Uma Solução para Compartilhamento de Dados de Saúde Baseada em Blockchain Permissionada e Internet das Coisas para Hospitais Inteligentes

Alan Nascimento Gomes[1], **Emanuel Ferreira Coutinho**[1]

[1]Programa de Pós-Graduação em Computação (PCOMP)
Universidade Federal do Ceará (UFC) – Quixadá – CE – Brasil

alanng@alu.ufc.br, emanuel.coutinho@ufc.br

Abstract. *Healthcare is an area that benefits greatly from emerging technologies and computer networks. The increase in solutions that use these applications contributed to the fact that the amount of information related to the health status of patients was increasingly present in computer systems. In this scenario, healthcare institutions and patients generate a large volume of data that can be shared. However, there are issues of information security and privacy. Blockchain emerges as a technology that can deal with such situations, as it allows data decentralization and traceability. The objective of this work is to propose a solution using IoT and blockchain to provide a shared view of health data for patients, doctors and hospital management administrators. The solution was evaluated from the viewpoint of data flow and latency, showing to be promising.*

Resumo. *Healthcare é um setor que se beneficia muito das tecnologias emergentes e de redes de computadores. O aumento de soluções que utilizam essas aplicações contribuíram para que a quantidade de informações relacionadas ao estado de saúde de pacientes fosse cada vez mais presente em sistemas computacionais. Nesse cenário, instituições de saúde e pacientes geram um grande volume de dados que podem ser compartilhados. Porém há questões de segurança da informação e privacidade. A blockchain surge como uma tecnologia que pode lidar com tais situações, por permitir a descentralização dos dados e rastreabilidade. O objetivo deste trabalho é propor uma solução utilizando IoT e blockchain para fornecer uma visão compartilhada dos dados de saúde para pacientes, médicos e administradores de gestão hospitalar. A solução foi avaliada do ponto de vista do fluxo dos dados e latência, mostrando-se promissora.*

1. Introdução

Nas últimas décadas, os processos do setor de *healthcare* (“cuidados de saúde”) 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 aumento de soluções que utilizam essas aplicações contribuíram para que a quantidade de informações relacionadas ao estado de saúde de pacientes fosse 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 o compartilhamento desses dados de extrema importância para estudos e diagnósticos mais rápidos [De Aguiar et al. 2020].

Instituições de saúde e pacientes podem compartilhar dados em bases centralizadas e com baixo custo de implantação. Contudo, mesmo com esses benefícios, existem 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. 2018]. *IoT* é 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 [Zemrane et al. 2019]. 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 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.

A *blockchain* surge como uma tecnologia que pode lidar com tais problemas mencionados. Sendo 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 [De Aguiar et al. 2020]. Além da *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]. *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, o objetivo deste trabalho é propor uma solução utilizando IoT e *blockchain* para fornecer uma visão compartilhada dos dados de saúde para pacientes, médicos e administradores de gestão hospitalar, fornecendo 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 desen-

volvimento de um sistema mais confiável.

2. Trabalhos Relacionados

Diversas aplicações utilizam *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 quanto dados de saúde em geral.

Jamil et al. (2020) citaram que ao compartilhar informações médicas, a segurança dos dados são requisitos essenciais para a interação e coleta de registros médicos eletrônicos. Por causa disso, propô-se uma plataforma *IoT* descentralizada para a área de saúde, baseada em uma *blockchain* permissionada, abordando desafios de segurança de dados, gerenciamento de identidades e escalabilidade. A arquitetura proposta estabelece comunicação entre os dispositivos físicos de saúde, o servidor IoT e *blockchain*.

Para Liang et al. (2017) , o compartilhamento seguro de dados pessoais de saúde é crucial para melhoria da interação e colaboração do setor de saúde. Devido aos 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. O sistema foi avaliado com uma ferramenta de *benchmark* própria. No entanto, no sistema proposto não foi utilizado um *middleware* para o tratamento da interoperabilidade e tratamento dos dados vindo dos sensores.

