Uma Arquitetura para Aplicações *mHealth* Descentralizadas Baseadas em Blockchain

Noeli Antonia Vaz[1,2], **Matheus Martins**[1], **Gislainy Velasco**[1], **Sergio T. Carvalho**[1]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Caixa Postal 131 – CEP 74001-970 – Goiânia - GO – Brasil

[2]Instituto Acadêmico de Ciências Exatas e Tecnológicas – Universidade Estadual de Goiás (UEG)
Caixa Postal 459 – 75132903 – Anápolis – GO – Brasil

{noelivaz,matheus.b.m,gislainycrisostomo}@discente.ufg.br, sergiocarvalho@ufg.br

Abstract. *Utilizing blockchain technology has enabled the creation of decentralized applications that consolidate smart contracts. These contracts automate the execution of agreed-upon clauses without the need for intermediaries or centralized elements. Although mHealth applications offer improvements in the availability and accessibility of healthcare services, they also pose data security and privacy challenges. The implementation of blockchain-based DApps in mHealth can provide significant benefits. This article presents an architecture for mHealth applications that focuses on a decentralized approach based on blockchain and emphasizes users' consent to access data. The mHealth IUProst application is an example of the proposed architecture, utilizing the permissioned blockchain Hyperledger Fabric. The article also details the technologies designed for each element of the architecture.*

Resumo. *O uso de blockchain tem permitido o desenvolvimento de aplicações descentralizadas, as quais agregam contratos inteligentes que automatizam a execução de cláusulas acordadas sem elementos intermediários e centralizados. Embora as aplicações mHealth tragam melhorias na disponibilidade e acessibilidade dos serviços de saúde, também apresentam desafios de segurança e privacidade dos dados. A utilização das DApps baseadas em blockchain em mHealth pode proporcionar benefícios significativos. Este artigo propõe uma arquitetura para aplicações mHealth, com foco em uma abordagem descentralizada baseada em blockchain e com propriedades relacionadas ao consentimento de acesso aos dados pelos usuários. Como exemplo de uso da arquitetura proposta, é apresentada a arquitetura da aplicação mHealth IUProst com uso da blockchain permissionada Hyperledger Fabric e os detalhamentos das tecnologias projetadas para cada elemento da arquitetura.*

1. Introdução

A tecnologia *blockchain* tem despertado um interesse crescente em uma variedade de setores, prometendo soluções inovadoras para desafios complexos. No campo da saúde, em que a segurança, privacidade e integridade dos dados são essenciais, a *blockchain* emerge como uma ferramenta poderosa para revolucionar a maneira como lidamos com informações médicas. Ao mesmo tempo, as aplicações móveis de saúde, conhecidas como

mHealth, têm se destacado como ferramentas essenciais na prestação de serviços e em informações de saúde acessíveis e eficazes.

A combinação entre *blockchain* e *mHealth* representa uma convergência promissora, oferecendo um potencial significativo para melhorar a segurança, privacidade e interoperabilidade dos dados de saúde. A natureza descentralizada e imutável da *blockchain* pode mitigar os riscos associados ao armazenamento centralizado de dados sensíveis de saúde, ao mesmo tempo que facilita o compartilhamento seguro e transparente dessas informações entre pacientes, prestadores de cuidados de saúde e outras partes interessadas.

Neste contexto, várias iniciativas e pesquisas têm explorado o uso da *blockchain* em aplicações de saúde, visando aprimorar a gestão de registros médicos, garantir a autenticidade e integridade dos dados e, facilitar o compartilhamento seguro de informações entre sistemas de saúde heterogêneos [Stamatellis et al. 2020, Díaz et al. 2019, Wang and Qin 2021]. No entanto, para alcançar todo o potencial da *blockchain* em *mHealth*, é essencial considerar não apenas a tecnologia subjacente, mas também a arquitetura das aplicações descentralizadas (DApps).

Nem todas as arquiteturas de DApps são criadas igualmente, e muitas vezes a ênfase na funcionalidade pode negligenciar considerações críticas relacionadas à segurança e privacidade dos dados. Neste sentido, este trabalho propõe uma análise aprofundada da arquitetura de DApps baseadas em *blockchain* para *mHealth*, com foco na definição de diretrizes e melhores práticas para o desenvolvimento de sistemas de saúde descentralizados.

Além disso, apresentamos uma proposta de arquitetura específica para DApps de saúde, projetada para atender às demandas exclusivas do setor. Esta arquitetura visa garantir a segurança e privacidade dos dados dos pacientes e, também, promove a interoperabilidade e transparência das informações médicas. Como estudo de caso, exploramos a aplicação *mHealth* IUProst[1][Estevam 2022], destacando como a arquitetura proposta pode ser implementada e integrada em cenários do mundo real.

Em resumo, este trabalho visa contribuir para o avanço do conhecimento em DApps baseadas em *blockchain* para saúde, oferecendo diretrizes claras e práticas para o desenvolvimento de sistemas de saúde descentralizados. Ao final, esperamos não apenas apresentar uma visão abrangente desta área, mas também inspirar futuras pesquisas e inovações neste campo em rápido desenvolvimento.

