UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

ALAN NASCIMENTO GOMES

UMA SOLUÇÃO PARA COMPARTILHAMENTO DE DADOS DE SAÚDE BASEADA EM BLOCKCHAIN PERMISSIONADA E INTERNET DAS COISAS PARA HOSPITAIS INTELIGENTES

QUIXADÁ

2022

ALAN NASCIMENTO GOMES

UMA SOLUÇÃO PARA COMPARTILHAMENTO DE DADOS DE SAÚDE BASEADA EM BLOCKCHAIN PERMISSIONADA E INTERNET DAS COISAS PARA HOSPITAIS INTELIGENTES

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Emanuel Ferreira Coutinho

QUIXADÁ

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

G612s Gomes, Alan Nascimento.
Uma solução para compartilhamento de dados de saúde baseada em blockchain permissionada e internet das coisas para hospitais inteligentes / Alan Nascimento Gomes. – 2022.
67 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Engenharia de Computação, Quixadá, 2022.
Orientação: Prof. Dr. Emanuel Ferreira Coutinho.

1. Telemedicina. 2. Blockchains (Base de dados). 3. Internet das coisas. I. Título.

CDD 621.39

ALAN NASCIMENTO GOMES

UMA SOLUÇÃO PARA COMPARTILHAMENTO DE DADOS DE SAÚDE BASEADA EM BLOCKCHAIN PERMISSIONADA E INTERNET DAS COISAS PARA HOSPITAIS INTELIGENTES

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Aprovada em: ____/_____/_____

BANCA EXAMINADORA

Prof. Dr. Emanuel Ferreira Coutinho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Me. Roberto Cabral Rabêlo Filho
Universidade Federal do Ceará (UFC)

Prof. Dr. Thiago Werlley Bandeira da Silva
Universidade Federal do Ceará (UFC)

Prof. Me. Maurício Moreira Neto
Centro Universitário Christus (UNICHRISTUS)

À minha família, amigos e colegas que sempre me apoiaram.

AGRADECIMENTOS

À Deus, pela vida e por preparar os meios para que eu chegasse até aqui.

Ao meu pai, Braz, por todo esforço e empenho feitos por mim.

Aos meus irmãos, Gracilane, Erlânia e Diogo por todo o apoio nessa jornada.

Ao professor Emanuel, pelas orientações e auxílios para a produção desse trabalho.

Aos amigos de graduação pelas experiências e aprendizados construídos juntos.

Agradeço o apoio do *Insight Data Science Lab* pelos recursos disponibilizados para a realização desse trabalho, oferecido por meio do projeto **Governo Digital do Estado do Ceará**, financiado pela FUNCAP número 04772314/2020.

À toda comunidade acadêmica da Universidade Federal do Ceará por todo apoio oferecido para o meu desenvolvimento pessoal, acadêmico e profissional.

“A persistência é o menor caminho do êxito.”

(Charles Chaplin)

RESUMO

Diversas tecnologias estão sendo utilizadas em conjunto para a melhoria da qualidade de serviço de saúde. Nesse contexto, aplicações que utilizam a tecnologia para beneficiar a área da saúde fazem parte da tecnologia *E-health*. Esse tipo de serviço está crescendo em importância ao longo do tempo, sendo utilizado desde o acesso remoto a prontuários médicos até a troca de dados em tempo real utilizando sensores corporais. De forma análoga, a utilização da tecnologia *blockchain* vem crescendo no setor da saúde, devido ao seu conjunto de possibilidades de soluções. Essa tecnologia funciona como um livro-razão distribuído e permite que transações sejam realizadas sem a intermediação de terceiros. Com isso, a integração dessas tecnologias pode trazer uma série de benefícios para o setor da saúde, como uma maior disponibilidade e privacidade aos dados de saúde. Este trabalho busca fornecer uma solução para monitoramento e compartilhamento de sinais vitais de pacientes que estejam sob os cuidados de uma instituição de saúde inteligente, baseado na tecnologia *blockchain*. Para isso, foi desenvolvido uma solução baseada em quatro camadas. Para a camada física foi construído um protótipo *IoT* para a aferição de algumas variáveis de saúde. Na camada de comunicação foi utilizado um *middleware* de comunicação *IoT*. Na camada de armazenamento foi desenvolvimento uma infraestrutura de rede *blockchain*. E, por fim, para a camada de aplicação foi desenvolvido protótipo de uma aplicação *WEB*. Testes de carga foram realizados para verificar a resposta do sistema em diferentes cenários. Com os resultados obtidos nota-se a possível implementação dessa solução em uma instituição de saúde inteligente. Apresentando também, uma contribuição no contexto de aplicações que integram *E-health* e *blockchain*.

Palavras-chave: *Telemedicina*. *Blockchains (Base de Dados)*. *Internet das Coisas*.

ABSTRACT

Several technologies are being used together to improve the quality of health services. In this context, applications that use technology to benefit the health area are part of E-health technology. This type of service is growing in importance over time, being used from remote access to medical records to real-time data exchange using body sensors. Similarly, the use of blockchain technology has been growing in the health sector, due to the set of possibilities for solutions that this technology has. This technology works like a distributed ledger and allows transactions to be carried out without the intermediation of third parties. Thus, the integration of these technologies can bring a series of benefits to the health sector, such as greater availability and privacy of health data. This work seeks to provide a solution for monitoring and sharing vital signs of patients under the care of a smart healthcare institution, based on blockchain technology. For this, a solution based on four layers was developed. For the physical layer, an IoT prototype was built to measure some health variables. In the communication layer, an IoT communication middleware was used. At the storage layer, a blockchain network infrastructure was developed. And, finally, for the application layer, a prototype of a WEB application was developed. Load tests were performed to verify the system response in different scenarios. With the results obtained, the possible implementation of this solution in an intelligent health institution is noted. Also presenting a contribution in the context of applications that integrate E-health and blockchain.

Keywords: Telemedicine. Blockchains (Database). Internet of Things.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

IoT	*Internet Of Things*
SenSE	*Sensor Simulation Environment*
HLF	*Hyperledger Fabric*
HSM	*Hardware Security Module*

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas, os processos do setor de *healthcare* (“Cuidados de saúde”, em português) foram beneficiados com melhorias de acesso, eficiência, qualidade e eficácia. Com isso, o uso de aplicações que beneficiam os cuidados de saúde, conhecidas como aplicações *E-health*, passaram a ser comumente relacionadas a Tecnologia da Informação e Comunicação (TICs) (ACETO *et al.*, 2018).

O significativo aumento de soluções que utilizam essas aplicações contribuíram para que a quantidade de informações relacionadas ao estado de saúde de pacientes permanecesse cada vez mais presente em sistemas computacionais. Prontuários eletrônicos, diagnósticos médicos e dados de sensores de monitoramento de saúde são exemplos de informações gerenciadas por esses sistemas, sendo que o compartilhamento desses dados são de extrema importância para estudos e diagnósticos mais rápidos (AGUIAR *et al.*, 2020).

Instituições de saúde e pacientes podem compartilhar dados em bases centralizadas e com baixo custo de implantação. Contudo, mesmo com esse proveito, existem maiores riscos em relação a problemas e limitações de compartilhamento de dados médicos. Dessa forma, são atribuídas características ineficientes aos dados como, por exemplo, baixa distribuição, inconfiabilidade e inconsistência (STANCIU, 2017).

Por se tratar de informações pessoais, o controle e a posse dos dados são diretamente pertencentes aos pacientes ou a quem possui consentimento de manipulação. Além disso, informações de saúde são protegidas por leis, por exemplo, a Lei Geral de Proteção de Dados (LGPD) (Lei n.13.709/2018), que regulam as atividades de tratamento de dados pessoais. No entanto, esses dados são geralmente controlados por diferentes provedores de serviços, fabricantes de dispositivos ou espalhados em diferentes sistemas de saúde (ZHANG *et al.*, 2016). Neste contexto, surgem algumas barreiras relacionadas ao risco de segurança e privacidade dos dados, visto que o armazenamento centralizado é um ponto de destaque para ataques cibernéticos (PETERSON *et al.*, 2016).

Para mitigar os problemas discutidos e potencializar os sistemas de saúde, a *IoT* tem se destacado na área de pesquisa nos últimos anos (FARAHANI *et al.*, 2018a). Em Zemrane *et al.* (2019), definem *IoT* como sendo uma tecnologia capaz de possibilitar a construção de um ambiente inteligente, usando objetos que têm a capacidade de gerar dados autonomamente a partir do ambiente em que são implantados.

O uso de sensores inteligentes para monitoramento do estado de saúde de pacientes

são também classificados como aplicações *E-health*, consequentemente as informações produzidas pela rede de sensores são dados sensíveis. Por isso, é necessário um ambiente que integra a tecnologia *IoT* com sistemas remotos e infraestruturas de maneira mais segura (RIFI *et al.*, 2018).

Tendo em vista os cenários dos problemas apresentados e a sensibilidade do acesso aos dados de saúde, existe a necessidade de um meio de compartilhamento que gerencie os dados de forma confiável para prover maior controle de dados dos pacientes (GAN *et al.*, 2020). A disseminação não permitida dos dados de saúde pode gerar consequências indesejadas e prejudicar não só aos pacientes, mas também as entidades ou profissionais de saúde que possuem acesso aos dados.

Com isso, a *blockchain* surge como uma tecnologia que pode realizar o tratamento dos problemas mencionados. Utilizando-a como uma solução de compartilhamento de dados, é possível que as transações sejam verificadas com alto grau de confiabilidade, além de permitir a descentralização dos dados (AGUIAR *et al.*, 2020). Além da tecnologia *blockchain* ser aplicada a aplicações de gerenciamentos de dados em geral, é possível que ela seja aplicada também a um cenário *IoT* que necessite de proteção de dados (RIFI *et al.*, 2018).

A tecnologia *blockchain* é uma rede *peer-to-peer* que armazena uma cadeia de blocos e utiliza algoritmo de consenso e criptografia para validação das transações (ZENG *et al.*, 2019). Devido às características de descentralização e a ausência de uma entidade centralizada, as tecnologias baseadas em *blockchain* ficaram populares (THAKKAR *et al.*, 2018), crescendo não só no setor financeiro, onde foi inicialmente proposta, mas também em diversas outras áreas, como em cenários *IoT*.

Nesse contexto, este projeto de pesquisa propõe uma solução utilizando as tecnologias *IoT* e *blockchain* para fornecer uma visão compartilhada dos dados de saúde para pacientes, médicos e administradores de gestão hospitalar. Este trabalho possui relevância para pesquisas que buscam analisar o uso da tecnologia *blockchain* em aplicações *E-health* de monitoramento. Além disso, a solução proposta poderá ser utilizada como base por profissionais da gestão de TI hospitalar, para implantação de outros serviços que não sejam de monitoramento do estado de saúde.

1.1 Objetivos

Nesta Seção, serão apresentados o objetivo geral deste trabalho e alguns objetivos específicos.

1.1.1 Objetivo Geral

O objetivo geral é fornecer uma solução para monitoramento e compartilhamento de sinais vitais de pacientes que estejam sob os cuidados de uma instituição de saúde inteligente. A solução a ser desenvolvida utiliza-se das características da *blockchain*, como imutabilidade, não repúdio e confiabilidade para o desenvolvimento de um sistema mais confiável. Além disso, os sinais vitais são obtidos a partir de um cenário *IoT* implantado na instituição de saúde.

1.1.2 Objetivos Específicos

Os objetivos específicos são:

- Projetar uma rede *blockchain* para compartilhamento de dados de sensores de saúde.
- Definir uma infraestrutura de comunicação entre um cenário *IoT* e uma rede *blockchain*.
- Propor uma aplicação que apresente de forma compreensível as informações relacionadas ao estado de saúde dos pacientes.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção tem o propósito de apresentar os conceitos, ferramentas e técnicas que foram abordados nesta pesquisa. De modo geral, serão apresentados quatro escopos de estudo e como estão relacionados entre si. Além disso, será exposto como esses conceitos estão sendo utilizados para este trabalho. Na Seção 2.1 será abordado os conceitos associados a tecnologia *blockchain*, com as suas principais características e seus modelos. Na Seção 2.2 será abordado sobre a plataforma *Hyperledger* que será utilizada para desenvolvimento de uma *blockchain* permissionada. Na Seção 2.3 apresentam-se os princípios e aplicações da tecnologia *IoT* (*Internet of Things*) e como está se relacionando com *E-health* e *blockchain*. E por fim, na Seção 2.4 é discutido sobre os conceitos e componentes do *middleware* FIWARE.

2.1 Tecnologia Blockchain

Blockchain é uma tecnologia emergente que possibilita a criação de livros-razão distribuídos que vem atraindo tanto a academia quanto a indústria para o desenvolvimento de pesquisas e aplicações (ZHOU *et al.*, 2020). O principal componente da tecnologia *blockchain* é o livro-razão. Este elemento é uma estrutura para armazenamento das transações realizadas pelo sistema, funcionando de forma análoga a livros contábeis do setor financeiro.

Junto com o desenvolvimento das criptomoedas, a tecnologia de livro-razão distribuída surgiu para revolucionar o mercado financeiro. Devido ao sucesso da implantação nesse setor e ao acréscimo de novas tecnologias no seu funcionamento, o uso da tecnologia *blockchain* expandiu-se para outras áreas. Um dos principais eventos que possibilitou essa expansão foi a implantação de contratos inteligentes (*Smart Contracts*) (SWAN, 2015).

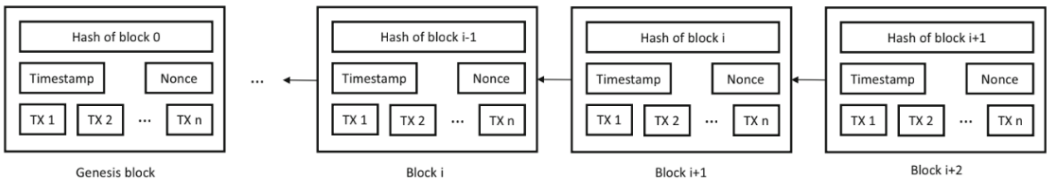
Problemas de confiança são atribuídos a sistemas de informação que não implementam verificação ou auditoria de dados na sua solução. Motivado pela situação exposta, Nakamoto (2008) propôs conceitos que buscavam amenizar problemas do mercado financeiro, como a criptomoeda Bitcoin e a cadeia de blocos (REYNA *et al.*, 2018). A ideia foi manter valores da criptomoeda virtual sem o apoio de qualquer autoridade centralizada ou entidade financeira. De encontro aos sistemas tradicionais, os valores monetários são mantidos de forma coletiva em uma rede *peer-to-peer* descentralizada e segura.

2.1.1 Característica da blockchain

Agora, nesta subseção será discutido sobre as principais características da *blockchain* e quais os principais benefícios oferecidos por essa tecnologia. Segundo Swan (2015) e Hoy (2017) a rede *blockchain* foi marcada por três fases. A primeira, chamada de *blockchain* 1.0, foi marcada pelo surgimento das criptomoedas, sendo proposta inicialmente por Nakamoto (2008). A segunda, chamada *blockchain* 2.0, é caracterizada pela implantação de contratos inteligentes. Esta fase foi baseada no artigo de Buterin *et al.* (2014) que possibilitou a realização de transações mais complexas. E por último, chamada de *blockchain* 3.0, esta é reconhecida pela expansão da utilização da *blockchain* para outras áreas, além do mercado financeiro.

Na Figura 1 é ilustrado uma cadeia de blocos. Esta é uma estrutura de dados utilizada pela *blockchain* para ser realizado o registro das transações. Os dados armazenados nessa estrutura são inalteráveis, devido a característica dada a cada bloco de validar a integridade do seu bloco pai (bloco anterior). Em cada bloco podem ser armazenados diferentes transações que podem ser validadas utilizando mecanismos criptográficos. Além disso, cada bloco possui um carimbo de data e hora (*timestamp*), o valor de resumo do bloco anterior e um número aleatório, denominado "*nonce*", utilizado para verificar o *hash* e, consequentemente, garantir a integridade de toda a cadeia (NOFER *et al.*, 2017).

Figura 1 – Blockchain e seus blocos.



Fonte: Adaptado de Nofer *et al.* (2017)

Em relação aos benefícios trazidos pela *blockchain* quando esta é aplicada em sistemas de informações, pode-se citar alguns, como: (LIN; LIAO, 2017; XU *et al.*, 2017):

- **Descentralização** - esta é uma característica de sistemas distribuídos, onde não existe uma entidade intermediária e centralizada para controle do sistema como um todo. Os sistemas que utilizam a *blockchain* não necessitam de um nó centralizado, as validações são efetuadas de forma distribuída e descentralizada. Possibilitando a redução de problemas como indisponibilidade, devido a cópias idênticas da cadeia de blocos que é difundida por toda a rede.
- **Tolerância a falhas** - em uma arquitetura descentralizada é fornecido tolerância a falhas,

pois é eliminado o risco de um único ponto de falha.