Azaria et al. (2016) apontaram que os registros médicos precisam passar por inovação e afirmam que os pacientes deixam os dados espalhados por várias servidores, perdendo o controle de acesso aos seus dados. Um sistema chamado MedRec foi proposto, sendo uma estrutura baseada em *blockchain* para armazenar registros médicos eletrônicos, sendo uma rede *peer-to-peer*, e integrando contratos inteligentes na plataforma *Ethereum*, a partir do consenso não permissionado. Porém, a proposta não apresenta tratamentos relacionados a privacidade dos pacientes.

Patel (2019) propôs uma estrutura onde pacientes podem compartilhar imagens médicas de forma segura e controlada. O objetivo é registrar uma lista de estudos e uma lista dos pacientes aos quais esses estudos pertencem. A *blockchain* empregada utiliza o algoritmo de consenso *Proof of Stake* e algoritmos de criptografia de chave pública. Uma alternativa para a implementação de uma ferramenta que certifique o compartilhamento de imagens médicas de forma confiável e sem adulterações é apresentada.

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. Existem cinco características avaliadas na Tabela 1. (1) ativos, relacionados ao tipo de informação que está sendo gerenciado pelo sistema; (2) plataforma de implementação *blockchain*, referindo-se à plataforma que foi utilizada para o desenvolvimento *blockchain*; (3) tipo de *blockchain*; e (4) a plataforma de comunicação IoT.

Nos trabalhos dos autores Jamil et al. (2020) e Liang et al. (2017) são encontradas limitações relacionadas à utilização de uma plataforma responsável por realizar a

Tabela 1. Comparação entre os trabalhos relacionados

Trabalho	**Ativos**	**Plat. Implementação**	**Tipo de *Blockchain***	**Plat. Comunic. IoT**
[Jamil et al. 2020]	Dados de Sensores	Hyperledger	Permissionada	Nenhuma
[Liang et al. 2017]	Dados de Sensores	Hyperledger	Permissionada	Nenhuma
[Azaria et al. 2016]	Registro Médico Eletrônico	Ethereum	Não permissionada	Não se aplica
[Patel 2019]	Imagens	Implementação Própria	Não permissionada	Não se aplica
Solução Proposta	Dados de Sensores	Hyperledger	Permissionada	Plataforma FIWARE

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*. 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. Dessa forma, a solução proposta utiliza o ecossistema de *blockchain* permissionado *Hyperledger* para implantação de uma rede permisisonada privada. 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. A plataforma FIWARE é utilizada para atuar como um *middleware* de comunicação entre o protótipo IoT e as camadas superiores.

3. Materiais e Métodos

3.1. Modelo da Solução Proposta

Este trabalho propõe uma solução para o compartilhamento de dados de saúde com *IoT*. A Figura 1 exibe o fluxo dos dados no ambiente. 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. 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.

3.2. Modelo em Camadas da Solução

O modelo em camadas proposto para este trabalho é exposto na Figura 2. Analisando de forma vertical ascendente, tem-se a primeira camada, chamada de Física. Nos blocos