As próximas seções do artigo estão estruturadas da seguinte forma: a Seção 2 apresenta fundamentos sobre aplicações *mHealth* e *blockchain*; a Seção 3 discute os trabalhos relacionados; a Seção 4 detalha a proposta da arquitetura e inclui um exemplo de sua aplicação na construção da IUProst. As discussões dos resultados são apresentadas na Seção 5 e, por fim, a Seção 6 traz as conclusões e trabalhos futuros.

2. Contextualização

Esta seção apresenta os principais conceitos e tecnologias utilizados para compreender a arquitetura proposta neste estudo.

[1]www.iuprost.com.br

2.1. Aplicações *mHealth*

A mobilidade e a disponibilidade dos *smartphones* favorecem a ampla utilização de ferramentas e soluções voltadas para a saúde. As aplicações *mHealth* se baseiam em três pilares fundamentais: computação móvel, sensores médicos e tecnologias de comunicação para a saúde [Istepanian 2022]. Essas aplicações são geralmente desenvolvidas utilizando arquiteturas centralizadas, o que apresenta desafios relacionados a falhas do sistema, segurança e privacidade dos dados dos usuários [Taralunga and Florea 2021].

Os serviços oferecidos pelas aplicações *mHealth* podem incluir o uso de diversas tecnologias, tais como dispositivos vestíveis, tecnologias de sensores, Internet das Coisas (*Internet of Things - IoT*), servidores, serviços de nuvem e dispositivos móveis. Segundo os autores [Istepanian 2022] e [de Faria et al. 2024], os aplicativos *mHealth* devem ser simples e fáceis de usar, além de serem embasados por evidências científicas e respaldados por leis de privacidade e segurança. Essas aplicações visam incentivar os usuários (*e.g.*: profissionais de saúde, clínicas e pacientes) a adotarem seu uso efetivo, apoiando tratamentos, orientações de saúde e o monitoramento remoto de pacientes.

Nesse contexto, o consentimento assume um papel especialmente importante na área da saúde, onde os dados são considerados sensíveis e podem impactar diretamente a dignidade e a privacidade do usuário. O consentimento é um dos princípios fundamentais da proteção de dados pessoais, caracterizado pela manifestação livre, informada e inequívoca do titular, que autoriza o tratamento de seus dados para uma finalidade específica [Buchain 2021].

2.2. Arquitetura de DApps Baseadas em *Blockchain*

Blockchain é uma tecnologia que possibilita o compartilhamento seguro e imutável de dados e transações em uma rede descentralizada. Essa estrutura é resultante da combinação de diversas tecnologias da ciência da computação, tais como computação distribuída, redes *peer-to-peer* (P2P), criptografia e algoritmos de consenso.

Há diferentes tipos de redes *blockchain*, classificadas como públicas, privadas/federadas, permissionadas e não permissionadas. Cada tipo possui características específicas e requisitos de participação distintos. A escolha do tipo de rede e do mecanismo de consenso é determinada pelos requisitos e objetivos do projeto. Além disso, a seleção da plataforma *blockchain* é crucial para o desenvolvimento de DApp, sendo Ethereum e Hyperledger as plataformas mais proeminentes na atualidade.

O uso de *blockchain* em aplicações de saúde visa garantir a segurança, confidencialidade e integridade dos dados, especialmente dos dados sensíveis, conforme a Lei Geral de Proteção de Dados (LGPD). No entanto, há limitações relacionadas à capacidade computacional e aos custos associados ao processamento de transações em redes públicas de *blockchain*.

Desta forma, as decisões sobre quais dados e operações devem ser realizadas na *blockchain* e quais devem ocorrer fora dela são cruciais para o desenvolvimento de DApps. Em termos de concepção arquitetural das aplicações descentralizadas, há uma discussão sobre o grau de descentralização (total ou parcial) desejado para essas aplicações, envolvendo principalmente duas dimensões: operacional e de dados.

Quando se trata da dimensão operacional, o grau de descentralização é anali-

sado com base no tipo de rede *blockchain* envolvida e no uso de contratos inteligentes [Xu et al. 2017]. Nesta vertente, as aplicações baseadas em redes *blockchain* públicas são consideradas totalmente descentralizadas, devido à natureza destas redes, que não possuem nós centralizadores. Em contraste, as aplicações em redes *blockchain* privadas são vistas como parcialmente descentralizadas, pois partem do pressuposto de existência (frequentemente predefinida, como em redes consorciadas) de nós com algum grau de confiança e, consequentemente, com potencial de centralização, uma vez que são responsáveis pela validação das atividades da rede. Ao analisar a dimensão de dados, o grau de descentralização é considerado também com base no serviço de armazenamento utilizado pelas aplicações. Entre as tecnologias de suporte às aplicações totalmente descentralizadas, destaca-se o *Interplanetary File System* (IPFS), um sistema de arquivos descentralizado que opera na estrutura de uma rede P2P [Zheng et al. 2023]. Portanto, uma aplicação totalmente descentralizada requer tanto uma rede *blockchain* pública quanto a descentralização do armazenamento por meio de uma rede P2P, como a proporcionada pelo IPFS. Já uma aplicação parcialmente descentralizada é caracterizada por estar baseada em uma rede *blockchain* privada ou por possuir um armazenamento centralizado.

