

UTILIZAÇÃO DE SIDECHAIN EM APLICAÇÃO BLOCKCHAIN ENVOLVENDO GRANDES VOLUMES DE DADOS¹

Victor Luiz Bernardes², Adriano Fiorese³

¹ Vinculado ao projeto “Seleção de Provedores de Nuvem Computacional - Estudo para aplicação de blockchain em redes ad hoc veiculares”

² Acadêmico (a) do Curso de Ciência da Computação. – CCT– Bolsista PROBIC/UDESC

³ Orientador, Departamento de Ciência da Computação – CCT – adriano.fiorese@udesc.br

Com a diminuição de custos e avanço das técnicas de armazenamento de informações, cada vez mais informação que desempenha um papel fundamental na sociedade e que influencia a tomada de decisão tem sido armazenada. O conjunto dessa informação armazenada, uma vez processada, molda a forma como interagimos no mundo físico. Com a crescente digitalização dos registros de saúde e o avanço do número de dados possíveis de serem analisados, as informações médicas, incluindo informações de usuários do sistema de saúde (ex: pacientes) tornaram-se uma fonte importante de conhecimento para pesquisas, melhorias em sistemas de saúde, equipamentos e métodos mais eficazes para tratamento de doenças.

A utilização de tecnologias de armazenamento como *blockchain* tem crescido na área de saúde, promovendo o armazenamento de informações de forma imutável e descentralizada, onde é possível registrar dados de pacientes de forma confiável sem o intermédio de uma terceira parte que faça a validação dos dados. Porém, a tecnologia *blockchain* possui algumas limitações e uma delas está no armazenamento de arquivos como imagens, vídeos e arquivos que possuem tamanho elevado (i.e., a partir dos megabytes). Essa limitação decorre de em certo momento o tamanho do *blockchain* ou dos seus blocos interfere nos tempos de validação dos blocos por consenso e conseqüente sincronização da *blockchain* por todos os nós envolvidos. Essa interferência se reflete em tempos inaceitáveis para execução de transações (armazenamento nesse caso) de grandes arquivos (seja em grandes blocos ou de forma fragmentada em diversos blocos). Uma alternativa para este problema é a utilização de *sidechains*.

Uma *sidechain* pode ser definida como uma comunicação bidirecional que permite a troca de informações entre a cadeia de blocos principal e uma cadeia de blocos secundária. *Sidechains* podem ter seu próprio mecanismo de consenso, implementações de novas funcionalidades e outras características diferentes da rede principal. Portanto, uma *sidechain* em conjunto com uma *blockchain* pode aumentar a escalabilidade do número de transações por segundo e possibilita armazenar arquivos médicos grandes que prejudicariam o desempenho da *blockchain* principal.

Este trabalho de iniciação científica tem como objetivo a análise, pesquisa e a criação de uma proposta de armazenamento utilizando *blockchain* e *sidechain* para armazenar arquivos médicos grandes como escaneamentos (raio-x) e prontuários médicos de modo a observar o desempenho da rede *blockchain* em termos de transações por segundo, tempo de recuperação dos arquivos e tamanho da rede para avaliar a viabilidade de utilização no contexto de um ambiente de cuidados de saúde inteligente. Para tanto, foi realizada uma extensa pesquisa bibliográfica na área de aplicações médicas utilizando *blockchain* bem como o uso de redes P2P dentro deste ambiente. Também foram realizadas pesquisas para determinar ferramentas e plataformas que seriam

utilizadas no trabalho a fim de obter a melhor escolha para o cenário de consórcio entre instituições de cuidados de saúde.

As ferramentas utilizadas para criação e configuração da rede Blockchain foram o *framework* quorum junto à rede goquorum, a qual é uma rede privada permissionada baseada na rede Ethereum. Visto que o *framework* possui uma gama de protocolos de consenso baseado em prova de autorização (PoA), a rede se fez ideal para o cenário de múltiplas instituições de saúde sem a necessidade de mineração (nome dado ao mecanismo de validação das transações realizadas), como é o caso da prova de trabalho (PoW) utilizada em redes públicas. Para a criação da *sidechain* foi utilizado o protocolo IPFS (InterPlanetary File System), utilizando-se dos principais conceitos como endereçamento por conteúdo, ou seja, cada conteúdo é único e possui um identificador (CID) na rede bem como tolerância a falhas.

Conforme a Figura 1, para realizar a interação entre a *blockchain* e IPFS foi necessário desenvolver uma aplicação que utiliza das APIs da blockchain para interagir com o contrato inteligente. A aplicação recebe os arquivos e informações do usuário (id do médico, data dos exames, tipo do exame, nome do paciente, CPF do paciente). Primeiramente são salvos os arquivos na rede IPFS usando API, e será retornado o identificador (CID) do arquivo na rede para a aplicação, logo após obter o CID do arquivo a aplicação irá interagir com o contrato inteligente e armazenar os dados junto ao CID dos arquivos, salvando todos os dados em uma transação na *blockchain*.

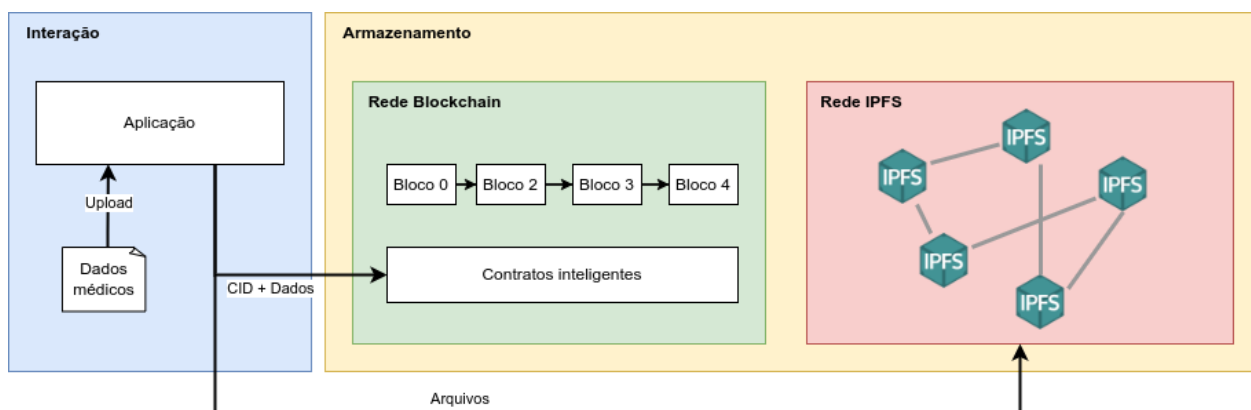


Figura 1. Interação entre Blockchain e IPFS

O trabalho apresentou um modelo de persistência no qual possibilitou o armazenamento de arquivos e imagens médicas sem o custo adicional na rede principal, deixando a *blockchain* com tamanho reduzido em comparação com trabalhos que realizam a persistência somente na rede principal.

Como trabalhos futuros, intenciona-se a criação de testes por categorias de exames médicos e escaneamentos a fim de verificar qual a melhor abordagem de configuração do IPFS para determinada categoria de exames e suas variações de tamanho; a implementação de um algoritmo de criptografia para manter os dados do IPFS anônimos bem como a implementação de serviços de monitoramento para o IPFS junto a um *dashboard* de análise para redes como o Grafana.

Palavras-chave: Blockchain, Sidechain, Registros Eletrônicos em Saúde (EHR).