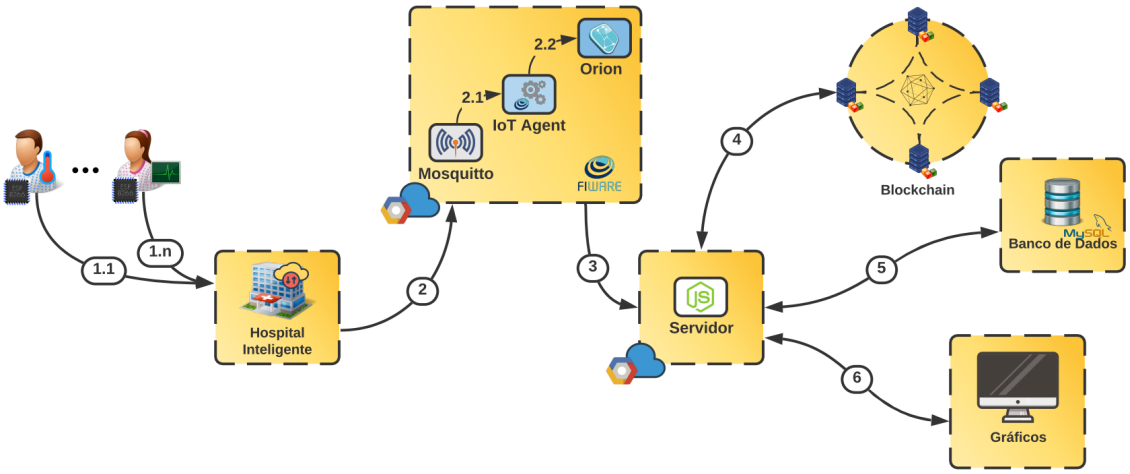


Figura 1. Fluxo de operações da solução.

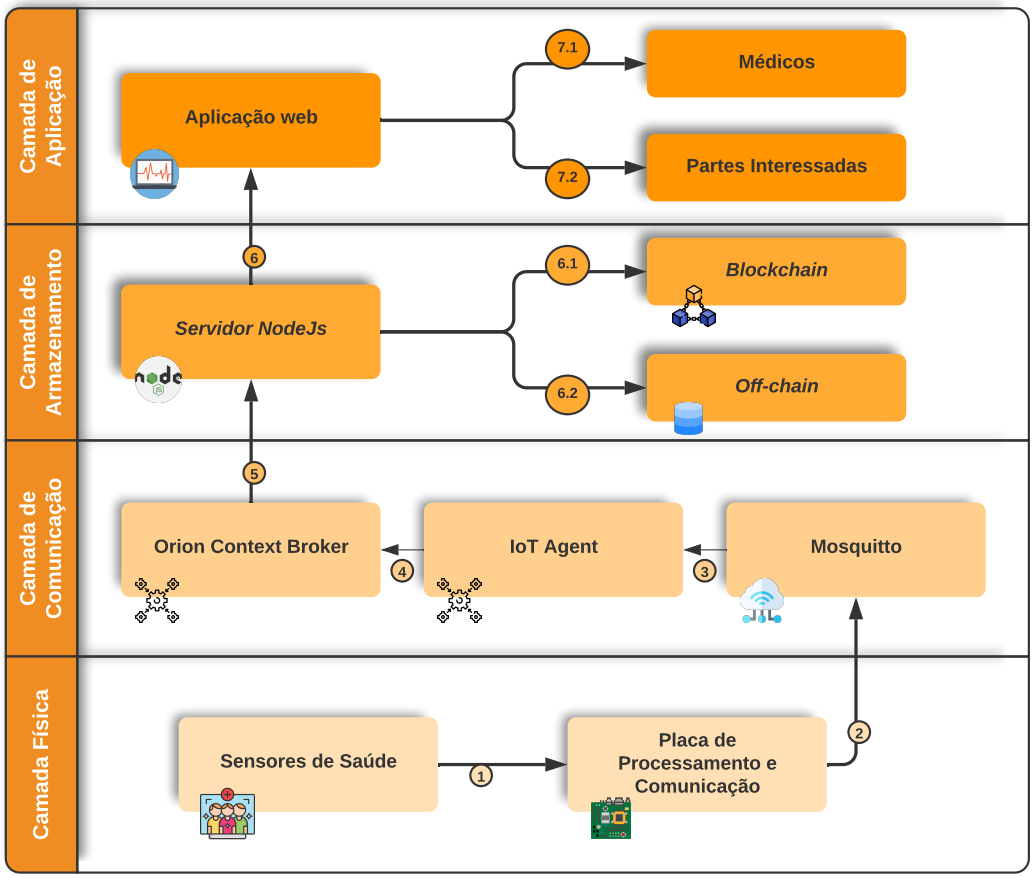


Figura 2. Modelo de Arquitetura em Camadas.

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, denominada Camada de Comunicação, são apresentados os blocos que compõem os componentes do *middleware*, responsáveis 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*, onde se traduz 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*, sendo o 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.

