possui potencial para sustentar um sistema rigoroso de preservação de dados dos pacientes e, ao mesmo tempo, ampliar o acesso à informação de novas descobertas e estudos científicos.

Com o desenvolvimento dessa aplicação foram surgindo alguns pontos que se relevaram interessantes que poderiam ser adicionados como novas funcionalidade. Algumas melhorias a serem feitas em uma futura implementação:

- Utilização de Contratos Inteligentes para Medicina e sistemas de saúde.

- Desenvolvimento de uma aplicação Front-End com conexões a sistemas como o Google Calendar via API.
- Implementação da Árvore de Merkle, definição do tamanho padrão dos blocos e utilização de intervalo de tempo para efetuar a criação de um Bloco.

6 REFERÊNCIAS BIBLIOGRÁFICAS

[1] **Como a criptografia funciona no certificado digital.** Disponível em: < https://blog.certisign.com.br/como-a-criptografia-funciona-no-certificado-digital/ > Acessado em 25 abr. 2021

[2] STAIR, Ralph M.; REYNOLDS, George W. **Principles of Information Systems 9th Edition**, 2009.

[3] STAIR, Ralph M.; REYNOLDS, George W. **Fundamentals of Information Systems 6th Edition**, 2011.

[4] TAYLOR, R.S. **Information and Productivity: On Defining information Output (II)*,** 1984**.**

[5] RAMAPRASAD, Arkalgud. **On the Definition of Feedback,** 1983.

[6] YAGA, Dylan; MELL, Peter; ROBY, Nik; SCARFONE, Karen. **Blockchain Technology Overview**, 2018.

[7] LAMPORT, Leslie. **The Part-Time Parliament**. ACM Transactions on Computer Systems, volume 16. 1998.

[8] SWAN, Melanie. **Blockchain: blueprint for a new economy**. Sebastopol: O`Reilly, 2015. 128 p.

[9] ROSIC, Ameer. **What Is Hashing?** [Step-by-Step Guide-Under Hood of Blockchain]. Disponível em: < https://blockgeeks.com/guides/what-is-hashing/ > Acessado em 12 de abr. 2021.

[10] FRANCO, Joel L. F. **Sistemas de informação.** Disponível em: < https://www.unasus.unifesp.br/biblioteca_virtual/pab/6/unidades_conteudos/unidade08/p_02.html/ > Acessado em 25 abr. 2021

[11] PLANEZ**,** Paulo. **Um pouco de História para entender os sistemas de informação.** Disponível em: < https://www.tiespecialistas.com.br/um-pouco-de-historia-para-entender-os-sistemas-de-informacao/#:~:text=A%20import%C3%A2ncia%20dada%20%C3%A0%20informa%

C3%A7%C3%A3o,bem%20como%20o%20alicerce%20do/ > Acessado em 25 abr. 2021

[12] **Lei de Proteção de Dados já está em vigor; saiba como adequar sua empresa.** Disponível em: < https://www.fecomercio.com.br/noticia/mp-959-e-aprovada-sem-prorrogacao-da-entrada-em-vigor-da-lgpd-para-2021#:~:text=Independentemente%20da%20aprova%C3%A7%C3%A3o%20da%20MP,de%20Direito%20Privado%20(RJET)./ > Acessado em 13 mai. 2021

[13] ALMEIDA, Lucas. **O que é e como a LGPD irá afetar a área de saúde?** Disponível em: < https://nexxto.com/como-a-lgpd-afetara-a-area-de-saude/ > Acessado em 13 mai. 2021

[14] LIANG, X.; ZHAO, J.; SHETTY, S.; LIU, J.; & LI, D. **Integrating blockchain for data sharing and collaboration in mobile healthcare applications.** IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017.

[15] ANTONOPOULOS, Andreas M. **Mastering Bitcoin: Unlocking Digital Cryptocurrencies 2nd ed.** Sebastopol: O`Reilly, 2017.

[16] **Árvores de Merkle.** Disponível em: < https://pt.wikipedia.org/wiki/%C3%81rvores_de_Merkle/ > Acessado em 20 mai. 2021

[17] DE NEGRI, Fernanda. **As tecnologias da informação podem revolucionar o cuidado com a Saúde?** Disponível em: < https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/107-as-tecnologias-da-informacao-podem-revolucionar-o-cuidado-com-a-saude/ > Acessado em 20 mai. 2021

[18] Agbo, Cornelius C.; Mahmoud, Qusay H.; Eklund, J. Mikael. **Blockchain Technology in Healthcare: A Systematic Review.** Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Oshawa, 2019.

[19] ALMEIDA, Lucas. **Blockchain na saúde: tecnologia e segurança em benefício do paciente** Disponível em: < https://nexxto.com/blockchain-na-saude/#:~:text=O%20blockchain%20no%20setor%20de%20sa%C3%BAde%20perm

ite%20o%20controle%20e,uma%20rede%20ponto%20a%20ponto./ > Acessado em 20 mai. 2021

[20] HIPAA Journal. **Healthcare Data Breach Statistcs** Disponível em: < https://www.hipaajournal.com/healthcare-data-breach-statistics/ > Acessado em 20 mai. 2021

[21] BISCHOFF, Paul. **Ransomware attacks on US healthcare organizations cost $20.8bn in 2020** Disponível em: < https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/#How_much_did_these_ransomware_attacks_cost_healthcare_organizations_in_2020/ > Acessado em 15 mai. 2021

[22] CASTRO, Guilherme. **Explaining blockchain basics.** Disponível em: < https://dev.to/gmfcastro/my-best-shot-explaining-blockchain-4873\ > Acessado em 10 mai. 2021

[23] Fórum Saúde Digital. **O papel do blockchain na Saúde Digital do paciente em 2018**. Disponível em: < https://forumsaudedigital.com.br/o-papel-do-blockchain-na-saude-digital-do-paciente-em-2018/ > Acessado em 15 mai. 2021.

[24] PATEL, Priyesh. **The State of NoSQL with MongoDB and Node.js 2019**. Disponível em: < https://blog.bitsrc.io/the-state-of-nosql-with-mongodb-and-node-js-2018-690588c03650/ > Acessado em 16 mai. 2021.

[25] NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Eletronic Cash System**. Disponível em: < https://bitcoin.org/bitcoin.pdf/ > Acessado em 20 abr. 2021.

[26] Node.js. **How to use the crypto module.** Disponível em: < https://nodejs.org/en/knowledge/cryptography/how-to-use-crypto-module/ > Acessado em 28 mai. 2021.

[27] MDN Web Docs. **JavaScript.** Disponível em: < https://developer.mozilla.org/pt-BR/docs/Web/JavaScript/ > Acessado em 28 mai. 2021.

[28] Node.js. **Introduction to Node.js.** Disponível em: < https://nodejs.dev/learn/ > Acessado em 28 mai. 2021.

[29] Node.js. **Node.js with TypeScript.** Disponível em: < https://nodejs.dev/learn/nodejs-with-typescript/ > Acessado em 28 mai. 2021.

[30] Node.js. **What is npm?** Disponível em: < https://nodejs.org/en/knowledge/getting-started/npm/what-is-npm/ > Acessado em 28 mai. 2021.

[31] MongoDB. **What Is MongoDB?** Disponível em: < https://www.mongodb.com/what-is-mongodb/ > Acessado em 28 mai. 2021.