As DApps baseadas em blockchain satisfazem, em algum nível, os critérios de descentralização, seja operacionalizando a lógica por meio de contratos inteligentes ou pelo armazenamento dos dados, que pode empregar tecnologias descentralizadas.

A Figura 1 ilustra uma arquitetura geral para DApps baseadas em *blockchain*.

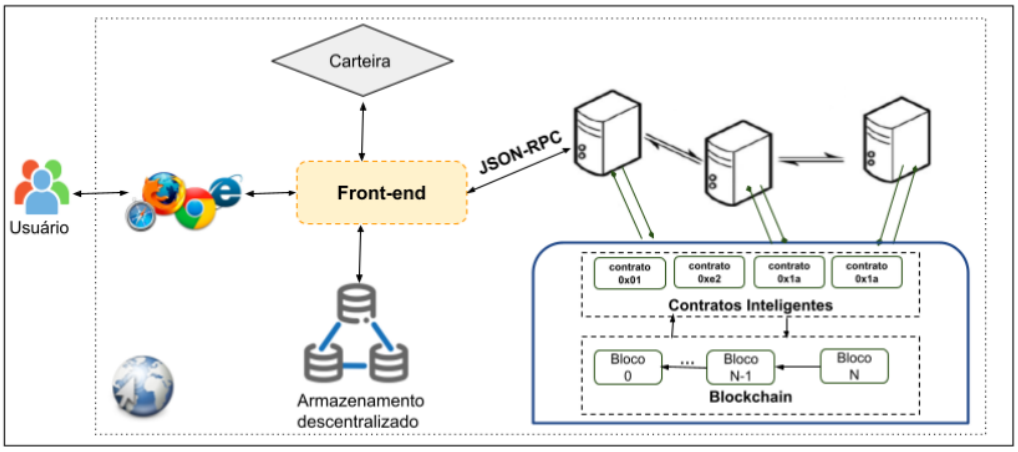

Figura 1. Arquitetura de DApp baseada em *blockchain*. Adaptado de [Ray 2023]

No nível da aplicação, a arquitetura envolve o uso de blocos de construção e tecnologias subjacentes, tais como protocolos de comunicação, *Application Programming Interface* (API), carteiras, e, no nível mais básico, a própria *blockchain* e o seu funcionamento geral.

- *Front-end*: define a interface do usuário, que interage com a lógica da aplicação por meio dos contratos inteligentes. Para a construção de interfaces, são utilizadas bibliotecas JavaScript como React.js, Node.js. Além disso, bibliotecas que permitem a interação com a *blockchain* Ethereum, como web3.js e ethers.js, são amplamente empregadas.
- Carteira: permite aos usuários que assinem transações utilizando sua chave privada antes de serem transmitidas para a *blockchain*. Também auxilia no gerenci-

amento de permissões para compartilhamento de dados, armazenamento de criptomoedas, entre outros aspectos. Exemplos de carteiras incluem Metamask[2] e Taho[3]. Em blockchains do tipo permissionadas, são utilizados diferentes mecanismos de autenticação e validação de usuários.
- JSON-RPC: protocolo de comunicação que permite a interação da aplicação com a *blockchain* sem a necessidade de participação direta na rede. Esse papel é frequentemente denominado *provider*. Um exemplo é a Infura.
- Armazenamento descentralizado: IPFS é um exemplo dessa tecnologia, oferecendo uma solução para armazenamento de dados em uma rede P2P.
- Contratos Inteligentes: definem a lógica de negócios das operações executadas na *blockchain*. Linguagens de programação de alto nível como Solidity e Vyper, além de linguagens de propósito geral como Golang, Java e Node.js, são utilizadas para desenvolver esses contratos.

Com isso, observa-se que a arquitetura destacada ilustra os elementos principais de uma aplicação descentralizada baseada em *blockchain*, exigindo, portanto, a consideração dos aspectos discutidos em termos de requisitos e de implementação dos diferentes graus de descentralização.

3. Trabalhos Relacionados

Aplicações *mHealth* e *blockchain* estão sendo discutidas por autores com o intuito de apresentar soluções descentralizadas baseadas em *blockchain* viáveis para o uso na saúde, assim como priorizar a privacidade e a segurança dos dados dos pacientes [Stamatellis et al. 2020, Díaz et al. 2019].

Ao considerar a segurança e a privacidade dos dados, uma plataforma de *blockchain* privada/permissionada frequentemente escolhida é a Hyperledger Fabric. Esta plataforma é utilizada em diversas aplicações, incluindo aplicações móveis [Díaz et al. 2019], gestão de dados [Wang and Qin 2021] e soluções arquiteturais [Stamatellis et al. 2020].