3.3. Protótipo IoT

Para a realização dos experimentos, um protótipo para a aferição das variáveis de saúde dos pacientes foi projetado. A Figura 3 apresenta 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. 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*.

3.4. 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*. A ferramenta foi utilizada

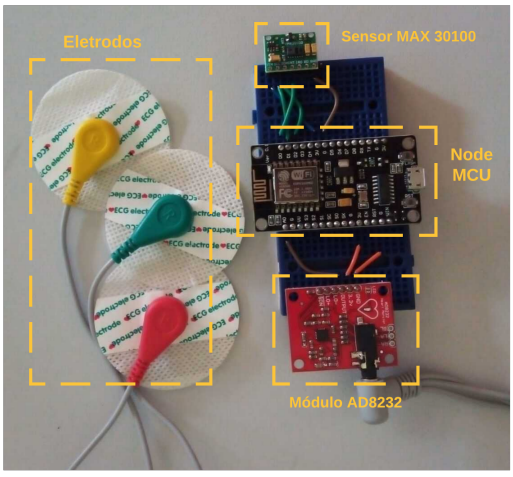


Figura 3. Protótipo IoT.

para simular diferentes sensores de saúde e consequentemente diferentes pacientes. É possível simular dois tipos de sensores: por tempo ou por evento. O sensor por tempo é caracterizado pelo envio de dados de forma periódica e sensor por evento envia 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 é de suma importância, pois a geração de carga de trabalho usando sensores físicos traz um alto custo para o projeto, devido aos preços desses tipos de dispositivos de aferição de saúde.

3.5. Infraestrutura da Rede *Hyperledger Fabric*

A Figura 4 apresenta a infraestrutura da rede *Hyperledger Fabric* projetada para os experimentos. No total foram utilizados sete nós executados em *containers* e estão distribuídos em três máquinas virtuais, executando em servidores Linux. Em uma rede *Hyperledger* as organizações (HLF) podem ser tão grandes quanto uma 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 consiste no conjunto de indivíduos que terão acesso aos dados de um determinado paciente. 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 das organizações são 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 das organizações esta sendo executadas em uma máquina virtual. Em cada uma dessas são instanciados *containers docker* que executarão os componentes da rede Hyperledger, por exemplo: os nós *peers* que armazenam a cadeia de blocos e os nós *orderers* que validarão as transações. Além disso, serão instanciadas 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.

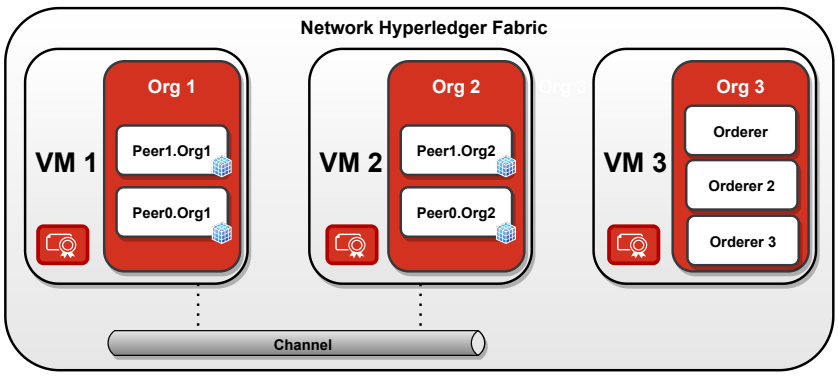


Figura 4. Infraestrutura Rede Hyperledger.

3.6. Contrato Inteligente

Na rede *Hyperledger Fabric*, um contrato inteligente desenvolvido na linguagem *Go* foi implantado. Com esse *chaincode*, denominação de contrato inteligente na rede *Hyper-*

ledger, é possível realizar operações de escritas e leituras no *ledger*. Os dados armazenados na rede consistem nos valores obtidos dos sensores representados pelas variáveis: BPM, *Oximeter* e ECG. Os métodos desenvolvidos no *chaincode* são: (1) ***initLedger*:** Este método é responsável por fazer a primeira operação de escrita na rede, com intuito de verificar se a rede está disponível; (2) ***createStatePatient:*** Neste método será possível a inserção do estado de saúde do paciente no banco de dados de estado global; (3) **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*; (4) **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; e (5) **queryPrivateImpliciteOrg1:** Através deste método será possível que os usuários pertencentes a uma das organizações recuperem os dados inseridos através do método *createPrivateImpliciteOrg1*.