- **Transparência** - os acessos que são efetuados aos dados são auditáveis e uma vez que são concretizado registros é possível realizar o rastreamento das informações.
- **Segurança** - por meio do uso de certificados digitais e funções criptográficas, os participantes recebem endereços e chaves privadas que usam para acessar a *blockchain*.
- **Pseudo-Privacidade** - as partes interessadas da rede podem verificar os dados enviados, bem como o remetente, sem ter que depender de servidores centralizados. Esses dados, quando adicionados a *blockchain*, não podem ser excluídos ou alterados.
- **Auditabilidade** - por meio de *logs* de atividades dos participantes da rede é garantido a auditabilidade e confiança entre os atores.

2.1.2 Modelos de Blockchain

As características discutidas na seção anterior são aplicadas a *blockchain* de uma forma geral. No entanto, esta tecnologia pode ser dividida em categorias de acordo como os dados são protegidos. Essas categorias são classificadas, como: permissionadas (*permissioned*, em inglês) e não-permissionadas (*permissionless*, em inglês) (WüST; GERVAIS, 2018; ALHADHRAMI *et al.*, 2017).

As redes não-permissionadas caracterizam-se por serem abertas e transparentes para todos os participantes da rede. O livro-razão pode ser analisado por qualquer usuário e qualquer participante da rede tem a opção de se tornar um componente capaz de realizar a validação dos blocos (HELLIAR *et al.*, 2020). Como exemplos de *blockchains* não permissionadas, podem ser citados a plataforma *Ethereum* e a *blockchain* da criptomoeda *Bitcoin*.

As redes *blockchains* permissionadas caracterizam-se pela inexistência de criptomoedas e a necessidade de nós responsáveis por realizar autenticação. Além disso, dividem-se em permissionadas públicas e privadas. As permissionadas públicas são reconhecidas pelo controle do ingresso na rede e os membros autenticados podem fazer parte do conjunto de nós validadores. As permissionadas privadas também possuem a característica de necessidade de controle de participação na rede, mas as permissões para persistência de dados são centralizadas em uma ou mais organizações confiáveis (VIRIYASITAVAT; HOONSOPON, 2019). O *Hyperledger Fabric* e a plataforma *Corda* são exemplos do tipo permissionada. Para este trabalho o tipo de *blockchain* utilizada será a permissionada privada, pois trabalhará com dados sensíveis e necessitará de autenticação para as partes interessadas interagirem com a rede.

2.1.3 Contratos Inteligentes

Tendo em vista a divisão dos tipos de *blockchains* citadas na seção anterior, pode-se perceber que é necessário um componente capaz de possibilitar a interação do usuário com esses modelos. O responsável por essa função em um cenário que utiliza a cadeia de blocos é o contrato inteligente. A concepção de contrato inteligente foi estabelecido por Szabo (1994), definido-o como um protocolo de transação computadorizado que executa a vigência de um contrato. A implantação de contratos inteligentes foi tão importante que marcou uma nova fase para a *blockchain*. Nesse contexto, o uso desses contratos possibilitam a utilização de redes *blockchains* para acordos dinâmicos e com maior confiança na troca de ativos digitais (SWAN, 2015).

Os contratos inteligentes funcionam como códigos executáveis que agem conforme as condições do acordo entre as partes interessadas, possibilitando a inexistência de uma entidade intermediária para garantia das transações. O uso de contratos inteligentes nas aplicações baseada em *blockchain* pode oferecer uma série de benefícios, como: atualizações rápidas em tempo real, menos intermediários, custo mais baixos e novos modelos de negócios (MOHANTA *et al.*, 2018). Os contratos inteligentes também serão abordados neste trabalho para possibilitar a comunicação de um usuário com a rede *blockchain*. Na Figura 2 é mostrado um contrato inteligente que determina o vencedor de um jogo, através dos métodos definidos é possível ler e escrever objetos na cadeia de blocos (BECKERT *et al.*, 2018).

2.2 Plataforma Hyperledger Fabric

O *Hyperledger Fabric Hyperledger Fabric* (*HLF*) é uma plataforma de livro-razão distribuída e permissionada mantida pela Linux Foundation. Esta plataforma foi projetada para ser altamente modular e extensível, oferecendo confidencialidade, privacidade e escalabilidade para *blockchains* empresariais. Por conta dessas características apresentadas foi possível a realização de experimentos com essa plataforma em aplicações reais (BALIGA *et al.*, 2018).

Além da plataforma *Hyperledger Fabric* existem outras iniciativas que pertencem ao projeto *Hyperledger*. Na Figura 3, é apresentada o ecossistema de *frameworks* e ferramentas do *Hyperledger*. O conjunto desses componentes busca promover e alavancar tecnologias *blockchain* para garantir auditoria, transparência e confiança entre parceiros de negócios. Dentre essas ferramentas pode-se citar alguns exemplos, como (YANG, 2018):

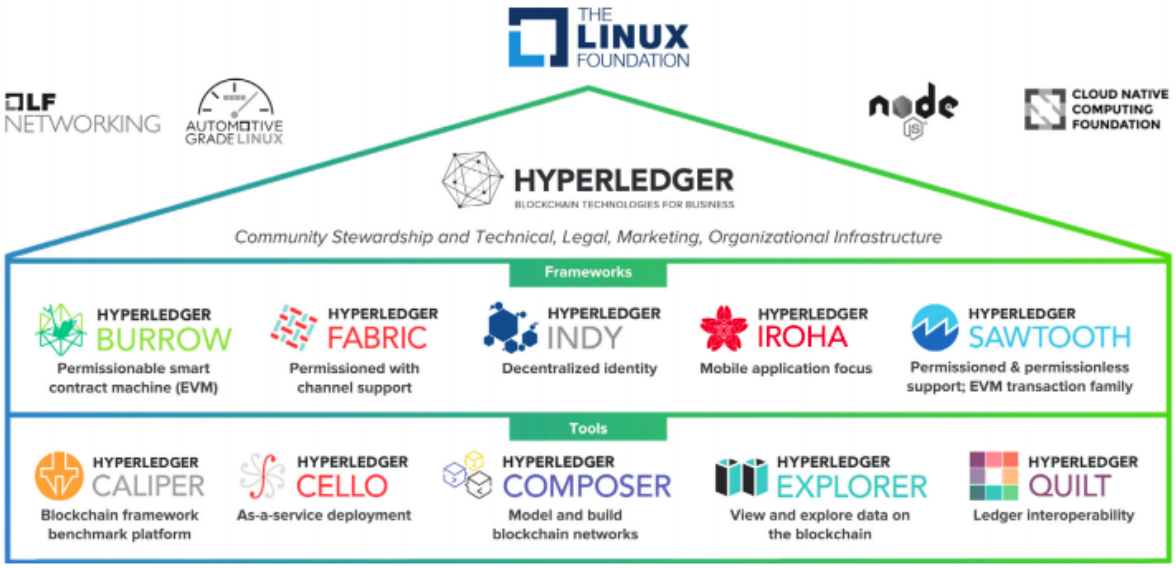
Figura 2 – Exemplo de Contrato Inteligente.

```
public class RPS extends ChaincodeBase {
  public Response getWinner(ChaincodeStub stub,
                            int gameId) {
    Game game = readGame(stub, gameId);
    int winner = 0;
    int s1 = game.sign1; int s2 = game.sign2;
    if (sign1Won(s1, s2)) winner = 1;
    else if (sign1Won(s2, s1)) winner = 2;
    game.winner = winner;
    writeGameToLedger(stub, gameId, game);
    return newSuccessResponse();
  }
  ...
  /*@ ensures \result <==>
    @   (s1 == ROCK && s2 == SCISSORS)
    @   || (s1 == PAPER && s2 == ROCK)
    @   || (s1 == SCISSORS && s2 == PAPER);
    @ assignable \nothing;
    @*/
  private boolean sign1Won(int s1, int s2) {
    return (3 + s1 - s2) % 3 == 1;
  }
}
```

Fonte: Adaptado de Beckert *et al.* (2018)

– **SAWTOOTH**: É uma plataforma *blockchain* que possibilita o paralelismo da execução de transações, através da divisão dos blocos em fluxos paralelos. Além disso, permite a mudança do algoritmo de consenso de forma simples.
– **IROHA**: É uma estrutura de *blockchain* e um dos projetos *Hyperledger*. Suporta manipulação de ativos digitais com comandos e operações de leituras rápidas.
– **INDY**: Surgiu para auxiliar na documentação e validação de empresas. Concebido para operar com identidade descentralizada e fornece ferramentas, bibliotecas, e componentes reutilizáveis. Permite interoperabilidade entre as identidades em diferentes tipos de *blockchains*.
– **EXPLORER**: Ferramenta que objetiva criar um explorador genérico de *blockchain* para *web*.
– **CALIPER**: Ferramenta de *benchmark* que permite os usuários avaliarem a performance de implementações específicas de *blockchain* com um conjunto pré-definido de casos de uso.

Figura 3 – Ecossitema *Hyperledger*.



Fonte: Adaptado de Yang (2018)

2.2.1 Rede Fabric

Em uma rede *Hyperledger* Fabric é utilizado um conjunto de nós que ao serem combinados criam uma rede que possibilita comunicação com aplicativos externos. As organizações são vistas como membros que fazem parte da rede *blockchain* e são identificadas pelo ID do provedor de serviços de associação (MSP). Este componente tem a função de gerenciar como novos membros podem receber assinaturas digitais e serem verificados. Uma organização de uma rede *HLF* pode ser tão grande quanto uma corporação multinacional ou tão pequena quanto um indivíduo *blockchain* (ANDROULAKI *et al.*, 2018).

Os nós na rede *HLF* podem pertencer a três categorias. A primeira categoria são os nós clientes, podendo ser aplicativos *web*/móveis, kit de desenvolvimento de *software* (SDK). A segunda categoria são os *peers*, esses componentes são responsáveis por manter o livro razão e executar o *chaincode*. Os *peers* são classificados em dois tipos. O primeiro tipo são os *peers* âncoras que lidam com a comunicação entre diferentes organizações na rede, compartilhando dados em suas respectivas organizações, já os *peers* endossantes lidam com a aprovação das transações (ANDROULAKI *et al.*, 2018). A rede Fabric também será abordada neste trabalho por possibilitar a implementação de um rede *blockchain* permissionada e privada.

2.2.2 Ledger e Banco de Dados de Estado Mundial

Um *ledger* é uma cadeia de blocos que contém registros de transações que são imutáveis. Depois que os nós validam as transações o estado do razão é distribuído entre os nós participantes. Existem duas variações do estado mundial: estado mundial e a cadeia de blocos (FABRIC, 2020). O estado mundial contém o estado do valor atual do razão, tornando mais fácil para aplicativos ou nós recuperarem rapidamente informações recentes sem ter que percorrer o razão. Já a cadeia de blocos refere-se a uma sequência restrita de blocos de transações encadeadas. O banco de dados de estado mundial será abordado neste trabalho, através da sua implementação no banco de dados CouchDB.

2.2.3 Chaincodes

Os contratos inteligentes da plataforma *Hyperledger* Fabric são comumentes denominados de *chaincode*. Os contratos inteligentes quando são implantados na rede são utilizados como aplicativos e são escritos nas liguagens Java, Go ou JavaScript. A sua principal função é gerenciar o acesso e as modificações realizadas nos conjuntos de pares de chave-valor no banco de dados de estado mundial. Os *chaincodes* serão os contratos inteligentes definidos para a solução deste trabalho, pois permitirá a inserção de dados de sensores na rede *blockchain* (UDDIN, 2021).

2.2.4 Mecanismos de Consenso

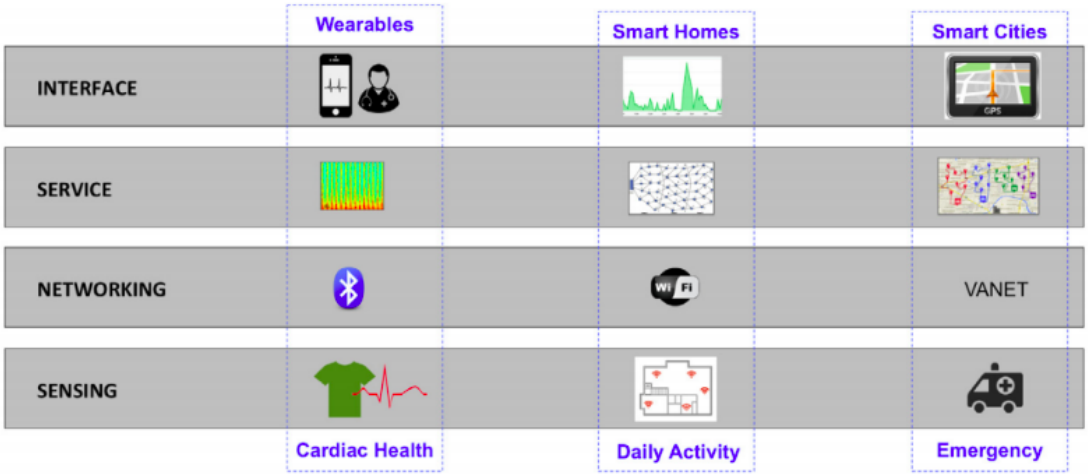
Em uma estrutura descentralizada, como é o caso da *blockchain*, é preciso existir a confiança entre as partes interessadas da rede. Com isso, são aplicados protocolos de consenso para permitir a confiança durante as validações dos blocos que serão incorporados a cadeia de blocos (CACHIN; VUKOLIĆ, 2017). Alguns exemplos de protocolos utilizados em plataformas *blockchain*, são: *Proof-of-Work* (PoW), *Pratical Binzantine Fault Tolerance* (PBFT), *Proof-of-Stake* (PoS) e Raft. Em cada um desses protocolos são definidas regras pré-estabelecidas que utilizam os próprios nós da rede para validação das transações. O mecanismo de consenso abordado na solução deste projeto será o protocolo Raft, pois é o indicado pela plataforma *Hyperledger* desde a versão 1.4.1.

2.3 Internet das Coisas

O avanço de diversas tecnologias proporcionou o surgimento da *Internet* das Coisas (do inglês, *Internet of Things*, *IoT*). Esta tecnologia interconecta dispositivos, denominados objetos inteligentes, que possuem poder computacional e de comunicação para captar e enviar dados sensoreados pela *internet* para proporcionar serviços aos seus usuários (FARAHANI *et al.*, 2018a). Existem diversos setores de aplicações *IoT* atualmente, por exemplo, a educação, transporte, agricultura, saúde, dentre outros.

Na Figura 4 é mostrado uma arquitetura multicamadas da tecnologia *IoT* (FARAHANI *et al.*, 2018a). Em geral, são definidos 4 níveis distintos em um cenário *IoT*. Do ponto de vista ascendente, a primeira camada é a de sensoreamento. Esta integra todos os diferentes tipos de hardware que fazem a coleta de dados. A segunda camada é a camada de rede, que oferece suporte de rede e transferência de dados em redes com e sem fio. A terceira camada é a camada de serviço que cria e gerencia todos os tipos de serviços com o objetivo de satisfazer os requisitos do usuário. A quarta é a camada de interface, que oferece métodos de interação para usuários e outros aplicativos, para que todos os dados possam ser analisados e todas as saídas possam ser apresentados.

Figura 4 – Camadas *IoT*.



Fonte: Adaptado de Farahani *et al.* (2018a)

Nesse contexto, em ecossitemas *IoT* existem vários protocolos de comunicação, componentes, soluções e aplicativos. No entanto, soluções e aplicativos de *IoT* são geralmente confundidos por uma "coisa", mas eles são diferentes. A solução é um produto ou serviço contendo dispositivos, plataformas, etc. E os aplicativos de *IoT* são software ou aplicativo móvel usados para acessar a solução (TAMBOLI, 2019). A seguir, serão apresentados alguns

dos principais conceitos abordados em *IoT*. A tecnologia *IoT* será utilizada na solução para possibilitar o monitoramento do estado vital de paciente, através da utilização de sensores inteligentes.

2.3.1 Definições Preliminares

As soluções de *IoT* contêm quatro blocos principais que são essenciais para a funcionalidade da solução, que são: (CHERUVU; WHEELER, 2020; GILCHRIST, 2017; TAMBOLI, 2019).

- **Dispositivos** - são os objetos *IoT* que realizam leituras do ambiente na qual estão monitorando, por exemplo sensores e atuadores. Os sensores podem medir ou detectar luz, calor, movimento ou qualquer outra quantidade física. Os dispositivos podem ter funcionalidade para realizar análise de dados e encriptar dados gravados no armazenamento interno (CHERUVU; WHEELER, 2020).
- ***Gateways*** - por conta da impossibilidade que alguns dispositivos possuem de não se conectar diretamente à *internet* para transmitir suas informações, são utilizados os *gateways* para prover essa comunicação. Os *gateways* são geralmente equipados com várias tecnologias de protocolo, como Bluetooth, *Wi-Fi*, GSM, Zigbee, etc. Os dispositivos móveis podem atuar como *gateways* que conectam os dispositivos *IoT* à *Internet*. O gateway precisa ser protegido, pois, pode ser alvo de invasores para obter acesso aos dados, já que os *gateways* funcionam como segregadores e duplicadores de dados (GILCHRIST, 2017).
- **Plataforma *IoT*** - Para um maior controle e gerenciamento dos dados são necessárias plataformas para oferecer esses serviços, geralmente eles estão hospedados em provedores da nuvem, como Azure ou AWS. Além disso, também realiza o processamento e a análise dos fluxos de dados. A plataforma funciona como orquestradora da solução *IoT*, fornecendo autenticação, análise e encriptação de dados armazenados (CHERUVU; WHEELER, 2020).
- **Aplicativos *IoT*** - Os aplicativos *IoT* são interfaces que comunicam as soluções *IoT* com o usuário. Os usuários raramente conseguem interagir diretamente com os sensores no ambiente, mas eles interagem por meio de aplicativos móveis, aplicativos da web, etc. Os aplicativos podem oferecer os dados da plataforma *IoT* em um formato utilizável para o usuário, por exemplo, gráficos (TAMBOLI, 2019).