Em [Stamatellis et al. 2020], os autores discutem como os Registros Eletrônicos de Saúde (RES) são frequentemente alvos de ataques cibernéticos, exemplificados pelo *ransomware WannaCry* e pelo *ataque Medjack*, que resultaram em perdas monetárias significativas e no comprometimento das informações pessoais dos usuários. Como resposta a esses problemas, o trabalho propõe a *Privacy-Preserving Healthcare (PREHEALTH)*, uma solução para o gerenciamento de RES. Essa abordagem envolve armazenar os RES em um livro-razão distribuído e imutável, utilizando a plataforma Hyperledger Fabric para garantir a privacidade dos usuários.

No estudo de [Díaz et al. 2019], os autores propõem um modelo de segurança para RES, além de desenvolver uma arquitetura específica para DApps. O trabalho analisa o uso das plataformas Ethereum e Hyperledger Fabric, optando pela Hyperledger Fabric devido à necessidade de privacidade na Ethereum, que, por ser uma rede pública, torna todas as transações visíveis aos participantes. Os resultados deste estudo destacam o desempenho do sistema baseado em *blockchain*, assegurando autenticidade, confidencialidade, integridade e disponibilidade dos dados em um ambiente controlado.

[2] `https://metamask.io/`
[3] `https://taho.xyz/`

O propósito do estudo de [Antwi et al. 2021] é abordar problemas de privacidade e segurança relacionados a RES utilizando a plataforma Hyperledger Fabric. O trabalho apresenta cenários específicos, discute os requisitos necessários para a implantação dessa tecnologia e destaca os desafios encontrados durante a pesquisa. No estudo de [Wang and Qin 2021], os autores exploram a melhoria do compartilhamento de dados de saúde utilizando *blockchain* e contratos inteligentes para assegurar o controle e a segurança das informações. Os resultados obtidos indicam que a estrutura da Hyperledger Fabric pode ser utilizada no desenvolvimento de DApps em grande escala, enquanto mantém a integridade dos dados dos pacientes.

A proposta deste artigo apresenta similaridades com os estudos discutidos nesta seção. A arquitetura proposta engloba a concessão de permissões para o uso dos dados do usuário, por meio de um módulo da *blockchain* destinado a proteger a privacidade dos dados dos usuários. A segurança é assegurada pelo registro das informações de forma imutável. Como diferencial, a arquitetura inclui um módulo especializado na preparação dos dados para consultas eficazes.

4. Arquitetura Proposta

A Figura 2 ilustra a arquitetura proposta para uma DApp baseada em *blockchain* voltada para *mHealth*, com foco na privacidade e segurança dos dados dos usuários de aplicações *mHealth*. Os componentes da arquitetura incluem o *front-end*, o *back-end* – que orquestra as chamadas realizadas pelo *front-end* aos demais componentes –, um banco de dados relacional, um serviço de mensageria e um serviço de mecanismo de análise e busca de dados distribuídos.

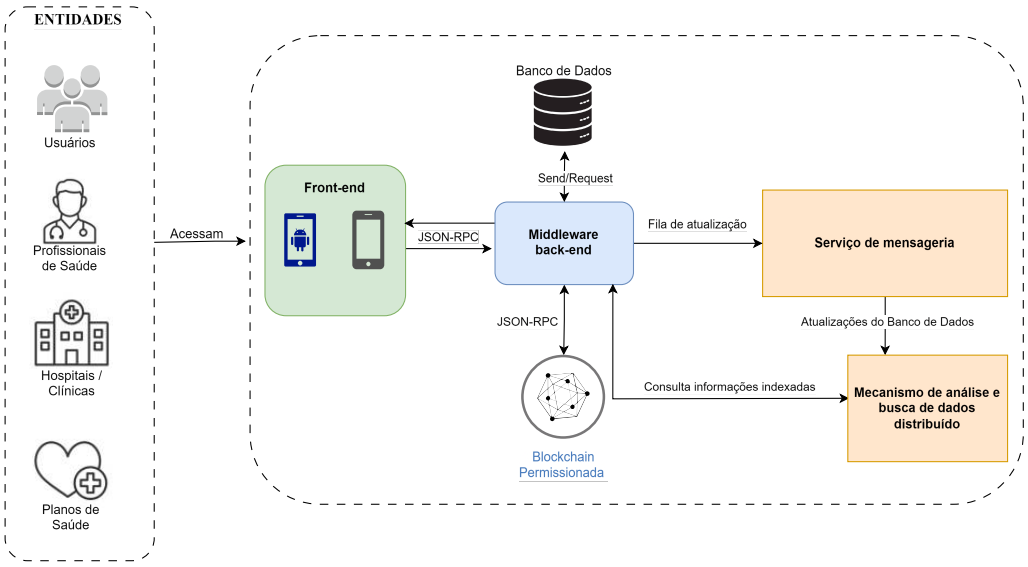

Figura 2. Proposta de arquitetura de aplicação descentralizada baseada em blockchain para *mHealth*.