4. Resultados e Análises

Neste trabalho foram realizados experimentos para verificar o comportamento da solução com diferentes cargas de trabalho, resumido na Tabela 2. O intuito desses experimentos foi verificar a latência do percurso da mensagem. Esse percurso considera-se desde a geração do dados na camada física até a validação da escrita na base de dados *on-chain*.

4.1. Configuração dos Experimentos

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: quantidade de dispositivos, periodicidade do envio de mensagens e duração do experimento.

Tabela 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 Sense (quantidade de dispositivos) e turnos
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.

Os experimentos foram baseados 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 feitas

diferentes configurações no SenSe alternando a 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 cenários 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. A Tabela 3 resume a configuração dos experimentos.

Tabela 3. Configuração dos experimentos

Experimentos	Qtd. dispositivos	Turno	Data	Duração
3	6	manhã / tarde / noite	09, 10 e 15 de dez. de 2021	1 hora
3	15	manhã / tarde / noite	08 e 09 de dez. de 2021	1 hora
3	30	manhã / tarde / noite	08 e 09 de dez. de 2021	1 hora

4.2. 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 leva para percorrer 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 5, T1 representa o tempo necessário para que a mensagem percorra o primeiro estágio e T2 representa o tempo necessário para que 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.

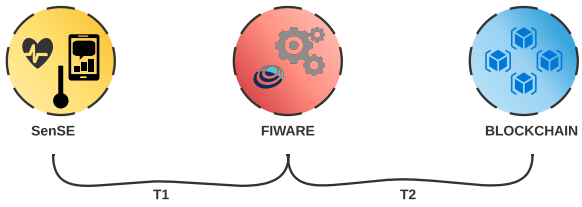


Figura 5. Caminho da mensagem

Durante os experimentos foram gerados diferentes quantidades de mensagens cuja soma apresentou-se diretamente proporcional a quantidade de dispositivos, conforme mostrado na Tabela 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.

Tabela 4. Quantidade de mensagens por experimento

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

4.3. Variação de Turnos

Em relação a variação dos turnos observou-se que a latência foi impactada. Na Tabela 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.

Tabela 5. Mediana dos turnos

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

A Figura 6 exibe 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*, possivelmente associados ao uso intenso da rede nesse turno. 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 1o. quartil do gráfico. Em contraste ao período da noite que houve uma maior tendência a dispersão. Essa característica pode ser melhor observada na Figura 7(a).