2.3.2 IoT e E-health

Atualmente, a saúde tem uma oportunidade clara de aproveitar os benefícios potenciais da tecnologia *IoT*. A *IoT* no mercado de saúde foi avaliada em US 113,75 bilhões de dólares em 2019 e deve atingir US 332,67 bilhões de dólares em 2027 (ARFI *et al.*, 2021). A utilização de dispositivos *IoT* está se tornando cada vez mais acessível, incluindo o uso de dispositivos médicos. Com a introdução da conexão entre dispositivos *IoT* e *smartphones*, várias tecnologias baseadas em *IoT* ajudaram a modificar e promover sistemas de saúde tradicionais em sistemas mais inteligentes e personalizados (FARAHANI *et al.*, 2018b).

Considerando esses domínios, a tecnologia *IoT* aplicada à saúde pode permitir o monitoramento do paciente em tempo real para coletar, transferir e armazenar dados médicos. Além disso, a *IoT* pode usar os protocolos de conectividade disponíveis (por exemplo, *Bluetooth*, *Wi-Fi*) para facilitar a troca de informações e permitir que os profissionais de saúde transformem a forma como detectam doenças e inovam no atendimento ao paciente (ARFI *et al.*, 2021).

2.3.3 IoT e Blockchain

A miniaturização de sensores possibilitou a implantação desses dispositivos em pacientes para monitoramento do estado de saúde. Neste cenário, da mesma forma que os demais dados de saúde são tratados, as informações geradas pelos sensores também devem ser gerenciados de forma segura. Devido às características da *blockchain*, a implantação dessa tecnologia também pode ser utilizada para tratar os dados gerados por sensores de saúde (RIFI *et al.*, 2018). Os autores (JAMIL *et al.*, 2020) destacaram algumas características essenciais quando as tecnologias *IoT* e *blockchain* são combinadas, por exemplo: escalabilidade, melhoria na taxa de transferência e transparência de sistemas.

2.4 Plataforma FIWARE

FIWARE é uma plataforma de código aberto para a construção de soluções inteligentes em diferentes domínios de aplicação. Oferece uma biblioteca de catálogos de componentes conhecidos como *Generic Enablers* (GEs), juntamente com um conjunto de implementações de referência que permitem a instalação de algumas funcionalidades como análise de *Big Data*, desenvolvimento de aplicativos de contexto, conexão com a Internet das Coisas (SANG *et al.*, 2020). Os GEs fornecem interfaces avançadas para redes e dispositivos, interfaces de usuário

baseadas na *web*, ecossistemas de aplicativos/serviços, redes de distribuição, hospedagem em nuvem, gerenciamento de dados de contexto, habilitação de serviço *IoT* e segurança (CELESTI *et al.*, 2019).

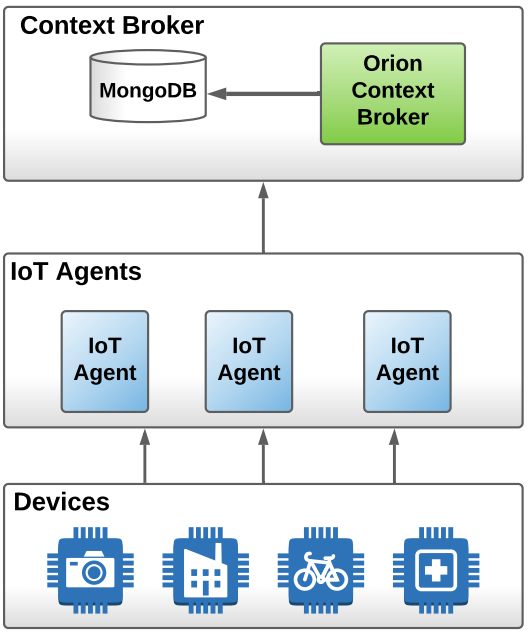
Os *Generics Enablers* da plataforma FIWARE são organizados em sete grupos principais que oferecem os serviços desta plataforma. A seguir serão mostrados esses grupos e uma breve descrição de cada (SALHOFER, 2018):

- **Gerenciamento de dados/contexto:** neste grupo são definidos todos os componentes necessários para armazenar, acessar, processar e analisar dados.
- **Internet das Coisas (*IoT*):** neste grupo estão todos os componentes necessários para configurar redes de sensores e rotear dados sensoriais para outros *GEs*.
- **Interface de usuário avançada baseada na *web*:** neste são definidos todos os componentes que projetam interfaces de usuário, incluindo informações geográficas e gráficos 3D interativos.
- **Segurança:** Componentes para adicionar, definir e reforçar a segurança.
- ***Middleware* para rede e dispositivos:** componentes responsáveis por possibilitar o uso de interfaces avançadas entre dispositivos e a rede.
- **Aplicativos/serviços e entrega de dados:** componentes e ferramentas para visualização de dados.
- **Cloud Hosting:** componentes e ferramentas que visam fornecer e gerenciar serviços FIWARE por meio de infraestrutura em nuvem.

Na Figura 5 é apresentado o uso dos componentes do FIWARE em um cenário *IoT* que utiliza sensores para detectar o estado de um ambiente. Fazendo uma análise ascendente, inicialmente existem um conjunto de sensores que coletam os dados do ambiente, em seguida, as informações geradas pelos dispositivos físicos são encaminhados para os componentes *IoT Agents*. Esses dados são processados de acordo com o protocolo utilizado pelo dispositivo e, em seguida, encaminhado para o componente *Orion Context Broker* com o padrão conhecido por este componente.

Tendo em vista os grupos definidos anteriormente, nas próximas duas subseções serão destacados dois componentes principais do FIWARE que serão de fundamental importância para a realização deste trabalho. O primeiro é o *GE Orion Context Broker* para processamento dos dados e o segundo é o GE *IDAS* que permite gerenciar os dados vindos de sensores.

Figura 5 – Cenário FIWARE.



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

2.4.1 Orion Context Broker

O *Orion Context Broker* é um componente que realiza operações centrais no ecossistema FIWARE. Atua como uma interface para que os desenvolvedores de aplicativos FIWARE possam obter informações de contexto, além de poder registrar entidades e atributos que representam o estado atual de determinados ambientes. Em cenários de *IoT*, ele lida com todas as entidades de contexto que representam os dispositivos de *IoT* e suas informações (ARAUJO *et al.*, 2019).

O *Orion Context Broker* usa a implementação do padrão *NGSI REST* que permite o uso de dados de contexto e a assinatura de aplicativos. O conceito principal do *Context Broker* é que o produtor dos dados pode gerar informações e armazená-lo sem um conhecimento prévio dos usuários ou do aplicativo que usará os dados. Esse componente é capaz de lidar com informações em grande escala através da implementação *APIs REST* padrão. Além disso, permite que os desenvolvedores gerenciem todo o ciclo de vida das informações de contexto, incluindo atualizações, consultas, registros e assinaturas (GÓMEZ *et al.*, 2019). Este componente será utilizado neste trabalho por permitir o processamento dos dados de contexto obtidos a partir dos sensores de saúde e por ser o principal componente da plataforma FIWARE para o gerenciamento das informações.

2.4.2 IDAS

O *IDAS* é um componente do FIWARE que fornece funcionalidades para conectar dispositivos físicos a outros componentes da plataforma FIWARE. Além disso, este GE inclui o gerenciamento de entidades de contexto relacionadas à *IoT*, gerencia as conexões e fornece aos integradores de *IoT* a capacidade de transformar modelos de dados específicos de dispositivos em modelos de dados compreendidos pelos outros componentes da plataforma (FERREIRA *et al.*, 2017).

O IDAS oferece módulos denominados *IoT Agent* que são softwares responsáveis por converter protocolos de dispositivos *IoT* específicos, como LWM2M/COAP, MQTT e SIGFOX para as chamadas NSGI que permitem a comunicação com outros FIWARE GEs. O *IoT Agent* representa uma camada de abstração entre os dispositivos e a plataforma FIWARE, oferecendo suporte a diferentes maneiras de se comunicar com os dispositivos para produzir dados de contextos que são baseados nas informações de leituras feitas pelos sensores (OLIVEIRA *et al.*, 2018). Neste trabalho, a utilização deste componente será de extrema importância por possibilitar que a solução aceite diferentes tipos de sensores, mesmo que trabalhe com protocolos que não são nativos do FIWARE.

3 TRABALHOS RELACIONADOS

Diversas são as aplicações que utilizam a tecnologia *blockchain* para o gerenciamento de dados médicos. Os dados compartilhados em uma rede *blockchain* variam de acordo com a proposta da aplicação, por exemplo dados gerados por sensores de sinais vitais (JAMIL *et al.*, 2020) e imagens médicas (PATEL, 2019). Ao investigar a literatura para discutir o tema de *blockchain* aplicada à saúde, foram coletados trabalhos com foco em compartilhamento de dados médicos provenientes tanto de sensores, como também de dados de saúde em geral. Apesar deste trabalho ter o foco em compartilhamento de dados gerados por sensores, os demais trabalhos que utilizam a *blockchain* como uma ferramenta para compartilhamento de dados também são aproveitados, pois as características dadas a essas informações são também utilizáveis em dados de sensores, como rastreabilidade, privacidade e imutabilidade, para citar alguns deles.

A seguir serão demonstrados os trabalhos organizados em duas subseções. Na Subseção 3.1 são apresentados os trabalhos relacionados que utilizaram dados de sensores e na Subseção 3.2 trabalhos que lidaram com compartilhamento de dados gerais. Ao final, na Subseção 3.3 serão apresentados comparações entre os trabalhos.

3.1 Compartilhamento de dados provenientes de sensores

3.1.1 Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals

No artigo de Jamil *et al.* (2020) os autores citaram que ao compartilhar informações médicas, a segurança dos dados são requisitos essenciais para a interação e coleta de registros médicos eletrônicos. No entanto, é difícil para os sistemas atuais atender a esses requisitos, por conta de políticas de segurança e estruturas de controle de acesso inconsistentes. Por causa disso, foi proposto uma plataforma para uma sistema IoT descentralizado para a área de saúde.

A plataforma proposta é baseada em uma rede *blockchain* permissionada e aborda os desafios como segurança de dados, gerenciamento de identidades e escalabilidade. A arquitetura proposta estabelece comunicação entre os dispositivos físicos de saúde, o servidor IoT e a rede *blockchain*. Foi implementado um estudo de caso no qual o paciente está equipado com sensores para monitorar sinais vitais. Para isso, foram utilizados os seguintes tipos de sensores: sensor ECG, sensores de pressão do sangue, sensores EMG, sensores SPo2, sensores

de temperatura corporal, dentre outros. Um Raspberry Pi foi usado para atuar como um gateway IoT, encaminhando os dados de sinais vitais para um servidor IoT de saúde.

O sistema proposto é projetado e desenvolvido usando *Hyperledger Fabric*, utilizando *chaincodes* para permitir que as aplicações interajam com a rede. O principal problema apresentado no trabalho está relacionado a impasses na comunicação entre o servidor e os dispositivos físicos, que pode ocasionar problemas de segurança. O sistema *blockchain* proposto é tolerante a falhas e confiável, mas no caso da rede IoT, o servidor deve ser configurado para detectar a falha dos nós.

3.1.2 Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications

Segundo os autores Liang *et al.* (2017) o compartilhamento seguro de dados pessoais de saúde é crucial para melhoria da interação e colaboração do setor de saúde. Por conta dos possíveis problemas de privacidade e vulnerabilidades existentes nos atuais sistemas de armazenamento, uma solução foi proposta para o compartilhamento de dados de saúde centrado no usuário e baseado em *blockchain* permissionada. Para isso, foi usado um esquema de formação de canal para melhorar o gerenciamento de identidade usando o serviço de associação suportado pela *blockchain* permissionada *Hyperledger Fabric*.

Foi implementado um esquema de controle de acesso utilizando o componente de serviço de associação (do inglês *Member Service Provider*, MSP) do Hyperledger Fabric com canais de comunicação. Em relação a privacidade do sistema, o usuário pode compartilhar dados de saúde de forma seletiva, com base na necessidade de como os dados pessoais são necessários para auxiliar o serviço de saúde.

No trabalho que está sendo discutido nesta subseção a rede *blockchain* está sendo utilizada para algumas finalidades, por exemplo para o armazenamento dos dados gerados por sensores e os dados provindos da própria assistência médica. Além disso, são gerados códigos *hashs* desses dados e armazenados na *blockchain* para garantir a integridade dos dados.

O sistema foi avaliado testando-se diferentes números de registros simultâneos com uma ferramenta de *benchmark* própria. A partir disso, pode-se concluir que o sistema pode lidar com um grande conjunto de dados em baixa latência, o que indica a escalabilidade e eficiência do processo de dados. No entanto, no sistema proposto não foi utilizado um *middleware* para o tratamento da interoperabilidade e tratamento dos dados vindo dos sensores que pode ocasionar

problemas relacionados a disponibilidade e interoperabilidade dos dados.

3.2 Compartilhamento de dados em geral

3.2.1 A Novel Blockchain-Based Integrity and Reliable Veterinary Clinic Information Management System Using Predictive Analytics for Provisioning of Quality Health Services

Os autores Iqbal *et al.* (2021) apontaram que existem dificuldades no gerenciamento de dados de saúde. Os sistemas de Prontuário Médico Eletrônico (do inglês *Electronic Medical Record*, EMR) existentes não são úteis para atender questões críticas de um processo médico, porque esses sistemas não têm uma estrutura consistente e confiável para políticas de segurança e confiabilidade de dados. Por isso, os autores desenvolveram uma plataforma segura e confiável para aumentar a segurança dos dados e o acesso autorizado às informações médicas sob a privacidade dos regulamentos governamentais.

Como objetivo foi proposto um sistema para gerenciamento de informações veterinárias, baseado em *blockchain* e técnicas de aprendizado de máquina. O RIVIMS, nome da solução proposta, consiste em dois módulos principais: gerenciamento de informações veterinárias seguras com base em *blockchain* e módulos de análise preditiva.

No primeiro módulo um sistema de gerenciamento de informações baseado em *blockchain* é desenvolvido usando o Hyperledger Fabric. Além disso, um contrato inteligente para inserção de dados usando a estrutura de *blockchain* permissionada e módulos de análise preditiva são implementados. Os módulos de predições visam analisar dados de consultas de pacientes em clínicas veterinárias, a fim de descobrir padrões subjacentes e construir modelos de previsões robustas usando algoritmos de aprendizado de máquina.

Para avaliação de desempenho do sistema foi utilizado o *Hyperledger Caliper* usado como uma ferramenta de *benchmark* para avaliar o desempenho do sistema (transações por segundo, taxa de transações com sucesso, rendimento de transação e latência de transação).

3.2.2 MedRec: Using Blockchain for Medical Data Access and Permission Management

Os autores Azaria *et al.* (2016) apontam que os registros médicos precisam passar por inovação e afirmam que os pacientes deixam os dados espalhados por várias servidores. Ao fazer isso, eles perdem o controle de acesso aos seus dados. Por isso, foi proposto um sistema chamado MedRec que é uma estrutura baseada em *blockchain* para armazenar registros médicos

eletrônicos. O trabalho está baseado em uma rede *peer-to-peer*, bem como integra contratos inteligentes por meio da plataforma *Ethereum*, a partir do consenso não permissionado. Assim, é possível gerenciar e rastrear as transições de estados dos ativos na rede.

Na solução proposta, o conteúdo do bloco representa a propriedade dos dados e as permissões de visualização compartilhadas por membros de uma rede privada. Através dos contratos inteligentes da rede *blockchain Ethereum* são registrados relacionamentos entre os provedor e os pacientes que associam um registro médico com permissões de visualização e instruções de recuperação de dados. Na *blockchain* é incluído um *hash* criptográfico para garantir a integridade dos dados. Os provedores podem adicionar um novo registro associado a um paciente específico e os pacientes podem autorizar o compartilhamento de registros entre os provedores.

Em relação as limitações, a proposta não apresenta tratamentos relacionados a privacidade dos pacientes, uma vez que, os autores não consideram fortemente esse aspecto. O sistema *MedRec* não afirma abordar a segurança de bancos de dados, isso ainda deve ser gerenciado adequadamente pelo administrador do sistema local.