Na arquitetura proposta, a *blockchain* oferece um serviço crucial, responsável pela privacidade e segurança dos dados do usuário. As aplicações *mHealth* não apenas fornecem serviços de saúde, mas manipulam dados que podem oferecer informações úteis para análises médicas. Levando em conta esse potencial de utilização dos dados, a arquitetura inclui componentes específicos que integram tecnologias de análise de dados.

4.1. Recursos da Arquitetura

Na arquitetura proposta, o *front-end* gerencia as informações necessárias para o funcionamento da aplicação *mHealth* [Istepanian 2022, de Faria et al. 2024] e pode ser desenvolvido utilizando *frameworks* ou bibliotecas adequados às demandas das aplicações. Quanto ao *Middleware (back-end)*, este pode ser desenvolvido em uma linguagem de *back-end* da preferência do desenvolvedor e atua como um elemento crucial na arquitetura da aplicação.

Para embasar a decisão sobre o tipo de rede e a blockchain que garanta a segurança dos dados dos usuários, é relevante destacar que se trata de uma aplicação de saúde com dados sensíveis. Desta forma, recomenda-se a escolha de uma rede privada [Díaz et al. 2019] para assegurar a proteção dos dados obtidos pelo aplicativo. Além da plataforma *blockchain*, este módulo inclui o desenvolvimento, validação e testes dos contratos inteligentes, visando implementar os requisitos para uma execução transparente e automatizada.

A adição de um módulo de *blockchain* traz significativas mudanças na gestão de dados da aplicação, permitindo que o usuário tenha total controle sobre seus dados de saúde e possa revogar o acesso a terceiros a qualquer momento [Stamatellis et al. 2020]. Além disso, este módulo facilita a disponibilização dos dados de saúde para outras instituições e plataformas, criando uma base de informações segura e confiável para estudos e pesquisas.

Na arquitetura proposta, outros tipos de armazenamento de dados são fundamentais, como um banco de dados relacional. Esse banco é responsável por armazenar informações de alto nível que não necessitam estar na *blockchain* (*off-chain*), tais como dados de acesso à plataforma, informações de questionários aplicados nos aplicativos, entre outros. Além disso, um mecanismo de análise e busca de dados distribuídos é utilizado para facilitar a criação de *dashboards* e outras análises de dados relevantes [Pham et al. 2018, Filho et al. 2020]. Para garantir que não ocorra perda de dados durante o processo de atualização entre o mecanismo de análise e o banco de dados relacional, um serviço de mensageria é empregado, permitindo que os dados de interesse da aplicação sejam transmitidos de forma organizada e coerente para o mecanismo de análise.

4.2. Exemplo: Aplicação mHealth IUProst®

O IUProst[4] é uma aplicação *mHealth* desenvolvida para auxiliar no tratamento da Incontinência Urinária (IU) em pacientes que realizaram a cirurgia de retirada da próstata (prostatectomia). Este projeto é uma iniciativa da Escola de Enfermagem da Universidade Federal de Minas Gerais (UFMG) em parceria com o Laboratório de Informática e Saúde do Instituto de Informática da Universidade Federal de Goiás (LabIS-INF-UFG) [Estevam 2022].

O aplicativo fornece uma oportunidade para o usuário realizar o tratamento da IU de maneira complementar ao acompanhamento do profissional de saúde. As principais funcionalidades do aplicativo são:

- orientações sobre o programa cognitivo comportamental para o tratamento de IU;

[4]www.iuprost.com.br

- exercícios para o treinamento da musculatura pélvica, que devem ser executados diariamente;
- textos e vídeos explicativos sobre os exercícios;
- acompanhamento do engajamento do usuário em seu tratamento e;
- acompanhamento da evolução do usuário.

Para manter o paciente motivado na execução dos exercícios e na continuidade do tratamento, o aplicativo, em sua versão 2.0, conta com a gamificação adaptativa utilizando o *framework* L, proposto por [Oliveira and Carvalho 2019]. Os blocos que compõem a arquitetura atual do IUProst estão divididos em:

1. *Front-end*: utilizando o *framework React-native* é possível o desenvolvimento de aplicações híbridas, onde podem ser gerados pacotes tanto para *Android* quanto para *IOS*, além da capacidade de criação de componentes da interface, assim como a utilização da linguagem de programação (*Javascript* ou *Typescript*), tornando assim uma ferramenta atrativa para a criação do aplicativo, executado no dispositivo do usuário.
2. *Back-end* (Servidor): A aplicação IUProst utiliza Node.js para a sua lógica de *back-end*, onde é possível construir APIs de forma escalável. Essa aplicação utiliza a API RESTful, que permite que a aplicação solicitante possa criar, ler, atualizar ou excluir (CRUD) informações, conforme as interações do usuário.
3. Banco de Dados: o MySQL foi escolhido como sistema de gerenciamento de banco de dados. A movimentação de informações desse banco vem das operações de CRUD.