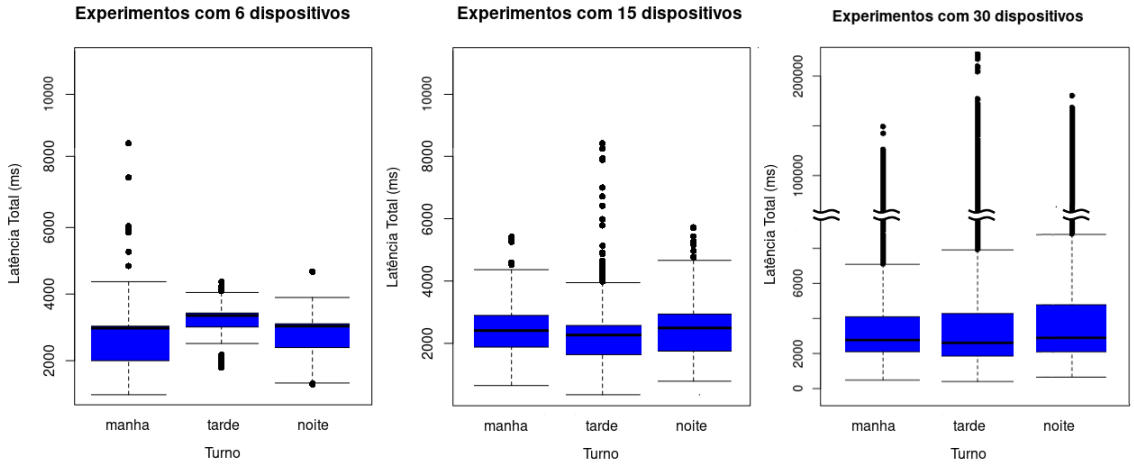


Figura 6. Experimentos com 6, 15 e 30 dispositivos

4.4. Variação da quantidade de dispositivos

Na Figura 7(a) são apresentados os valores das dispersões dos 9 experimentos, agrupados por quantidade de dispositivos. Esses valores foram obtidos a partir dos gráficos da seção

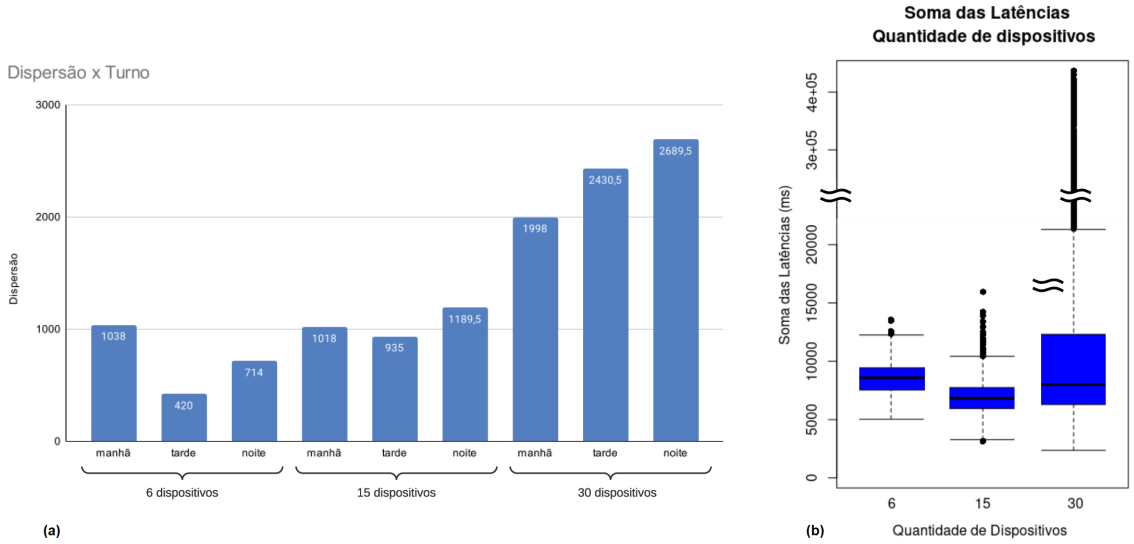


Figura 7. Gráficos de (a) Dispersão x Turnos e (b) Variação de dispositivos

anterior, sendo que a dispersão foi calculada com a subtração do 3o. e 1o. 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 7(b) são apresentados os resultados da latência após essa operação. Com isso, observa-se que as medianas das latências não foram proporcionais à variação dos dispositivos. No entanto, observa-se que existiu uma maior quantidade de *outliers* em relação aos experimentos com 30 dispositivos, como já esperado. Experimentos com menor quantidade de dispositivos tiveram uma menor variabilidade considerando a dispersão dos gráficos *boxplot*. Isso implica que para os experimentos que continham a quantidade de dispositivos inferior a 30, uma maior quantidade de latência ficou mais próxima da mediana. Dessa forma, demonstrando uma maior estabilidade.

4.5. 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 procurou-se 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 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.