3.2.3 A framework for secure and decentralized sharing of medical imaging data via blockchain consensus.

No trabalho do autor Patel (2019) é proposto uma estrutura onde pacientes podem compartilhar imagens médicas de forma segura e controlada. A base para a implementação da rede é baseada na estrutura *Image Share Network* (ISN), da Rede Nacional de Radiologia Norte-americana. A estrutura ISN é utilizada como apoio para a construção da proposta do trabalho, através das análises dos problemas apresentados por essa rede centralizada de compartilhamento.

O objetivo do trabalho é registrar uma lista de estudos e uma lista dos pacientes aos quais esses estudos pertencem. Dessa forma, o paciente será responsável por definir com quem deseja compartilhar seus dados. A *blockchain* que é implementada para o trabalho prosposto utiliza o algoritmo de consenso *Proof of Stake* e algoritmos de criptografia de chave pública para fazer a validação das transações e possibilitar que a rede seja mais confiável. Ao ser utilizado o algoritmo *PoS* obtém-se a vantagem em relação a baixa carga gerada na rede, possibilitando menos atrasos nas interações realizadas com a *blockchain*.

Desse modo, é apresentado uma alternativa para a implementação de uma ferramenta que certifique o compartilhamento de imagens médicas de forma confiável e sem adulterações.

Apesar disso, é alertado aos pesquisadores que desejam reutilizar o método proposto, sobre a necessidade de atentar-se a privacidade dos dados compartilhados, porque a proposta do trabalho não é eficaz quanto a esse requisito e que é importante para os sistemas de saúde.

3.3 Sumário e Comparação dos Trabalhos

Para discutir e comparar as principais aspectos de cada trabalho foi elaborado o Quadro 1. As características que foram utilizadas para realizar a comparação implicam diretamente no compartilhamento de dados quando uma solução utiliza a *blockchain* como um meio de compartilhamento de informações. Além disso, com base nos trabalhos coletados foi possível realizar comparações com a solução proposta.

3.3.1 Descrição do Quadro de Comparação

Existem cinco características avaliadas no Quadro 1. A primeira característica são os ativos, esses estão relacionados ao tipo de informação que está sendo gerenciado pelo sistema, por exemplo: dados de sensores, registros eletrônicos médicos, imagens, dentre outros. A segunda caraterística é o método de armazenamento, onde será definido qual tecnologia está sendo usada como uma solução de armazenamento. A terceira característica é a plataforma de implementação *blockchain*, essa característica refere-se a plataforma que foi utilizada para o desenvolvimento da rede *blockchain*, como por exemplo: *Ethereum*, *Hyperledger*, dentre outros. A quarta característica é o tipo de *blockchain* utilizada relacionado ao modelo de permissão. E por fim, a plataforma de comunicação IoT, essa é responsável por fazer o gerenciamento de dados obtidos pelos sensores e encaminhá-los para os outros componentes da solução.

3.3.2 Relação entre os Trabalhos

Nos trabalhos dos autores Jamil *et al.* (2020) e Liang *et al.* (2017), apresentados nas Subseções 3.1.1 e 3.1.2 respectivamente, são encontradas limitações relacionadas à utilização de uma plataforma responsável por realizar a comunicação e gerenciamento dos dispositivos IoT. Apesar disso, esses trabalhos se relacionam com a solução proposta por trabalhar com o gerenciamento de dados gerados por sensores e também utilizar o método de armazenamento como sendo a *blockchain* e a plataforma de implementação de livro-razão distribuída como sendo a plataforma *Hyperledger*. O trabalho de Iqbal *et al.* (2021) compara-se a solução proposta

Quadro 1 – Comparacação entre os trabalhos

Trabalho	**Ativos**	**Método de Armazenamento**	**Plataforma de Implementação**	**Tipo de *Blockchain***	**Plataforma de Comunicação IoT**
(JAMIL *et al.*, 2020)	Dados de Sensores	*Blockchain*	Hyperledger	Permissionada	Nenhuma
(LIANG *et al.*, 2017)	Dados de Sensores	*Blockchain*	Hyperledger	Permissionada	Nenhuma
(IQBAL *et al.*, 2021)	Dados veterinários	*Blockchain*	Hyperledger	Permissionada	Não se aplica
(AZARIA *et al.*, 2016)	Registro Médico Eletrônico	*Blockchain*	Ethereum	Não permissionada	Não se aplica
(PATEL, 2019)	Imagens	*Blockchain*	Implementação Própria	Não permissionada	Não se aplica
Solução Proposta	Dados de Sensores	*Blockchain*	Hyperledger	Permissionada	Plataforma FIWARE

Fonte: elaborado pelo autor.

por utilizar a plataforma *Hyperledger* para implementação da solução. No entanto, não utiliza plataforma de comunicação IoT por não está gerenciando dados de sensores.

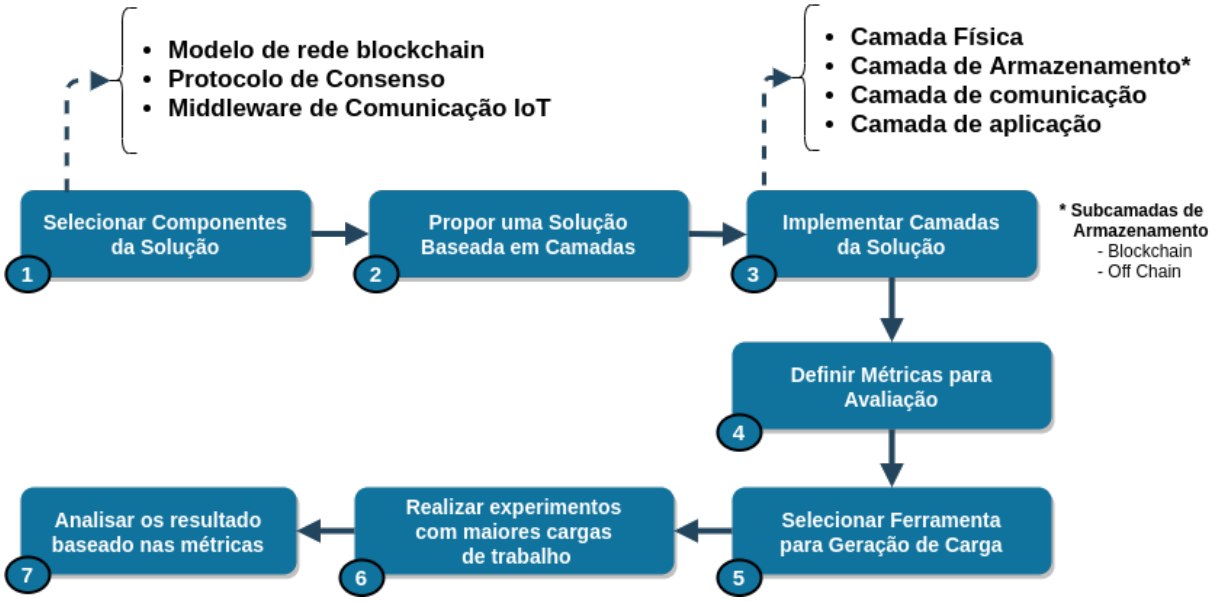
Por fim, os trabalhos de Patel (2019) e Azaria *et al.* (2016) apresentam vulnerabilidades que podem deixar os sistemas médicos sob risco de privacidade por utilizar *blockchain* pública. No entanto, esses trabalhos estão diretamente relacionados com a solução proposta por utilizar a *blockchain* como uma solução de compartilhamento e também usar dados médicos como sendo os ativos.

Por fim, a solução proposta utiliza o ecossistema de *blockchain* permissionado *Hyperledger* para implantação de uma rede permisisonada privada e controlada em relação à participação de organizações e pessoas. Além disso, é usada uma base de dados *off-chain* para armazenamento de dados que não deverão ser armazenados na rede *blockchain*, como por exemplo a grande quantidade de dados vindos dos sensores. Também o protocolo RAFT é utilizado por ser disponibilizado e recomendado pela plataforma *Hyperledger* a partir da versão 1.4.1. A plataforma FIWARE é utilizada para atuar como um *middleware* de comunicação entre o protótipo IoT e o ponto inteligente para escolha de armazenamento de dados. Apesar desse *middleware* de comunicação ser desenvolvido para cidades inteligentes, também é possível a sua implementação em cenários *E-health*, por se tratar de uma plataforma genérica e disponibilizar uma série de componentes para gerenciamento e controle de dados de contexto.

4 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo serão apresentados os passos necessários para a execução deste trabalho. As oito seções a seguir representam as etapas de desenvolvimento do projeto, organizados da seguinte forma: na Seção 4.1, é explicado sobre a escolha dos componentes para a implementação da solução, como os detalhes do protótipo *IoT*, a rede *blockchain* utilizada, o protocolo de consenso, o *middleware* de comunicação *IoT* e a aplicação *web* para monitoramento dos dados; na Seção 4.2 é mostrado uma visão geral do modelo baseado em camadas da solução; na Seção 4.3 é explicado como foi realizado o desenvolvimento das camadas; na Seção 4.4 são definidas as métricas para avaliação da solução; na Seção 4.5 é apresentado a ferramenta para geração de carga de trabalho; na Seção 4.6 são mostrados como serão realizados os experimentos a partir da ferramenta de geração de carga escolhida; na Seção 4.7 é feita a análise dos resultados dos experimentos.

Figura 6 – Diagrama de Fluxo dos Procedimentos Metodológicos.



Fonte: Elaborado pelo autor.

4.1 Selecionar Componentes da Solução

Inicialmente, para o desenvolvimento deste trabalho foi feita a seleção das tecnologias e componentes baseando-se nos problemas apresentados. Em relação a parte física da solução, como sensores e placas desenvolvimento *IoT*, foi pesquisado na literatura e no mercado os principais dispositivos que fossem capazes de realizar aferições do estado de saúde dos

pacientes, levando em conta também os custos do protótipo *IoT*. Com isso, foram selecionados dois componentes capazes de realizar a aferição de variáveis de saúde. O primeiro foi o módulo *ECG AD8232*, que é responsável por avaliar a atividade elétrica do coração e o segundo foi o sensor *MAX30100*, este permite analisar a taxa de oxigênio no sangue e os batimentos por minuto do coração (BPM). Considerando também a aplicabilidade e custos para a utilização do módulo de processamento dos dados e comunicação foi escolhido o microcontrolador ESP8266 integrado a plataforma *NodeMCU*.

Em relação a tecnologia responsável por realizar a comunicação do protótipo *IoT* com as demais partes da solução a plataforma FIWARE mostrou-se como uma opção para esta funcionalidade. Essa tecnologia foi escolhida por ser de código livre e por está impulsionando os principais padrões de tecnologias, inclusive no setor de saúde. Além de disponibilizar um conjunto universal de padrões para gerenciamento de dados de contexto que facilitam o desenvolvimento de soluções inteligentes para diferentes domínios.

Sobre as soluções voltadas para o armazenamento dos dados foram adotadas as tecnologias *blockchain* e o *MySQL*. A *blockchain* foi selecionada como uma alternativa de armazenamento de dados por proporcionar características importantes aos dados de saúde, por exemplo: descentralização e rastreabilidade. O modelo de *blockchain* adotado foi a permissionada privada, pois com esse modelo é possível ter um maior controle do acesso aos dados dos pacientes.

Dentre os modelos de *blockchains* permissionadas a plataforma *Hyperledger Fabric* foi a utilizada para implementação da solução, por ser o livro-razão mais desenvolvido do projeto *Hyperledger* e oferecer diversas ferramentas, *frameworks* e serviços para o desenvolvimento de aplicações descentralizadas. Além da *blockchain*, também foi selecionado um banco de dados para armazenar o grande volume de dados gerados pelos sensores, devido aos custos de manter a cadeia de blocos quando esta é submetida a grandes quantidades de dados. Para isso, foi selecionado o *MySQL* por permitir a manipulação de grandes volumes de leituras e escritas simultâneas sem conflitos.

Em uma rede *blockchain* uma das principais variáveis a ser analisada para o funcionamento da rede é o protocolo de consenso que é responsável pela validação dos blocos. Para a rede *blockchain* utilizada neste projeto foi aplicado o protocolo de consenso *RAFT*, por ser o recomendado pela plataforma *Hyperledger* desde a versão 1.4.1, além de ser mais simples a sua implantação em relação aos outros protocolos.

E por fim, foi feito a seleção da tecnologia que possibilitará o desenvolvimento de uma aplicação *web* capaz de mostrar para os usuários do sistema os dados de saúde em uma interface intuitiva e dinâmica. O *framework VueJs* foi utilizado para a construção dessa aplicação por possibilitar o uso de componentes que implementam gráficos e *dashboards* para visualização das informações.

4.2 Propor uma Solução Baseada em Camadas

Em relação ao modelo de arquitetura do sistema foi implementada uma solução baseada em camadas, sendo que cada camada corresponderá aos principais serviços oferecidos pela proposta da solução deste trabalho. As camadas são: camada física, camada de comunicação, camada de armazenamento e camada de aplicação. Esse modelo foi utilizado por permitir a modularização dos componentes da solução.

A camada física está relacionada aos componentes físicos que contribuirão para a implementação da solução, que serão responsáveis pela geração das cargas de trabalho. Nessa camada estarão os sensores de saúde, a placa de processamento dos dados e a definição de protocolos *IoT*.

A camada de comunicação é a responsável por realizar a comunicação do protótipo *IoT* e um *endpoint* inteligente para realizar o armazenamento dos dados. Nesta camada foi definido o *middleware* de comunicação e os seus respectivos protocolos. Além disso, serão especificados os subcomponentes utilizados pelas tecnologias implantadas nesta camada. Esta camada foi implementada para prover escalabilidade do sistema, tornando o sistema mais dinâmico e capaz de operar com diferentes quantidade de sensores e/ou atuadores.

A camada de armazenamento divide-se em duas subcamadas: *off-chain* e *blockchain*. A camada *off-chain* é responsável por armazenar a maioria dos dados provindos dos sensores e a subcamada *blockchain* responsável por armazenar anomalias dos sinais vitais e médias de valores dos sinais vitais. Por fim, a camada de aplicação. Esta é responsável por disponibilizar uma aplicação *web* capaz de proporcionar a visualização dos dados para as partes interessadas de uma forma mais amigável e compreensível.

4.3 Implementar Camadas da Solução

A implementação de cada camada foi baseada no que foi discutido na Seção 4.1. Para a camada física foi construído um protótipo *IoT* para leitura dos sinais vitais. As variáveis de saúde que serão analisadas, serão: batimentos por minuto do coração (BPM), taxa de oxigênio no sangue e atividade elétrica do coração, com o sensor *MAX30100*, para as duas primeiras variáveis, e o módulo *AD8232* para a terceira variável, respectivamente. O módulo *ESP8266* foi utilizado para o processamento dos dados e realização da comunicação com o *middleware*. Os sensores serão dispostos em um paciente e após serem realizados as aferições do seu estado, os dados serão processados e encaminhados para a camada de comunicação.

A camada de comunicação foi implementada com a plataforma FIWARE. Esta plataforma fornece microserviços para o gerenciamento de dados de contexto das informações geradas pelos sensores. Os microserviços utilizados da plataforma foram concedidos pelos seguintes componentes do FIWARE: *Orion Context Broker*, componente responsável por fazer o gerenciamento dos dados de contexto e o *IoT Agent* que permite a comunicação de dispositivos físicos que trabalham com diferentes protocolos. Sendo assim, um grupo de dispositivos são capazes de enviar enviar seus dados e o *Orion Context Broker* pode realizar o processamento das informações com protocolos nativos.

É possível a comunicação direta entre os dispositivos físicos e a plataforma FIWARE, no entanto, em *IoT* é viável a utilização de protocolos específicos para esta área para possibilitar que as soluções sejam mais escaláveis e sem dependências entre quem gera e quem recebe os dados. Como é o caso do protocolo *MQTT* que permite a comunicação com publicações e assinaturas de tópicos. Dessa forma, foi utilizado o *broker Mosquitto* para permitir a comunicação via protocolo *MQTT* entre os dispositivos físicos e o componente *IoT Agent*. Após os dados serem processados pela plataforma *FIWARE*, as informações serão encaminhadas para um *endpoint* inteligente para realizar a inserção dos dados na camada de armazenamento.

Para a implementação das subcamadas de armazenamento foi utilizada a plataforma *Hyperledger Fabric* para a subcamada *blockchain* e o banco de dados *MySQL* para armazenamento do grande volume de dados gerados pelos sensores. Essa divisão é importante, pois existem preocupações relacionadas à *blockchain* quanto a capacidade de lidar com um grande volume de transações em baixa latência. A construção da rede *Hyperledger Fabric* foi feita através da definição de organizações e subcomponentes que representarão as partes interessadas das instituições de saúde, onde o acesso ao livro-razão foi controlado através da definição do

contrato inteligente que controlará as operações de escritas e leituras entre os membros da rede.

A camada de aplicação foi desenvolvida em *VueJs* com intuito de exibir informações para os usuários. Essas informações serão mostradas através de *dashboards* para os dados atuais do paciente e também gráficos de barras e linhas para visualização do histórico de dados vitais dos pacientes.