A Figura 3 apresenta a arquitetura descentralizada baseada em *blockchain* para a aplicação *mHealth* IUProst.

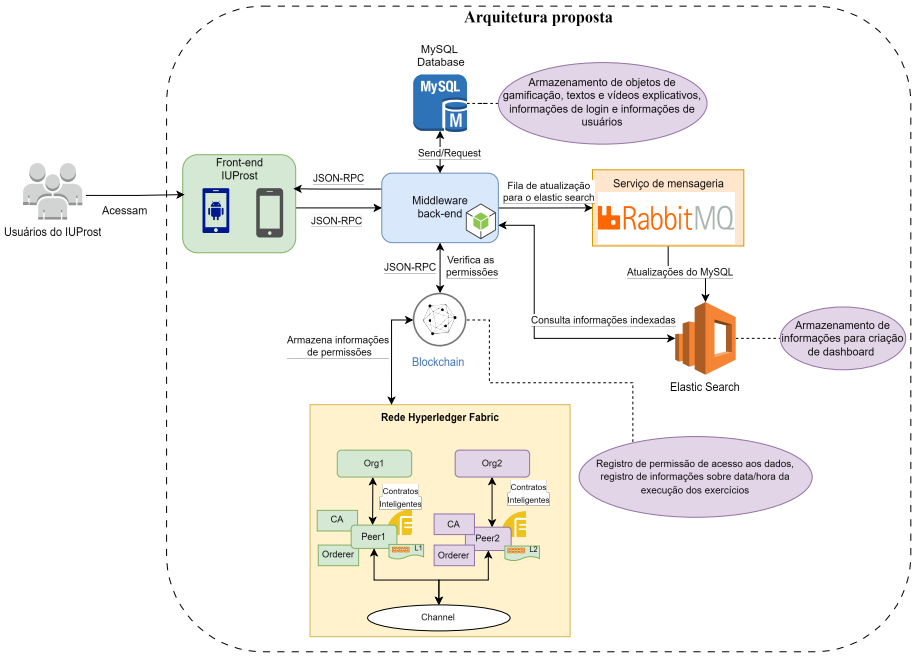

Figura 3. Arquitetura de aplicação descentralizada baseada em *blockchain* para o IUProst.

Nesta arquitetura, o *front-end* interage com o *back-end*, por meio de protocolos de comunicação (JSON-RPC). O *Middleware back-end* atua como API *gateway* para enviar requisições aos *end-points* da *blockchain*, armazena dados das ações dos usuários e, também, realiza a padronização das informações para armazenamento no Elastic Search, ação que facilita a consulta das informações indexadas para serem consumidas pela aplicação. A plataforma *blockchain* Hyperledger Fabric é utilizada para o armazenamento das informações de permissões de acesso aos dados, além de registrar informações de maneira imutável, dados como: registro de data/hora de acesso e realização de exercícios, concessão de acesso aos dados dos usuários e o registro de acessos aos dados.

Os elementos que compõem a arquitetura para a DApp baseada em *blockchain* no IUProst são:

Front-end – Usuário interage com as funcionalidades do sistema. Como o IUProst está em ambiente de produção e com muitas funcionalidades desenvolvidas, foi escolhido manter a tecnologia React Native durante este processo, visto que a tecnologia abrange os requisitos necessários, além de permitir uma implementação mista entre IOs e Android, e como consequência, permitindo um desenvolvimento mais ágil das demandas em termos de interface.

Middleware (Back-end) – Responsável por gerenciar todos os componentes da arquitetura: Blockchain (Hyperledger Fabric), Banco de dados (MySQL), fila de mensagens e o Elastic Search. Assim como o Front-end, o back-end foi mantido na mesma tecnologia anterior a arquitetura, pois as funcionalidades principais do aplicativo não se alteram. Como diversos componentes da nova arquitetura se diferem da arquitetura atual, novas funcionalidades devem ser implementadas. Para isso, a experiência da equipe de desenvolvimento em uma linguagem já conhecida é importante para, além de evoluir a arquitetura da aplicação, conseguir desenvolver novas demandas existentes.

Este componente também é responsável pela criptografia e descriptografia dos dados do usuário. Para garantir que os dados do usuário só possam ser utilizados após a permissão do mesmo, o *middleware* faz a criptografia das informações de acordo com uma chave pessoal do usuário disponível na blockchain. Ao ser solicitado algum dado de um usuário, este componente verifica se as informações estão liberadas, e caso esteja, a retorna de forma descriptografada para o usuário que está fazendo a requisição. Além disso, o *middleware* realiza a orquestração das trocas de dados entre os componentes, incluindo a decisão de quais dados são enviados para o Elastic Search.

Banco de dados (MySQL) – Responsável pelo armazenamento de informações não pessoais dos usuários, como: credenciais de acesso ao aplicativo, informações sobre questionários utilizados pelo aplicativo, vídeos e imagens ilustrativas de forma descriptografada.