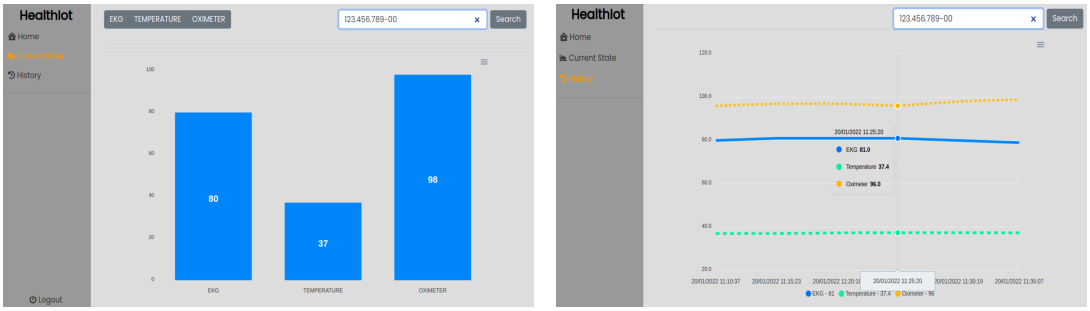
4.6. Aplicação WEB

Nesta seção o protótipo da aplicação *WEB* é descrito. Esta aplicação inicialmente possui 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 considerou-se apenas um paciente, cuja identificação está sendo nomeada pelo valor 123.456.789-00.

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 8(a) 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%). Dessas variáveis, apenas a temperatura corporal está sendo gerada em *software*. Esse gráfico pode ser usado por profissionais para facilitar a visualização da situação atual do paciente por meio dos valores aferidos.

Na Figura 8(b) 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 8(b).

Vale ressaltar que essa aplicação está em um estágio inicial, sendo apenas ilustrativa, e 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.



(a) (b)

Figura 8. Gráfico de barras (a) e Gráfico de linhas (b) da aplicação web com dados dos sensores

5. Conclusão

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.

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. 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 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 natural que novas implementações de gráficos e *dashboards* surjam, como por exemplo, a geração de relatórios que mostre para o usuário uma visão geral dos dados gerados pelos sensores utilizando diferentes recursos. 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.

Agradecimentos

Este trabalho foi realizado com o apoio do Insight Data Science Lab por meio do projeto **Governo Digital do Estado do Ceará**, financiado pela FUNCAP número 04772314/2020.

Referências

Aceto, G., Persico, V., and Pescapé, A. (2018). The role of information and communication technologies in healthcare: taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications*, 107:125–154.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., and Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. *ACM Computing Surveys (CSUR)*, 53(2).

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., and Mankodiya, K. (2018). Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare. *Future Generation Computer Systems*, 78:659–676.

Gan, C., Saini, A., Zhu, Q., Xiang, Y., and Zhang, Z. (2020). Blockchain-based access control scheme with incentive mechanism for ehealth systems: patient as supervisor. *Multimedia Tools and Applications*, pages 1–17.

Jamil, F., Ahmad, S., Iqbal, N., and Kim, D.-H. (2020). Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors*, 20(8):2195.

Liang, X., Zhao, J., Shetty, S., Liu, J., and Li, D. (2017). 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)*, pages 1–5.

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, 25(4):1398–1411.

Peterson, K., Deeduvanu, R., Kanjamala, P., and Boles, K. (2016). A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare*, volume 1, pages 1–10.

Rifi, N., Agoulmine, N., Chendeb Taher, N., and Rachkidi, E. (2018). Blockchain technology: is it a good candidate for securing iot sensitive medical data? *Wireless Communications and Mobile Computing*, 2018.

Stanciu, A. (2017). Blockchain based distributed control system for edge computing. In *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, pages 667–671.

Thakkar, P., Nathan, S., and Viswanathan, B. (2018). 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)*, pages 264–276.

Zemrane, H., Baddi, Y., and Hasbi, A. (2019). *Improve IoT Ehealth Ecosystem with SDN*.

Zeng, J., Zhang, J., and Liu, Y. (2019). Blockchain based smart park: Cleaning management. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, ICBTA 2019, page 53–58.

Zhang, J., Xue, N., and Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access*, 4:9239–9250.