4.4 Definir Métricas para Avaliação

A solução proposta foi avaliada com intuito de verificar o seu estado quando submetido a diferentes cenários de cargas de trabalho. Para isso, as variáveis escolhidas foram definidas com intuito de avaliar a escalabilidade do sistema. Dessa forma, a aferição do estado do sistema esteve voltado a variação da quantidade de dispositivos definido em cada experimento. Sendo assim, a alternância de valores dessa variável impacta de forma significa, como por exemplo a quantidade de mensagens que serão tratadas pelo sistema. Nesse sentido, a variável escolhida para verificar como a solução respondeu a variação de dispositivos foi o tempo necessário que uma mensagem gerada pelo sensores levou para ser inserida na camada de armazenamento.

4.5 Selecionar Ferramenta para Geração de Carga

Para geração de diferentes cargas de trabalho foi escolhido um simulador capaz de simular e replicar diferentes quantidades de sensores. O simulador *Simulator Environment Sensor* (*SenSE*) foi o escolhido para realização dessa atividade. Com essa ferramenta é possível configurar a quantidade de dispositivos por experimento, a periodicidade de envio de mensagens e o tempo de realização de cada experimento.

O *SenSE* é uma ferramenta capaz de gerar dados sintéticos de sensores. É um software de código aberto e genérico desenvolvido para simular ambientes complexos, por exemplo cenários *E-health*. Além disso, é possível gerar uma grande quantidade de dados de sensores heterogêneos de forma simultânea, sendo possível que dezenas de sensores possam gerar carga de trabalho para avaliação do desempenho de sistemas.

4.6 Realizar Experimentos com Diferentes Cargas de Trabalho

Os experimentos da solução desenvolvida foram realizados em duas categorias: experimentos reais e experimentos simulados. Nos experimentos reais foram utilizados os

sensores *MAX30100*, o Módulo *AD8232* e a placa *NodeMCU*. Nesta categoria de experimentos os sensores foram dispostos em um indivíduo para a realização de experimentos com intervalos de tempos definidos para avaliação do funcionamento dos dispositivos e validação de comunicação com o sistema. Nessa categoria não foi realizado experimentos de longa duração para avaliação de desempenho ou escalabilidade da solução, mas foi realizado apenas para verificação de possibilidade de comunicação dos dispositivos físicos com o sistema.

Já em relação aos experimentos simulados foi utilizado o simulador *SenSE* para geração de cargas. Foram realizados replicações dos experimentos, onde foram variados a quantidade de sensores para simular a variação de indivíduos que utilizaram o sistema. A configuração da geração de carga foi baseada no funcionamento de uma instituição hospitalar, onde cada sala possui uma determinada quantidade de pacientes e dispositivos físicos, que estão diretamente relacionadas ao número de pessoas. Para as simulações foi considerado também a realização de aleatoriedade dos experimentos, com intuito de considerar a interferência externa do sistema, relacionados a *internet* por exemplo.

4.7 Analisar os Resultados Baseado nas Métricas Definidas

Nesta etapa foi realizada a análise dos resultados obtidos dos experimentos. Com os valores obtidos dos tempos que foram necessários para que as mensagens fossem processadas por todos as camadas da solução, foram realizados comparações desses resultados. Dessa forma, é possível obter como o sistema foi impactado com diferentes quantidades de dispositivos e mensagens. A principal ferramenta de análise para as comparações foram a utilização de gráficos. O principal desses foi o *boxplot* por permitir avaliar características importantes do conjunto de dados como dispersão, assimetria e *outliers* (valores discrepantes).

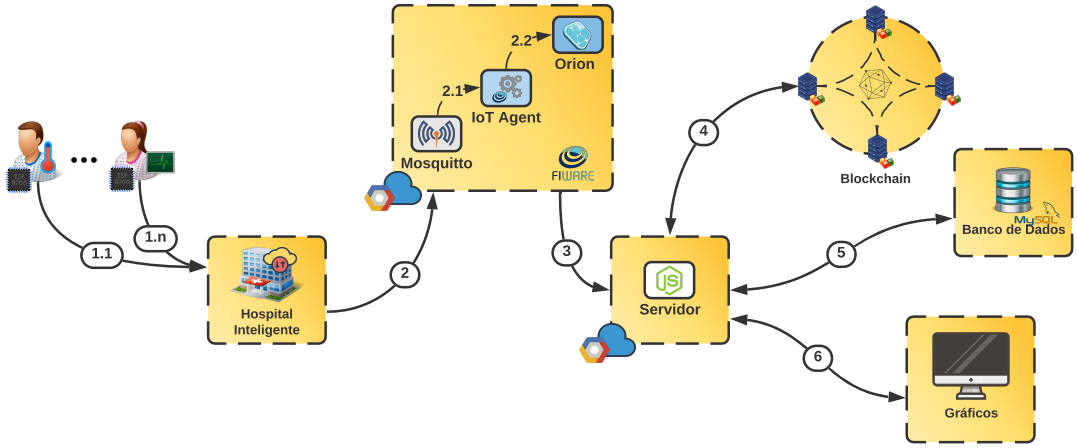
5 MATERIAIS E MÉTODOS

Nesta seção, será descrita a solução baseada em *blockchain* e IoT para o compartilhamento de dados de saúde. Os módulos e componentes da solução que serão apresentados a seguir atuarão em conjunto oferecendo o serviço de compartilhamento de dados de saúde.

5.1 Modelo da Solução Proposta

Este trabalho propõe uma solução para o compartilhamento de dados de saúde baseado em um cenário *IoT*. Na Figura 7, é apresentado o fluxo que define o percurso dos dados. Analisando de forma horizontal, da esquerda para a direita, inicialmente, são apresentados os pacientes que estão conectados a sensores inteligentes para a aferição dos sinais vitais. As setas representadas com *1.1* e *1.n* indicam que n pacientes estão sendo aferidos por sensores de saúde. Os dados gerados são encaminhados para os componentes da solução implantados nos hospitais inteligentes.

Figura 7 – Fluxo de operações da solução.

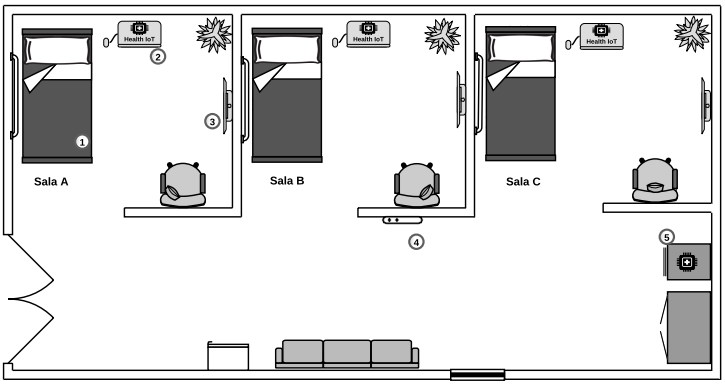


Fonte: Elaborado pelo autor.

Após isso, os dados são encaminhados para os componentes do *middleware* FIWARE (2) para serem processados e enviados para um servidor *NodeJs* (3). Esse servidor atua como um ponto inteligente para escolha de armazenamento *on-chain* (4) ou *off-chain* (5). Além disso, uma aplicação *WEB* recebe subscrições do servidor que atualizam os gráficos e *dashboards* que indicam o estado de saúde dos pacientes.

5.2 O Hospital Inteligente

Figura 8 – Sala dos Hospitais Inteligentes.



Fonte: Elaborado pelo autor.

Na Figura 8, está sendo mostrado um possível cenário de uma sala de hospital inteligente. No item 1, da Figura 8, é apresentado o leito do paciente, que estará conectado ao conjunto de sensores representados pelo item 2. Já o item 3 representa um monitor que estará apresentando uma aplicação *WEB* com os dados de saúde do paciente. Essa organização de componentes é feita para todos os leitos. No item 4, está o componente *WI-FI*, responsável por receber os dados vindos do *kit* de sensores de saúde e encaminhá-los para o servidor que irá processar essas informações, apresentado no item 5.

5.3 Modelo em Camadas da Solução

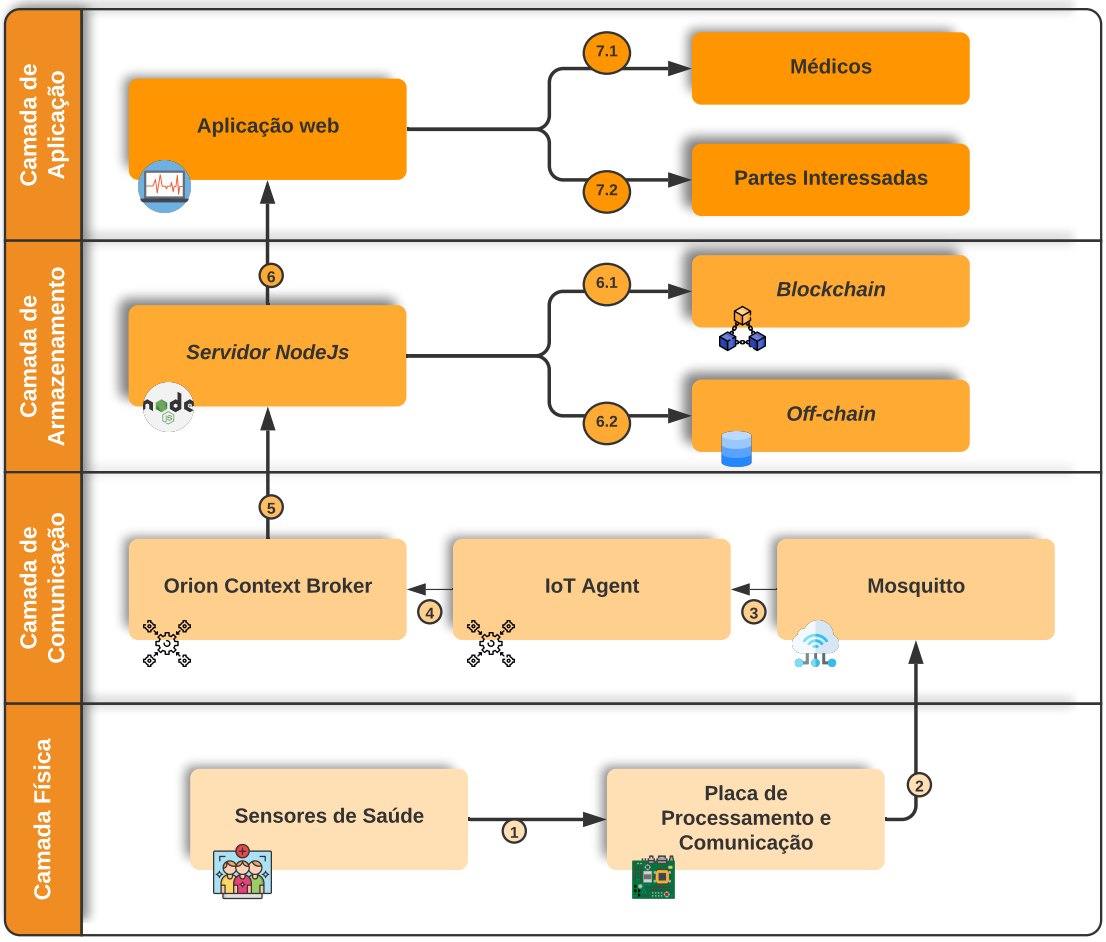
O modelo em camadas proposto para este trabalho é exposto na Figura 9. Realizando uma análise vertical de forma ascendente, temos a primeira camada, chamada de física. Nos blocos apresentados nesta camada, estão os sensores de saúde e a placa de comunicação *IoT*. Em (1), é definido o fluxo de dados gerados pelos sensores que são enviados para a placa de processamento e comunicação *Wi-Fi*. Os componentes físicos adquiridos são: placa de desenvolvimento embarcado com o microcontrolador ESP8266 e os sensores de saúde MAX30100 e o módulo ECG AD2832.

Na segunda camada, intitulada de camada de comunicação, são apresentados os blocos que compõem os componentes do *middleware*, responsável pela comunicação entre o protótipo *IoT* e as camadas superiores. Esses componentes apresentados são os *Generic Enablers* do *middleware* FIWARE que tratam as questões de interoperabilidade e comunicação.

Em (2), é mostrado o fluxo de dados tratado pela placa de desenvolvimento embarcada e sendo enviada para o *Broker Mosquitto*. Este *broker* é utilizado para possibilitar a comunicação *MQTT* através de escrita dos dados nos tópicos desse *broker*. Em (3), é definido o fluxo de dados entre o *Mosquitto* e o componente *IoT Agent*, esse realiza a tradução do protocolo *MQTT* para o padrão NGSI.

Em (4), é apresentado o fluxo de dados entre o *IoT Agent* e o principal componente do FIWARE, denominado *Orion Context Broker*, esse e é responsável por realizar o processamento dos dados e realizar subscrições a um *endpoint* de um servidor *NodeJs*, definido em (5). Após os dados estarem disponíveis no servidor *NodeJs*, é possível realizar três operações. A primeira é alimentar uma aplicação *WEB* para a construção de gráficos e *dashboards*, representado por (6). A segunda é inserir os dados na cadeia de blocos, representado por (6.1). E, por último, armazenar os dados em um banco de dados tradicional, representado por (6.2). Sendo assim, através da aplicação *WEB*, é possível que os médicos (7.1) e as demais partes interessadas (7.2) tenham acesso a esses dados.

Figura 9 – Modelo de Arquitetura em Camadas.

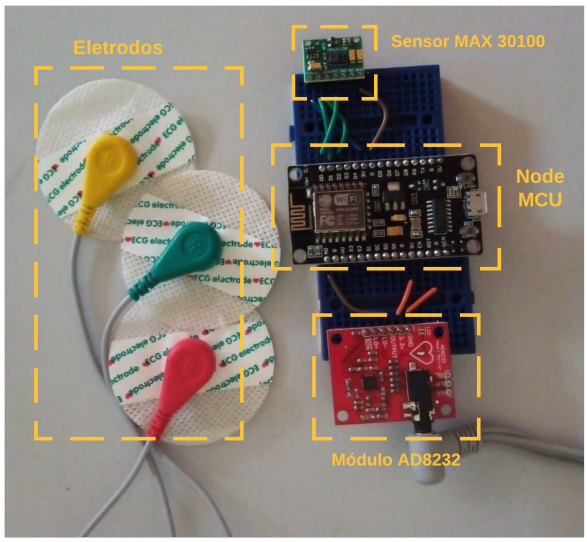


Fonte: Elaborado pelo autor.

5.4 Protótipo IoT

Para a realização dos experimentos, foi construído um protótipo para a aferição das variáveis de saúde dos pacientes. Na Figura 10, é apresentado o protótipo *IoT* com os sensores *MAX30100* e o módulo *AD8232*, sendo o primeiro responsável por aferir a taxa de oxigênio no sangue e o batimento por minuto do coração através da disposição do dedo indicador no *LED* do sensor. Já o segundo sensor é responsável por aferir a atividade elétrica do coração através da fixação dos eletrodos no corpo do paciente. Para o processamento e comunicação com as demais camadas da solução, foi utilizada a placa *NodeMCU*, conforme demonstrado na Figura 10.

Figura 10 – Protótipo IoT.



Fonte: Elaborado pelo autor.

5.5 *SenSE* - Sensor Simulation Envitonment

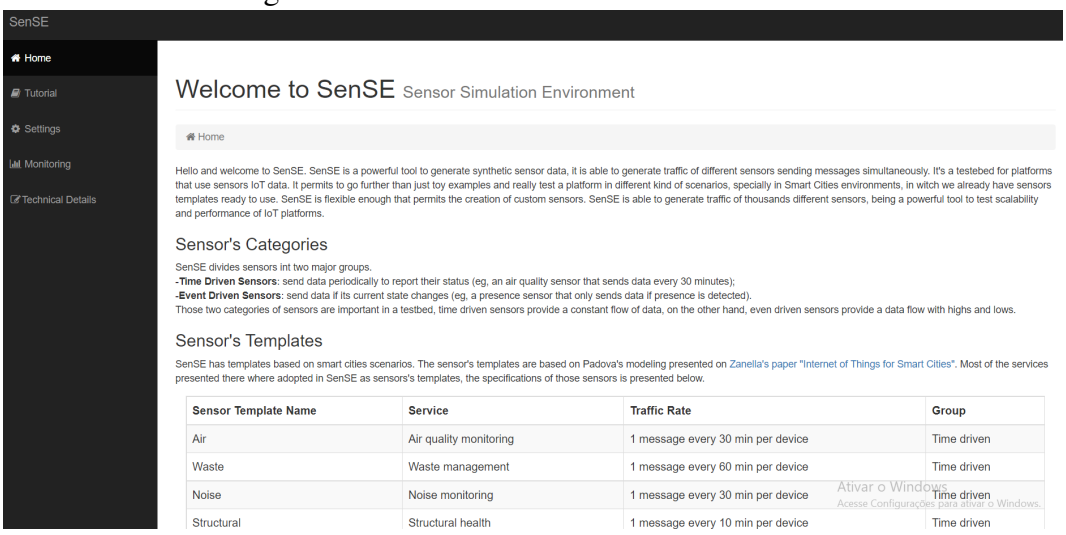
O *SenSE* é uma ferramenta capaz de gerar cargas de trabalhos com o intuito de averiguar a escalabilidade de sistemas que gerenciam dispositivos *IoT*. Neste trabalho, essa ferramenta foi utilizada para simular diferentes sensores de saúde e consequentemente diferentes pacientes. É possível simular dois tipos de sensores, que são eles: sensores movidos por tempo ou evento. O primeiro é caracterizado pelo envio de dados de forma periódica e os sensores movidos por evento enviam dados caso o seu estado atual seja alterado. Como os dados de estado de saúde são simulados e gerados de forma aleatória, os experimentos serão realizados com sensores movidos por tempo para testar a escalabilidade da solução. A utilização dessa ferramenta será de suma importância, pois a geração de carga de trabalho usando sensores físicos

traria um alto custo para o projeto, devido aos preços desses tipos de dispositivos de aferição de saúde.