Serviço de mensageria (RabbitMQ ou Kafka) – Responsável por manter a organização e o padrão entre o banco de dados e o serviço do Elastic Search. Essa funcionalidade, assim como o uso de um mecanismo de análise e busca de dados, são devido às necessidades de se prover funcionalidades voltadas à ciência de dados.

Mecanismo de análise e busca de dados distribuído (Elastic Search) - Juntamente com o serviço de mensageria, este serviço é voltado para análise de dados coletados no aplicativo. Elastic Search foi escolhido devido à sua facilidade durante a criação de métricas em direção à criação de dashboard.

***Blockchain* (Hyperledger Fabric)** – Responsável por gerenciar as permissões de uso de dados dos usuários, assim como armazenar informações leves, como data e hora da execução de um exercício. As informações que estão na blockchain somente são acessadas com a permissão do usuário e, com isso, é possível manter a privacidade de seus dados.

A escolha do Hyperledger Fabric considera sua arquitetura modular e flexível, que permite a personalização de diversos aspectos da rede, como o modelo de dados, o modelo de transações, o modelo de consenso, o modelo de identidade, entre outros. Essa arquitetura facilita a adaptação da rede às diferentes demandas e requisitos das organizações participantes, bem como a integração da rede com outros sistemas e tecnologias. Conforme a documentação do Hyperledger Fabric[5], os principais componentes da rede são:

- ***Peer***: é uma entidade que compõe a rede, que pode ter diferentes funções e responsabilidades, como:
  - ***Peers* de cliente**: são os peers que representam os usuários finais da rede, que podem criar e enviar transações para a rede, usando uma interface de aplicação (API).
  - ***Peers* de validação**: são os peers que armazenam e validam as transações e os blocos na rede, usando um ledger distribuído e um mecanismo de consenso.
  - **Peers de comprometimento**: são os peers que apenas recebem e armazenam os blocos validados.
  - ***Peers* de endosso**: são os peers que endossam as transações, ou seja, que verificam e assinam as transações, de acordo com uma política de endosso, que define quais e quantos peers devem endossar uma transação para que ela seja válida.
- ***Channels***: são os mecanismos que permitem a criação de sub-redes privadas e isoladas na rede, que podem ter diferentes organizações participantes, políticas, livro-razão (*ledger*) e contratos inteligentes (*chaincodes*). Os canais permitem que as organizações participantes compartilhem dados e transações de forma seletiva e confidencial, sem afetar ou interferir nos outros canais da rede.
- ***Chaincodes***: são os contratos inteligentes do Hyperledger Fabric, sendo códigos de programação que executam ações pré-definidas e automáticas na rede, de acordo com condições estabelecidas pelas partes envolvidas. Os *chaincodes* podem ser escritos em diferentes linguagens, como Go, Java ou Node.js, e podem ser instalados e invocados pelos *peers*. Os *chaincodes* podem acessar e modificar o estado do *ledger*, bem como emitir eventos para as aplicações.
- ***Ledger***: é o livro-razão digital compartilhado pela rede, que registra e armazena as transações e os blocos na rede, de forma imutável e auditável. O ledger é composto por dois componentes: o *world state*, sendo uma base de dados que armazena o estado atual dos ativos e dos dados na rede, e o blockchain, que é uma cadeia de

[5]https://hyperledger-fabric.readthedocs.io/en/release-2.5/

blocos que armazena o histórico das transações e das mudanças no *world state* na rede.

- **MSP**: é o provedor de serviços de membros (*Membership Service Provider*), que é o componente que gerencia a identidade e a associação dos participantes na rede, usando certificados digitais e Autoridades de certificação (CA). O MSP define e verifica as credenciais e os papéis dos participantes, bem como as políticas de acesso e de permissão na rede.
- **CA**: é a autoridade de certificação (*Certificate Authority*), sendo o componente que emite e revoga os certificados digitais dos participantes na rede, usando um protocolo de registro e inscrição (Enrollment and Registration).
- **Organização**: conjunto de diferentes peers unidos. Representa um grupo que trabalha com um mesmo propósito e nível de informações.
- *Orderer*: Tipo especial de Peer. Mantém o estado consistente dos ledgers na rede. Promove o consenso entre os peers.

5. Discussão

As DApps baseadas em *blockchain* têm o potencial de apoiar os cuidados de saúde, colocando o paciente no centro do sistema de saúde e aumentando a segurança, a privacidade e a interoperabilidade dos dados [Onik et al. 2019] [Pandey and Litoriya 2020].

As características de segurança e imutabilidade dos dados garantidas pela tecnologia *blockchain* são relevantes no contexto das aplicações *mHealth*. A capacidade de descentralização da *blockchain* possibilita a implementação de arquiteturas que permitem o compartilhamento de dados de forma mais segura, sem depender de uma autoridade central.