Na Figura 11, é mostrada a página principal do simulador, na qual são descritas informações sobre o simulador e os tipos de simulações. Na Figura 12, é possível verificar as configurações necessárias para a realização do experimento. Em *MQTT Broker IP address* e *Port*, é definido o local onde será enviada a carga de trabalho. Além disso, é possível definir o nome do experimento, a duração e onde os *logs* serão salvos.

Na Figura 13, pode-se verificar os campos necessários para a realização dos experimentos com sensores movidos por tempo. No campo *type (name)*, é definido o nome do sensor, em *MQTT Topic* é definido o tópico *MQTT*, em que serão feitas as subscrições dos dados, em *Periodicity*, é definido a periodicidade em que os dados serão enviados. E, por último, em *Data Typer*, é permitido definir o tipo de dado que será escrito no tópico *MQTT*. Já *Max Value* e *Min Value* são utilizados quando é necessário definir os limites dos valores dos dados.

Figura 11 – Tela inicial do SenSe

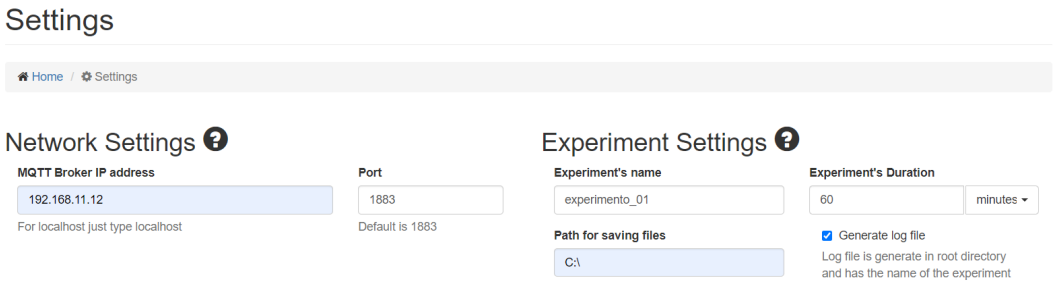


Fonte: Elaborado pelo autor.

5.6 Infraestrutura da Rede *Hyperledger Fabric*

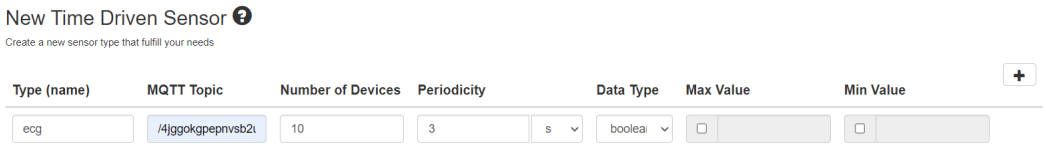
Na Figura 14, é apresentada a infraestrutura da rede *Hyperledger Fabric* construída para a realização dos experimentos. No total foram utilizados sete nós que estão sendo executados em *containers* e estão distribuídos em três máquina virtuais. Essas máquinas estão sendo executadas em servidores presentes na UFC - campus Quixadá executando o sistema operacional *Linux*. Em uma rede *Hyperledger* as organizações (*HLF*) podem ser tão grandes quanto uma

Figura 12 – Exemplo de configuração de experimento de tempo do *SenSE*



Fonte: Elaborado pelo autor.

Figura 13 – Exemplo de configuração de experimentos do *SenSE*.

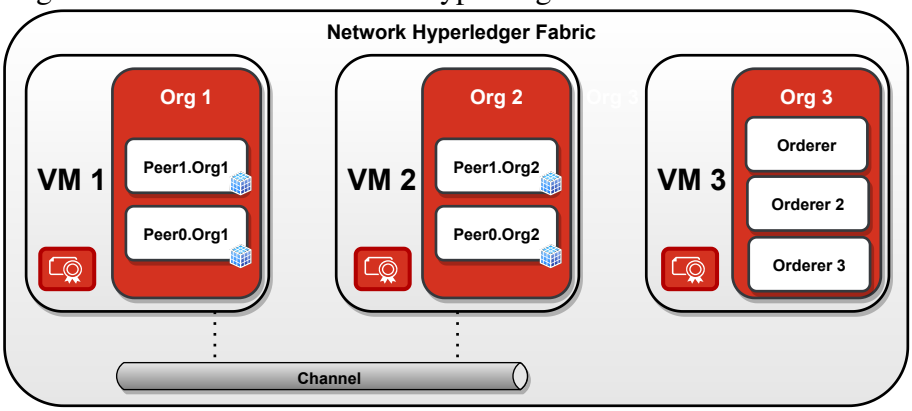


Fonte: Elaborado pelo autor.

corporação multinacional ou tão simples quanto um indivíduo. Com isso, tendo em vista o nível de privacidade em que os dados devem ser tratados, a representação de uma organização da rede *Hyperledger* na solução proposta será o conjunto de indivíduos que terão acesso aos dados de um determinado paciente. Sendo assim, somente os usuários que estiverem autorizados a realizar transações para uma determinada organização da rede *HLF* poderão ter acesso aos dados dos pacientes. Todas as requisições feitas para uma dessas organizações serão assinadas através da disponibilização dos serviços do *HLF*, para que a garantia de privacidade dos dados sejam assegurados e apenas as partes interessadas possam ter acesso aos dados sensíveis.

Cada uma dessas organizações esta sendo executadas em uma máquina virtual. E em cada uma dessas são instanciados *containers docker* que irão executar os componentes da rede Hyperledger, como por exemplo: os nós *peers* que armazenam a cadeia de blocos e os nós *orderes* que irão realizar a validação das transações. Além disso, serão instaciadas as autoridades de certificação para distribuição de certificados digitais para as aplicações que desejarem se associar as organizações. Na infraestrutura implementada é também utilizado um canal de comunicação que possibilita a comunicação entre todas as organizações.

Figura 14 – Infraestrutura Rede Hyperledger.



Fonte: Elaborado pelo autor.

5.7 Contrato Inteligente

Na Figura 15, é demonstrado o contrato inteligente desenvolvido em *Go* que foi implantado na rede *Hyperledger Fabric*. Com esse *chaincode*, denominação de contrato inteligente na rede *Hyperledger*, é possível realizar operações que possibilitam aos usuários executar escritas e leituras no *ledger*. Os dados que serão armazenados na rede está sendo demonstrado na *struct* da Figura 15, que são as seguintes variáveis: BPM, *Oximeter* e ECG. A seguir serão descritos os métodos desenvolvidos no *chaincode*.

- ***initLedger*:** Este método é responsável por fazer a primeira operação de escrita na rede, com intuito de verificar se a rede está disponível.
- ***createStatePatient:*** Neste método será possível a inserção do estado de saúde do paciente no banco de dados de estado global.
- **queryStatePatient:** Este método tem a função de realizar a leitura das variáveis de estado de saúde do paciente que já foi armazenado na rede. Considerando que será possível ser acessado apenas as informações que estão no banco de dados de estado global, ou seja, os dados que foram armazenados com o método *createStatePatient*.
- **createPrivateImpliciteOrg1:** Através deste método será possível que os usuários insiram na rede informações que poderão ser acessadas apenas a nível de organização, ou seja, apenas os usuários que estão autenticados em uma determinada organização poderá ter acesso aos dados.
- **queryPrivateImpliciteOrg1:** Através deste método será possível que os usuários pertencentes a uma das organizações recuperem os dados inseridos através do método *createPrivateImpliciteOrg1*.

Figura 15 – Chaincode.

```
type StatePatient struct {
        Oximeter  string `json:"oximeter"`
        Bpm string `json:"bpm"`
        Ecg string `json:"ecg"`
}

func (s *SmartContract) Invoke(APIstub shim.ChaincodeStubInterface) sc.Response {

        function, args := APIstub.GetFunctionAndParameters()

        if function == "initLedger" {
           return s.initLedger(APIstub)
        } else if function == "query" {
           return s.query(APIstub, args)
        } else if function == "create" {
           return s.create(APIstub, args)
        } else if function == "readPrivateImpliciteForOrg1" {
           return s.readPrivateImpliciteForOrg1(APIstub, args)
        } else if function == "createPrivateImpliciteForOrg1" {
           return s.createPrivateImplicitForOrg1(APIstub, args)
        }
        return shim.Error("Invalid Smart Contract function name.")
}
```

Fonte: Elaborado pelo autor.

6 EXPERIMENTOS E RESULTADOS

Neste trabalho foram realizados experimentos para verificar o comportamento da solução com diferentes cargas de trabalho. Para a realização desses experimentos foi implementado a arquitetura proposta baseada na plataforma Hyperledger Fabric. O intuito desses experimentos foi verificar a latência do percurso da mensagem. Esse percurso considera-se que é desde a geração do dados na camada física até a validação da escrita na base de dados *on-chain*. Devido ao alto custo dos sensores para a realização dos experimentos, foi utilizado um simulador para geração da carga de trabalho.

6.1 Configuração dos Experimentos

O Quadro 2 apresenta de forma resumida os experimentos realizados para avaliação da latência. Para a geração da carga de trabalho foi utilizado o simulador *SenSE* que simula sensores enviando pacotes para um tópico *MQTT*. Nesse simulador é possível realizar a configuração de algumas variáveis, como: a quantidade de dispositivos, a periodicidade do envio de mensagens e a duração do experimento.

Quadro 2 – Descrição dos Experimentos

Critérios	**Descrição**
Sistema	Infraestrutura baseada na *blockchain* Hyperledger Fabric
Métricas	Latência
Parâmetros	CPU, memória, quantidade de máquinas virtuais, quantidade de dispositivos, periodicidade e duração do experimento.
Fatores	Configuração do *benchmark*
Carga de Trabalho	Geração de sequências aleatórias de envio de mensagens no *SenSE*, variando a quantidade de dispositivos.
Projeto de Experimentos	**Experimento 1:** geração da carga de trabalho com quantidade de dispositivos = 6, repetida 3 vezes e com 1 hora de duração; **Experimento 2:** geração da carga de trabalho com quantidade de dispositivos = 15, repetida 3 vezes e com 1 hora de duração; **Experimento 3:** geração da carga de trabalho com quantidade de dispositivos = 30, repetida 3 vezes e com 1 hora de duração.

Fonte: elaborado pelo autor.

Neste trabalho foram realizados experimentos baseando-se em um cenário hospitalar, onde cada paciente é equipado com dispositivos com a capacidade de gerar um total de 3 sinais vitais por paciente. Dessa forma, para simular a variação da quantidade de pacientes foram realizados experimentos no *SenSE* com diferentes quantidades de dispositivos para representar diferentes quantidades de pacientes.

Nesse sentido, os experimentos foram configurados para representar a utilização do

sistema por 2, 5 e 10 indivíduos. Sendo assim, a quantidade de sensores simulados em cada experimento foram 6 (2 pacientes x 3 sinais vitais), 15 (5 pacientes x 3 sinais vitais) e 30 (10 pacientes x 3 sinais vitais) dispositivos, respectivamente. Além disso, para cada um desses foram realizadas 3 repetições em dias, turnos e horários distintos para garantia de aleatoriedade dos experimentos. Totalizando em uma quantidade de 9 experimentos e com a duração de 1 hora para cada experimento. No Quadro 3 é resumido a configuração dos experimentos.

Quadro 3 – Configuração dos experimentos

Experimento	**Quantidade de dispotivos**	**Turno**	**Data**	**Duração**
1	6	manhã	09/12/2021 às 05:30hs	1 hora
2	6	tarde	10/12/2021 às 13:30hs	1 hora
3	6	noite	15/12/2021 às 18:30hs	1 hora
4	15	manhã	09/12/2021 às 07:00hs	1 hora
5	15	tarde	09/12/2021 às 15:00hs	1 hora
6	15	noite	08/12/2021 às 20:00hs	1 hora
7	30	manhã	09/12/2021 às 08:30hs	1 hora
8	30	tarde	08/12/2021 às 16:30hs	1 hora
9	30	noite	08/12/2021 às 18:30hs	1 hora

Fonte: elaborado pelo autor.

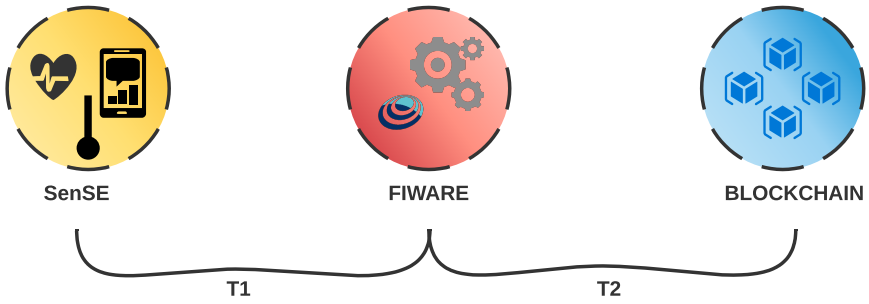
6.2 Avaliação da Latência

Nos experimentos realizados foi analisado o tempo necessário para que uma mensagem gerada no simulador fosse armazenada na camada de comunicação *on-chain*. Para a captura do tempo necessário que a mensagem percorre o caminho completo no sistema foram definidos dois estágios do percurso.

O primeiro é o tempo necessário para que uma mensagem seja gerada no *SenSE* e esta seja tratada pelos componentes do *FIWARE* e fique disponível em um servidor pronta para o armazenamento. O segundo estágio é o tempo necessário para que o dado seja armazenado na *blockchain*. Na Figura 16, T1 representa o tempo necessário para a mensagem percorra o primeiro estágio e T2 representa o tempo necessário para a mensagem percorra o segundo estágio. Dessa forma, após a obtenção das latências encontradas em T1 e T2 foi analisado o

comportamento de T1 + T2 medido em milissegundos.

Figura 16 – Caminho da mensagem



Fonte: Elaborado pelo autor.

6.3 Avaliação de Desempenho

Baseado na avaliação de dois estágios foram realizados experimentos utilizando o simulador *SenSE*. Nesse sentido, durante os experimentos foram gerados diferentes quantidades de mensagens cuja soma apresentou-se diretamente proporcional a quantidade de dispositivos, conforme mostrado no Quadro 4. Inicialmente, notou-se que a quantidade de mensagens variou em decorrência da variação do turno e também devido a variação da quantidade de dispositivos. No entanto, a variação da quantidade de dispositivos ocasionou uma maior variação de quantidade de mensagens quando comparada a variação de turnos. Esse comportamento já era esperado, pois o aumento da quantidade de dispositivos gera uma maior quantidade de mensagens.

Quadro 4 – Quantidade de mensagens por experimento

Quantidade de dispositivos	**Quant. de mensagens (manhã)**	**Quant. de mensagens (tarde)**	**Quant. de mensagens (noite)**	**Média**
6	2154	2157	2157	2156
15	5373	5383	5380	5378
30	7651	7443	7427	7507

Fonte: elaborado pelo autor.

Nas próximas duas subseções serão mostradas as análises de como as latências totais das mensagens foram impactadas em relação a variação de turno e variação de dispositivos.

6.3.1 Variação de turnos

Em relação a variação dos turnos observou-se que a latência foi impactada. No Quadro 5 são mostradas as medianas das latências em milissegundos dos experimentos para cada

turno. Observa-se que houve uma baixa variação da mediana das latências quando os diferentes turnos são comparados para cada quantidade de dispositivos, sendo a maior diferença de latência inferior a 400 ms.

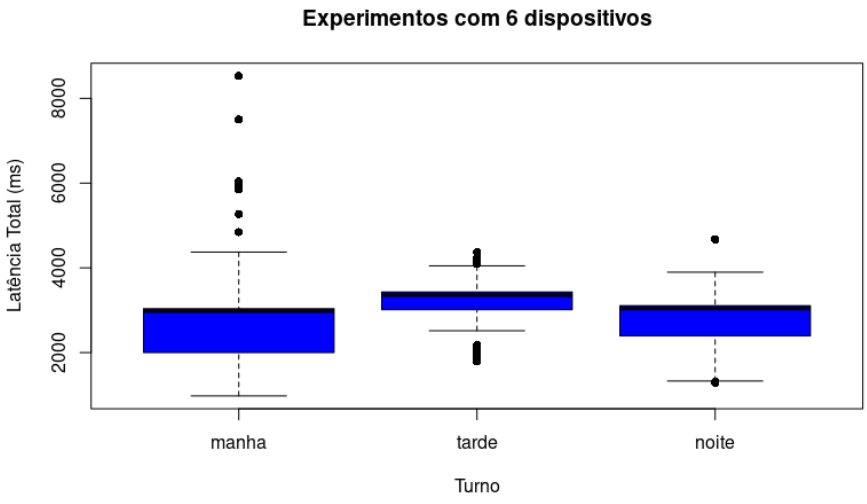
Quadro 5 – Mediana dos turnos

Quantidade de dispositivos	**Manhã**	**Tarde**	**Noite**
6	2978ms	3038ms	3356ms
15	2411ms	2494.5ms	2268ms
30	2770ms	2893ms	2612ms

Fonte: elaborado pelo autor.

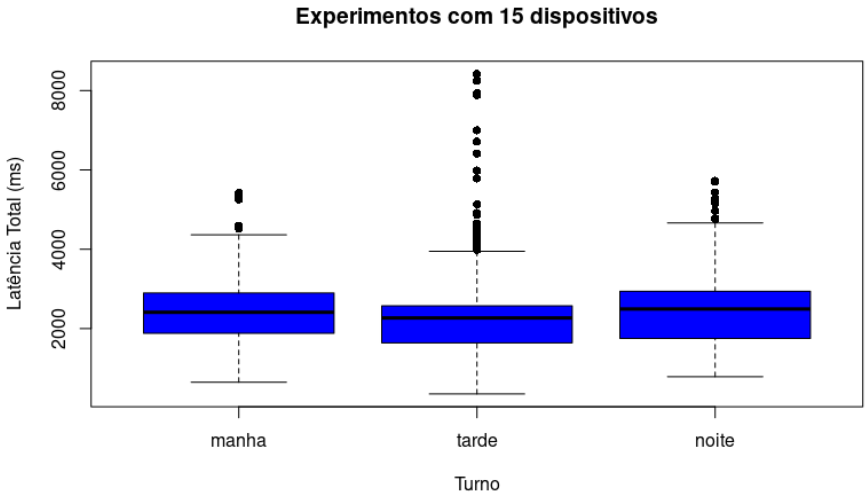
Nas Figuras 17, 18 e 19 são mostrados os valores da latência total dos experimentos com 6, 15 e 30 dispositivos, respectivamente, durante os diferentes turnos. Observa-se que para a maioria dos experimentos durante o turno da tarde houve uma maior ocorrência de *outliers* que possivelmente esteja associado ao uso intenso da rede nesse turno. Essa característica pode ser observada principalmente nas Figuras 18 e 19. Outra observação está associada a dispersão das latências durante o turno da manhã e tarde. Nesses períodos houve uma menor tendência de dispersão, calculada pela subtração do 3º e 1° quartil do gráfico. Em contraste ao período da noite que houve uma maior tendência a dispersão. Essa característica pode ser melhor observada na Figura 20.

Figura 17 – Experimento com 6 dispositivos



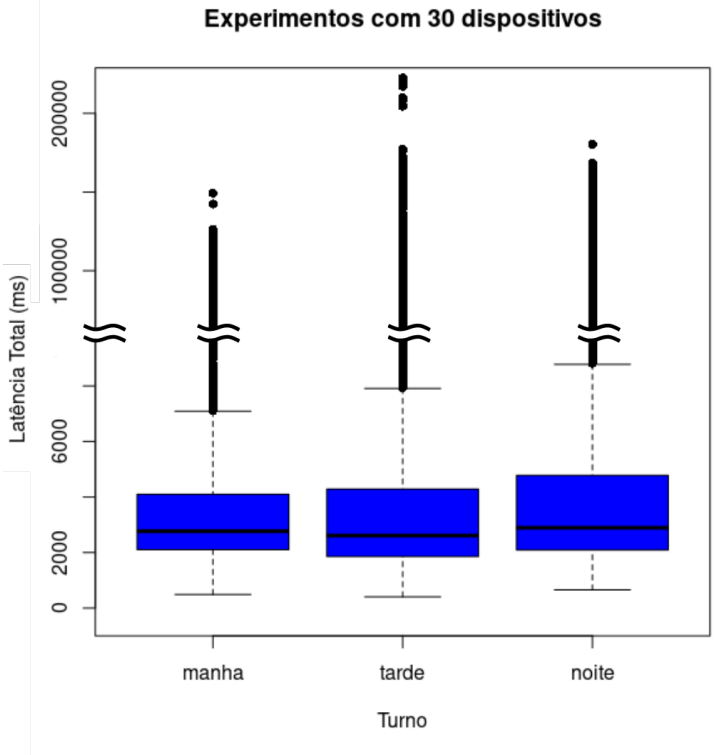
Fonte: Elaborado pelo autor.

Figura 18 – Experimento com 15 dispositivos



Fonte: Elaborado pelo autor.

Figura 19 – Experimento com 30 dispositivos



Fonte: Elaborado pelo autor.

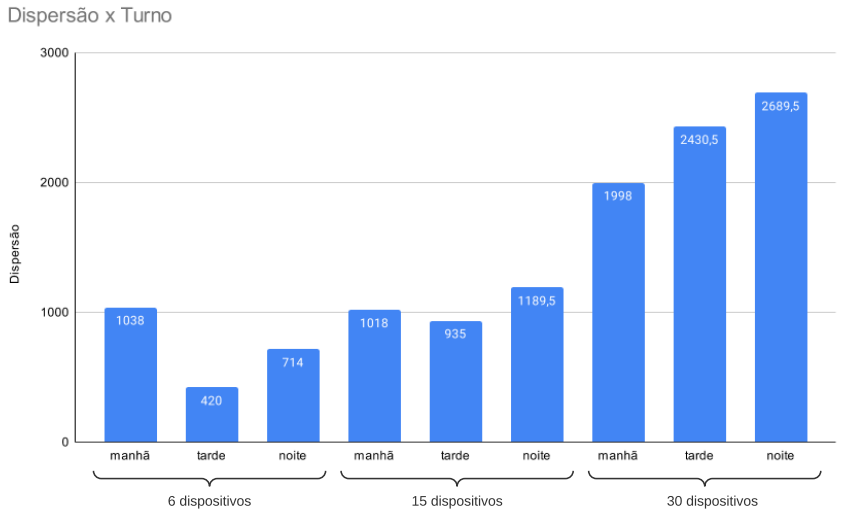
6.3.2 Variação da quantidade de dispositivos

Na Figura 20 são apresentados os valores das dispersões dos 9 experimentos que estão agrupados por quantidade de dispositivos. Esses valores foram obtidos a partir dos gráficos da seção anterior, sendo que a dispersão foi calculada com a subtração do 3° e 1° quartil, respectivamente. Nesse sentido, é possível verificar que os experimentos com uma maior

quantidade de dispositivos tiveram uma maior dispersão, podendo ser causada principalmente pela sobrecarga de mensagens gerada pela maior quantidade de sensores simulados.

Para a análise da variação de dispositivos foi realizado a soma dos experimentos com a mesma quantidade de dispositivos, mas com turnos diferentes. Isso foi realizado para uma melhor avaliação da variação de dispositivos. Na Figura 21 é apresentado os resultados da latência após essa operação. Com isso, observa-se que a mediana das latências não foram proporcionais a variação dos dispositivos. No entanto, observa-se que existiu uma maior quantidade de *outliers* em relação aos experimentos com 30 dispositivos, como já esperado. E também experimentos com menor quantidade de dispositivos tiveram uma menor variabilidade considerando a dispersão dos gráficos *boxplot*. Isso implica que para os experimentos que possuíram a quantidade de dispositivos inferior a 30, uma maior quantidade de latência ficou mais próxima da mediana. Dessa forma, demonstrando uma maior estabilidade.

Figura 20 – Dispersão x Turnos

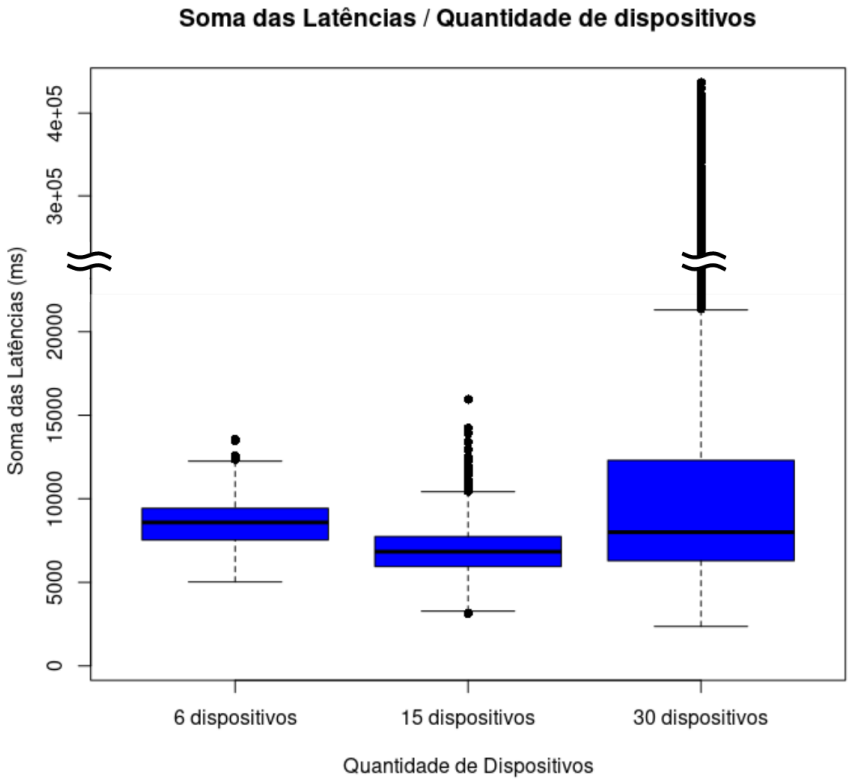


Fonte: Elaborado pelo autor.

6.4 Considerações dos Resultados

Com os experimentos realizados, nesta seção percebeu-se a possível utilização dessa solução em uma instituição de saúde inteligente. Com esses experimentos foi buscado analisar o comportamento da latência da mensagem levando em consideração a maior parte dos componentes utilizados em cada camada. Desde os componentes do *FIWARE*, como o *Orion Context Broker* e *IoT Agent*, até os componentes da rede *Hyperleger* da camada de

Figura 21 – Variação de dispositivos



Fonte: Elaborado pelo autor.

armazenamento *on-chain*.

No geral, com os experimentos realizados foi observado que com as menores quantidades de sensores simulados, a solução proposta obteve um melhor desempenho. Esse comportamento já era esperado devido a menor quantidade de tráfego de mensagens geradas. Além disso, também houve uma tendência de estabilidade de latência para experimento com menores quantidades de dispositivos.

Os testes de desempenhos executados foram realizados em uma pequena escala. Por conta disso é possível levantar algumas ameaças à sua validade. Na experimentação contou-se com uma infraestrutura onde a implementação da camada de comunicação utilizando *containers* do *middleware FIWARE* não escalam seus recursos de acordo com o recebimento de requisições. Da mesma forma para os componentes da rede *Hyperledger Fabric*. Isso pode gerar uma sobrecarga na utilização dos serviços ou até mesmo uma subutilização dos recursos.

6.5 Aplicação WEB

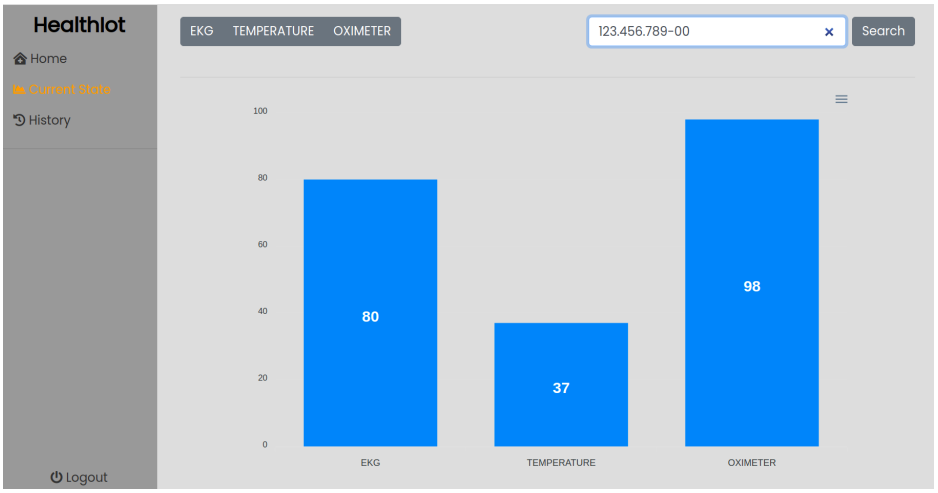
Nesta seção o protótipo da aplicação *WEB* será descrito. Esta aplicação inicialmente tem a finalidade de exibir através de gráficos o estado de saúde do paciente, baseando-se em três variáveis que indicam: batimento por minuto do coração (BPM), temperatura corporal e taxa de oxigênio no sangue. No cenário proposto está sendo considerado apenas um paciente, cuja identificação está sendo nomeada pelo valor 123.456.789-00. Para este trabalho não foi possível a utilização de um sensor de temperatura corporal, mas para essa variável os dados foram gerados em *software*. No entanto, devido a essa implementação um sensor de temperatura pode ser facilmente adicionado no sistema.

Como a cadeia de blocos da rede é imutável e transparente, é possível tirar proveito dessas características para realizar o rastreamento das transações e assim obter o estado atual e o histórico dos sinais vitais do paciente. A Figura 22 exibe o último dado armazenado na rede referente as medições que indicam a frequência cardíaca (80 batimentos por minuto), temperatura (37 graus) e a saturação de oxigênio sanguínea (98%). Esse gráfico pode ser usado por profissionais para facilitar a visualização da situação atual do paciente por meio dos valores aferidos.

Na Figura 23 os gráficos de linhas exibem amostras do histórico de dados. Por meio deles é possível investigar de forma individual e em conjunto as três variáveis que estão sendo aferidas pelos sensores. Dessa forma, é facilitado para o usuário da aplicação o estudo da situação do paciente. Além disso, mediante a seleção de um dos marcadores é proporcionado aos usuários uma imediata visualização dos valores medidos em cada instante, como está sendo mostrado na Figura 23.

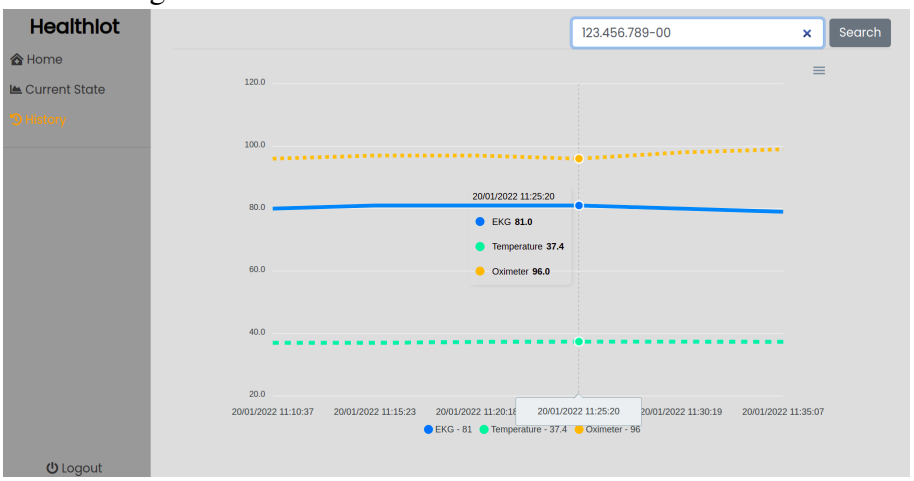
O gráfico de linhas é composto pela apresentação de três variáveis: na linha superior (laranja e pontilhada) é mostrado os valores medidos referentes a porcentagem de oxigênio no sangue, na linha intermediária (azul e contínua) refere-se ao valor obtido do sensor ECG e a linha inferior (verde e pontilhada) trata-se da temperatura corporal. A variação do eixo horizontal indica o deslocamento no tempo e variações no eixo vertical define o valor medido para cada variável. Vale ressaltar que essa aplicação está em um estágio inicial, a princípio foi criada para validar o fluxo dos dados. Apesar disso, é possível a sua utilização em trabalhos futuros para criação de um sistema mais robusto.

Figura 22 – Gráfico de barras.



Fonte: Elaborado pelo autor.

Figura 23 – Gráfico de linhas.



Fonte: Elaborado pelo autor.