Além disso, o uso dos contratos inteligentes permite o gerenciamento do consentimento de acessos aos dados de forma transparente e automatizada. Adicionalmente, na arquitetura, foram propostos elementos visando auxiliar as aplicações na preparação dos dados, facilitando o uso de mecanismos de análise e busca de dados distribuídos. Garantir a segurança e a privacidade dos dados dos usuários de aplicações *mHealth* é fundamental. Portanto, as estruturas utilizadas em seu desenvolvimento devem incorporar recursos de segurança robustos para proteger contra acesso não autorizado aos dados dos usuários.

As contribuições do nosso trabalho podem ser resumidas da seguinte forma:

- a privacidade do acesso aos dados de saúde é realizada, registrando na *blockchain* o consentimento de acesso aos dados pelo usuário. Desta forma, os dados somente são acessados, após a verificação do consentimento registrado na blockchain;
- a segurança é possibilitada pelo uso de uma *blockchain* permissionada, em que os participantes da rede são autorizados e identificados; e
- utilização de mecanismos que possibilitam o uso de tecnologias para preparar os dados, facilitando assim processos de análise de dados.

6. Considerações Finais

Este estudo oferece uma análise da arquitetura de aplicações descentralizadas baseadas em *blockchain*, apresentando uma proposta de arquitetura para orientar o desenvolvimento de aplicações *mHealth*. Um exemplo de aplicação prática da arquitetura é apresentado como prova de conceito e avaliação.

As decisões de projeto são detalhadas, incluindo a seleção das tecnologias para a aplicação *mHealth* IUProst. Investigar questões de segurança e privacidade em DApps representa uma oportunidade valiosa para pesquisas adicionais, dadas as evidências de experimentos e uso de *blockchain* na área da saúde.

Como trabalhos futuros, além da implementação da arquitetura proposta na aplicação *mHealth* como prova de conceito, podem ser realizados estudos comparativos das métricas de desempenho de DApps, considerando diferentes abordagens em relação ao tipo de rede. Além disso, a criação de ferramentas de teste para avaliar o desempenho da *blockchain* pode validar sua utilização.

Referências

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M. H., and Kerrache, C. A. (2021). The case of hyperledger fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*, 2(1):100012.

Buchain, L. C. (2021). Proteção de dados: legítimo interesse e consentimento. `https://lume.ufrgs.br/handle/10183/255007`. Acesso em: 29 de dezembro de 2023.

de Faria, B. S. F., Carvalho, C., Triches, M. I., de Araújo Vieira, L. M. S. M., and de Oliveira Sato, T. (2024). Mobile health technologies for workers' health and wellbeing: A systematic search of mhealth applications in brazil. *Journal of Bodywork and Movement Therapies*, 38:54–59.

Díaz, A., Armas, J., Madrid, J., and Peña, C. (2019). Security model to protect patient data in mhealth systems through a blockchain network. `https://lume.ufrgs.br/handle/10183/255007`. Acesso em: 05 de abril de 2024.

Estevam, F. E. B. (2022). Iuprost: aplicativo movel para controle da incontinencia urinaria em homens submetidos a prostatectomia radical. `https://repositorio.ufmg.br/handle/1843/50908`. Acesso em: 29 de março de 2024.

Filho, I. B., Sampaio, S. C., Tenório, J. C. A., de C. Filho, E. V., de C. Pessoa, M. E., Malaquias, R. S., and Fernades, P. A. (2020). Development of a health dashboard for an electronic health record system. In *2020 20th International Conference on Computational Science and Its Applications (ICCSA)*, pages 16–22.

Istepanian, R. S. (2022). Mobile health (m-health) in retrospect: the known unknowns. *International journal of environmental research and public health*, 19(7):3747.

Oliveira, L. W. and Carvalho, S. T. (2019). Framework l para desenvolvedores de mhealth no contexto de self-care e gamificaçao. In *Anais Estendidos do XIX Simpósio Brasileiro de Computação Aplicada à Saúde*, pages 61–66. SBC.

Onik, M. M. H., Aich, S., Yang, J., Kim, C.-S., and Kim, H.-C. (2019). Blockchain in healthcare: Challenges and solutions. In *Big data analytics for intelligent healthcare management*, pages 197–226. Elsevier.

Pandey, P. and Litoriya, R. (2020). Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. *Health Policy and Technology*, 9(1):69–78.

Pham, Q., Graham, G., Lalloo, C., Morita, P. P., Seto, E., Stinson, J. N., and Cafazzo, J. A. (2018). An analytics platform to evaluate effective engagement with pediatric mobile health apps: Design, development, and formative evaluation. *JMIR Mhealth Uhealth*, 6(12):e11447.

Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*.

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., and Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, 20(22).

Taralunga, D. D. and Florea, B. C. (2021). A blockchain-enabled framework for mhealth systems. *Sensors*, 21(8):2828.

Wang, Q. and Qin, S. (2021). A hyperledger fabric-based system framework for healthcare data management. *Applied Sciences*, 11(24).

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)*, pages 243–252. IEEE.

Zheng, P., Jiang, Z., Wu, J., and Zheng, Z. (2023). Blockchain-based decentralized application: A survey. *IEEE Open Journal of the Computer Society*.