7 CONCLUSÕES E TRABALHOS FUTUROS

A tecnologia *E-health* nos últimos anos vem crescendo em diversos aspectos, desde o acesso remoto a receitas médicas até o uso de sensores para verificação do estado de saúde. De forma análoga, a tecnologia *blockchain* atua como uma solução descentralizada que possibilita a ausência de terceiros para ser a solução de diversos problemas do âmbito da saúde. A disponibilidade e privacidade dos dados são exemplos de características importantes atribuídas aos dados associadas a esses contextos. Dessa forma, a integração dessas duas tecnologias pode gerar promissoras aplicações tanto na academia, quanto na indústria.

7.1 Considerações Finais

Neste trabalho foi proposto uma solução para compartilhamento de dados de saúde baseado em *blockchain* permissionada em um cenário *IoT*. O objetivo geral foi fornecer uma solução para monitoramento e compartilhamento de sinais vitais de pacientes que estejam sob os cuidados de uma instituição de saúde inteligente. Foi construída uma infraestrutura para geração do cenário e utilizado sensores de saúde para validar a utilização da solução. Por fim, foram realizadas simulações de sensores de saúde para geração de carga de trabalho e realizado a análise do comportamento do sistema.

De acordo com os experimentos realizados no capítulo anterior verificou-se a possibilidade da implementação da solução proposta neste trabalho em uma instituição hospitalar. Isso é observado devido aos resultados obtidos com as simulações de diferentes quantidades de dispositivos. Notou-se também que o funcionamento e a utilização de recursos para a execução da solução está diretamente relacionada a quantidade de sensores envolvidos no sistema.

Dessa forma, foi constatado que para uma menor quantidade de dispositivos a solução teve um melhor desempenho quando comparado a experimentos com maiores quantidades de carga de trabalho. No entanto, isso pode ser corrigido com melhorias na implementação dos componentes das camadas, por exemplo utilizando ferramentas para gerenciar o balanceamento de carga.

7.2 Benefícios e Dificuldades

Este projeto de pesquisa possui contribuições científicas em relação as discussões que foram realizadas nos trabalhos relacionados que envolveram aplicações *E-health* e *blockchain*.

Dessa forma, foram realizadas comparações entre pesquisas e aplicações desses contextos. Além disso, foi proposto uma solução fundamentada em um modelo em camadas para o compartilhamento de dados de saúde que pode auxiliar em outras pesquisas que envolvem *IoT*, *E-health* e *blockchain*. Apesar do sistema implementado não possuir alguns pré-requisitos do ambiente de produção, como por exemplo o tratamento de chaves privadas com o *Hardware Security Module* (*HSM*) (*Hardware Security Module*) e tratamento de disponibilidade dos componentes da arquitetura, a infraestrutura proposta pode ser utilizada como base para outros trabalhos.

Em relação as contribuições técnicas este trabalho implementa serviços distintos. Na camada física é implementado um protótipo *IoT* no contexto de *E-health*. Na camada de comunicação é implementado a utilização de um *middleware* de comunicação *IoT*. Na camada de armazenamento é implementado uma infraestrutra de rede *blockchain* permissionada através da utilização de *containers* para execução dos nós. Além disso, é implementado um contrato inteligente que possibilita que dados de sensores possam ser armazenados na cadeia de blocos. E por fim, um protótipo de uma aplicação *WEB* é desenvolvido para a visualização dos dados gerados pelos sensores.

7.3 Trabalhos Futuros

Com a elaboração da solução e realização dos experimentos notou-se a possível implementação deste trabalho em escalas maiores devido ao potencial apresentado. A utilização de ferramentas para manter a disponibilidade dos componentes da solução é uma possível implementação que pode ser feita para um melhor desempenho do funcionamento do sistema em geral. Para a camada física é possível realizar experimentos que permita a execução do protótipo *IoT* por longos períodos de tempo para que seja possível a verificação do estado do protótipo.

Para a camada de comunicação é possível realizar um melhor gerenciamento dos componentes do *FIWARE*, além oferecer um melhor serviço dessa camada como por exemplo a configuração de diferentes *brokers MQTT* para o tratamento dos dados vindos dos sensores. Na camada de armazenamento *blockchain* é possível realizar um melhor tratamento de proteção de dados usando recursos do próprio *Hyperledger* usando canais ou coleções de dados privados.

Em relação a realização dos experimentos é possível ser analisado os tempos de leituras *on-chain*, pois essa também é uma operação realizada pelas demais partes do sistema, como por exemplo a aplicação de visualização de dados. Nesse sentido, é possível também uma melhor recuperação de dados utilizando os recursos do *Hyperledger* para a rastreabilidade de

dados, como por exemplo a verificação de como os sinais vitais dos pacientes foram alterados de acordo com cada identificador. É aceitável que novas implementações de gráficos e *dashboards* sejam executados na aplicação *WEB*, como por exemplo, a geração de relatórios que mostre para o usuário uma visão geral dos dados gerados pelos sensores utilizando diferentes recursos, como os oferecidos pela própria *blockchain*. E finalmente, em paralelo a utilização de ferramentas para manter a escalabilidade dos componentes da infraestrutura é possível a realização de experimentos com maiores cargas de trabalho.

REFERÊNCIAS

ACETO, G.; PERSICO, V.; PESCAPé, A. The role of information and communication technologies in healthcare: taxonomies, perspectives, and challenges. **Journal of Network and Computer Applications**, v. 107, p. 125–154, 2018. ISSN 1084-8045. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804518300456. Acesso em: 09 out. 2021.

AGUIAR, E. J. D.; FAIÇAL, B. S.; KRISHNAMACHARI, B.; UEYAMA, J. A survey of blockchain-based strategies for healthcare. **ACM Computing Surveys (CSUR)**, ACM New York, NY, USA, v. 53, n. 2, p. 1–27, 2020.

ALHADHRAMI, Z.; ALGHFELI, S.; ALGHFELI, M.; ABEDLLA, J. A.; SHUAIB, K. Introducing blockchains for healthcare. In: **2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)**. [*S. l.*: *s. n.*], 2017. p. 1–4.

ANDROULAKI, E.; BARGER, A.; BORTNIKOV, V.; CACHIN, C.; CHRISTIDIS, K.; CARO, A. D.; ENYEART, D.; FERRIS, C.; LAVENTMAN, G.; MANEVICH, Y.; MURALIDHARAN, S.; MURTHY, C.; NGUYEN, B.; SETHI, M.; SINGH, G.; SMITH, K.; SORNIOTTI, A.; STATHAKOPOULOU, C.; VUKOLIć, M.; COCCO, S. W.; YELLICK, J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: **2021 Association for Computing Machinery**. New York, NY, USA: [*S. n.*], 2018. ISBN 9781450355841. Disponível em: https://doi.org/10.1145/3190508.3190538. Acesso em: 14 set. 2021.

ARAUJO, V.; MITRA, K.; SAGUNA, S.; ÅHLUND, C. Performance evaluation of fiware: A cloud-based iot platform for smart cities. **Journal of Parallel and Distributed Computing**, v. 132, p. 250–261, 2019. ISSN 0743-7315. Disponível em: https://www.sciencedirect.com/science/article/pii/S0743731519300164. Acesso em: 09 ago. 2021.

ARFI, W. B.; NASR, I. B.; KONDRATEVA, G.; HIKKEROVA, L. The role of trust in intention to use the iot in ehealth: Application of the modified utaut in a consumer context. **Technological Forecasting and Social Change**, v. 167, p. 120688, 2021. ISSN 0040-1625. Disponível em: https://www.sciencedirect.com/science/article/pii/S0040162521001207. Acesso em: 13 jul. 2021.

AZARIA, A.; EKBLAW, A.; VIEIRA, T.; LIPPMAN, A. Medrec: Using blockchain for medical data access and permission management. In: **2016 2nd International Conference on Open and Big Data (OBD)**. [*S. l.*: *s. n.*], 2016. p. 25–30.

BALIGA, A.; SOLANKI, N.; VEREKAR, S.; PEDNEKAR, A.; KAMAT, P.; CHATTERJEE, S. Performance characterization of hyperledger fabric. In: IEEE. **2018 Crypto Valley conference on blockchain technology (CVCBT)**. [*S. l.*], 2018. p. 65–74.

BECKERT, B.; HERDA, M.; KIRSTEN, M.; SCHIFFL, J. Formal specification and verification of hyperledger fabric chaincode. In: **Proc. Int. Conf. Formal Eng. Methods**. [*S. l.*: *s. n.*], 2018. p. 44–48.

BUTERIN, V. *et al.* A next-generation smart contract and decentralized application platform. **white paper**, v. 3, n. 37, 2014.

CACHIN, C.; VUKOLIĆ, M. **Blockchain consensus protocols in the wild**. [*S. l.*: *s. n.*], 2017.

CELESTI, A.; FAZIO, M.; MÁRQUEZ, F. G.; GLIKSON, A.; MAUWA, H.; BAGULA, A.; CELESTI, F.; VILLARI, M. How to develop iot cloud e-health systems based on fiware: a lesson learnt. **Journal of Sensor and Actuator Networks**, Multidisciplinary Digital Publishing Institute, v. 8, n. 1, p. 7, 2019.

CHERUVU, S.; WHEELER. **Demystifying Internet of Things Security**. [*S. l.*: *s. n.*], 2020.

FABRIC, H. **The Operations Service — hyperledger-fabricdocs master**. [*S. l.*: *s. n.*], 2020.

FARAHANI, B.; FIROUZI, F.; CHANG, V.; BADAROGLU, M.; CONSTANT, N.; MANKODIYA, K. Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare. **Future Generation Computer Systems**, v. 78, p. 659–676, 2018. ISSN 0167-739X. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167739X17307677. Acesso em: 03 set. 2021.

FARAHANI, B.; FIROUZI, F.; CHANG, V.; BADAROGLU, M.; CONSTANT, N.; MANKODIYA, K. Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare. **Future Generation Computer Systems**, Elsevier, v. 78, p. 659–676, 2018.

FERREIRA, D.; CORISTA, P.; GIÃO, J.; GHIMIRE, S.; SARRAIPA, J.; JARDIM-GONÇALVES, R. Towards smart agriculture using fiware enablers. In: **2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)**. [*S. l.*: *s. n.*], 2017. p. 1544–1551.

GAN, C.; SAINI, A.; ZHU, Q.; XIANG, Y.; ZHANG, Z. Blockchain-based access control scheme with incentive mechanism for ehealth systems: patient as supervisor. **Multimedia Tools and Applications**, Springer, p. 1–17, 2020.

GILCHRIST, A. **IoT security issues**. [*S. l.*: *s. n.*], 2017.

GÓMEZ, Y. R. B.; ESQUIVEL, H. E.; REBOLLAR, A. M.; VÁSQUEZ, D. V. A novel air quality monitoring unit using cloudino and fiware technologies. **Mathematical and Computational Applications**, v. 24, n. 1, 2019. ISSN 2297-8747. Disponível em: https://www.mdpi.com/2297-8747/24/1/15. Acesso em: 17 jul. 2021.

HELLIAR, C. V.; CRAWFORD, L.; ROCCA, L.; TEODORI, C.; VENEZIANI, M. Permissionless and permissioned blockchain diffusion. **International Journal of Information Management**, v. 54, p. 102136, 2020. ISSN 0268-4012. Disponível em: https://www.sciencedirect.com/science/article/pii/S0268401219314586. Acesso em: 23 out. 2021.

HOY, M. B. An introduction to the blockchain and its implications for libraries and medicine. **Medical Reference Services Quarterly**, Routledge, v. 36, n. 3, p. 273–279, 2017. PMID: 28714815. Disponível em: https://doi.org/10.1080/02763869.2017.1332261. Acesso em: 05 out. 2021.

IQBAL, N.; JAMIL, F.; AHMAD, S.; KIM, D. A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services. **IEEE Access**, v. 9, p. 8069–8098, 2021.

JAMIL, F.; AHMAD, S.; IQBAL, N.; KIM, D.-H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 20, n. 8, p. 2195, 2020.

LIANG, X.; ZHAO, J.; SHETTY, S.; LIU, J.; LI, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: **2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)**. [*S. l.*: *s. n.*], 2017. p. 1–5.

LIN, I.-C.; LIAO, T.-C. A survey of blockchain security issues and challenges. **Int. J. Netw. Secur.**, v. 19, n. 5, p. 653–659, 2017.

MOHANTA, B. K.; PANDA, S. S.; JENA, D. An overview of smart contract and use cases in blockchain technology. In: IEEE. **2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**. [*S. l.*], 2018. p. 1–4.

NAKAMOTO, S. **Bitcoin**: A peer-to-peer electronic cash system. [*S. l.*: *s. n.*], 2008. v. 4.

NOFER, M.; GOMBER, P.; HINZ, O.; SCHIERECK, D. Blockchain. **Business & Information Systems Engineering**, v. 59, n. 3, p. 183–187, Jun 2017. ISSN 1867-0202. Disponível em: https://doi.org/10.1007/s12599-017-0467-3. Acesso em: 12 nov. 2021.

OLIVEIRA, C. T.; MOREIRA, R.; SILVA, F. de O.; MIANI, R. S.; ROSA, P. F. Improving security on iot applications based on the fiware platform. In: **2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)**. [*S. l.*: *s. n.*], 2018. p. 686–693.

PATEL, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. **Health Informatics Journal**, v. 25, n. 4, p. 1398–1411, 2019. PMID: 29692204.

PETERSON, K.; DEEDUVANU, R.; KANJAMALA, P.; BOLES, K. A blockchain-based approach to health information exchange networks. In: **Proc. NIST Workshop Blockchain Healthcare**. [*S. l.*: *s. n.*], 2016. v. 1, n. 1, p. 1–10.

REYNA, A.; MARTÍN, C.; CHEN, J.; SOLER, E.; DÍAZ, M. On blockchain and its integration with iot. challenges and opportunities. **Future generation computer systems**, Elsevier, v. 88, p. 173–190, 2018.

RIFI, N.; AGOULMINE, N.; TAHER, N. C.; RACHKIDI, E. Blockchain technology: is it a good candidate for securing iot sensitive medical data? **Wireless Communications and Mobile Computing**, Hindawi, v. 2018, 2018.

SALHOFER, P. Evaluating the fiware platform. In: **Proceedings of the 51st Hawaii International Conference on System Sciences**. [*S. l.*: *s. n.*], 2018.

SANG, G. M.; XU, L.; VRIEZE, P. de; BAI, Y. Towards predictive maintenance for flexible manufacturing using fiware. In: SPRINGER. **International Conference on Advanced Information Systems Engineering**. [*S. l.*], 2020. p. 17–28.

STANCIU, A. Blockchain based distributed control system for edge computing. In: **2017 21st International Conference on Control Systems and Computer Science (CSCS)**. [*S. l.*: *s. n.*], 2017. p. 667–671.

SWAN, M. **Blockchain**: Blueprint for a new economy. [*S. l.*]: O'Reilly Media, Inc., 2015.

SZABO, N. **Smart contracts**. 1994. Disponível em: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Acesso em: 12 jul. 2021.

TAMBOLI, A. **Build Your Own IoT Platform**. [*S. l.*]: Apress, 2019.

THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: **2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)**. [*S. l.*: *s. n.*], 2018. p. 264–276. ISSN 2375-0227.

UDDIN, M. Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. **International Journal of Pharmaceutics**, v. 597, p. 120235, 2021. ISSN 0378-5173. Disponível em: https://www.sciencedirect.com/science/article/pii/S0378517321000399. Acesso em: 15 jul. 2021.

VIRIYASITAVAT, W.; HOONSOPON, D. Blockchain characteristics and consensus in modern business processes. **Journal of Industrial Information Integration**, v. 13, p. 32–39, 2019. ISSN 2452-414X. Disponível em: https://www.sciencedirect.com/science/article/pii/S2452414X18300815. Acesso em: 11 jul. 2021.

WüST, K.; GERVAIS, A. Do you need a blockchain? In: **2018 Crypto Valley Conference on Blockchain Technology (CVCBT)**. [*S. l.*: *s. n.*], 2018. p. 45–54.

XU, X.; WEBER, I.; STAPLES, M.; ZHU, L.; BOSCH, J.; BASS, L.; PAUTASSO, C.; RIMBA, P. A taxonomy of blockchain-based systems for architecture design. In: IEEE. **2017 IEEE international conference on software architecture (ICSA)**. [*S. l.*], 2017. p. 243–252.

YANG, S. T. D. V. G. W. B. **An Introduction to Hyperledger**. [*S. l.*: *s. n.*], 2018.

ZEMRANE, H.; BADDI, Y.; HASBI, A. **Improve IoT Ehealth Ecosystem with SDN**. [*S. l.*: *s. n.*], 2019.

ZENG, J.; ZHANG, J.; LIU, Y. Blockchain based smart park: Cleaning management. In: **Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications**. [*S. n.*], 2019. (ICBTA 2019), p. 53–58. ISBN 9781450377430. Disponível em: https://doi.org/10.1145/3376044.3376046. Acesso em: 12 out. 2021.

ZHANG, J.; XUE, N.; HUANG, X. A secure system for pervasive social network-based healthcare. **IEEE Access**, v. 4, p. 9239–9250, 2016.

ZHOU, Q.; HUANG, H.; ZHENG, Z.; BIAN, J. Solutions to scalability of blockchain: A survey. **IEEE Access**, v. 8, p. 16440–16455, 2020.