Tratamento de Concessão e Revogação de Acesso a Registros Eletrônicos de Saúde em Blockchain

Ronan D. Mendonça[1], **Otávio S. Gomes**[1], **Alex Borges Vieira**[1], **José Augusto Nacif**[1]

[1]Instituto de Ciências Exatas e Tecnológicas, Campus UFV-Florestal
Universidade Federal de Viçosa

{ronan.dutra,otavio.s.gomes,jnacif}@ufv.br, alex.borges@ufjf.edu.br

Abstract. *The sharing of electronic health records is essential for the improvement and agility of medical procedures concerning patients. These records are considered highly critical in terms of security, and access to them must be controlled safely and effectively. The control of this data can be carried out in a traditionally centralized way. However, with blockchain technology, the records' management becomes secure, transparent, and includes the transaction history. This article presents a framework for using blockchain to control access and share electronic health records. Our structure can maintain data ownership control through authorization and revocation of permissions related to specific data in a simple and efficient way. The patient-centered control of permissions has resulted in security advantages over legislation and fragmented data sharing between patients, doctors, and healthcare institutions.*

Resumo. *O compartilhamento de registros eletrônicos de saúde é extremamente importante para a melhoria e agilidade dos procedimentos médicos em relação ao paciente. Estes registros são considerados altamente críticos em relação à segurança e o acesso a eles deve ser controlado de forma segura e eficaz. O controle desses dados pode ser realizado de maneira tradicionalmente centralizada, porém, com a utilização da tecnologia blockchain, o controle dos registros se torna seguro, transparente e com histórico das transações. Neste artigo, apresentamos uma estrutura para a utilização de blockchain no controle de acesso e compartilhamento de registros eletrônicos de saúde. Essa estrutura é capaz de manter o controle de posse dos dados por meio de autorização e revogação de permissões relacionadas aos dados individualizados de maneira simples e eficiente. O controle das permissões centrado no paciente resultou em vantagens de segurança em relação à legislação e ao compartilhamento fragmentado dos dados entre paciente, médicos e instituições de saúde.*

1. Introdução

A importância que vem sendo direcionada à disponibilização de dados relacionados aos cuidados com a saúde está impulsionando inúmeros estudos voltados para este segmento. A geração de dados relacionados à saúde acontece de maneira contínua e estes dados são considerados extremamente sensíveis e por isso, há uma grande preocupação em relação à segurança dos dados e à privacidade dos usuários. Uma vez que as pessoas estão cada vez mais focadas em acompanhar seu estado de saúde por meio do monitoramento dos seus dados, o controle individualizado passa a ser um requisito fundamental na obtenção

de privacidade e segurança de acesso aos dados. Isso implica diretamente na maneira de acompanhamento e decisão em conceder ou revogar o acesso aos dados por terceiros. Desta forma, a abordagem centrada no paciente implica em manter os dados de saúde privados, e todos que tenham interesse nestes dados devem pedir permissão ao próprio paciente para acessá-los. Existe uma variedade de aplicações que fazem parte deste ecossistema que envolve dados médicos de paciente como, por exemplo, hospitais, farmácias, cuidadores, médicos, exames e plano de saúde. Essas aplicações geram uma diversidade de dados que se relacionam sempre ao paciente e que, se controlado por ele, a privacidade e segurança pode ser preservada [Zhuang et al. 2020].

Nos últimos anos, com o aumento do interesse de indivíduos e governos acerca da segurança de dados no ambiente virtual, ocorreram mudanças na lei de proteção de dados em diversos países. Em 2016, foi proposta a *General Data Protection Regulation* (GDPR)[1] pela união europeia, lei criada com o objetivo de regulamentar o uso e acesso aos dados de cidadãos europeus. A lei entrou em vigor em maio de 2018 e desde então, foi seguida por inúmeras legislações ao redor do mundo. No Brasil, foi proposta a Lei Geral de Proteção de Dados (LGPD)[2], que foi sancionada em agosto de 2018. No país, a lei entrou em vigor em dezembro de 2020 e já impacta o tratamento de dados online. Entre os dados descritos pela lei como sensíveis, estão os dados de saúde. Esses dados devem ser mantidos sob controle de quem os gerou, sendo vedada a utilização para fins comerciais. Nesse sentido, o paciente deve ser capaz de acessar, apagar e transferir seus dados de qualquer instituição a qualquer momento.

Entre as ferramentas utilizadas pelas instituições de saúde atualmente, o registro eletrônico de saúde (*Electronic Health Records* – EHR) é um exemplo. O EHR é o padrão de armazenamento de dados de saúde em que os dados são controlados de forma centralizada por instituições de saúde. Diferentemente do funcionamento atual dessas instituições, que mantém dados pessoais de seus pacientes sob seu controle, a lei transfere para os pacientes o domínio sobre seus dados. As tecnologias recentes podem permitir que o processo de coleta, controle e armazenamento dos dados sejam centrados no indivíduo, auxiliando no controle de acesso, compartilhamento e análise de seus dados. Nessa linha, *blockchain* [Nakamoto and Bitcoin 2008] tem um grande potencial em favorecer significativamente a área da saúde[Hölbl et al. 2018] e [Hussien et al. 2019].

Nesse contexto, propusemos uma estrutura, (Figura 2), que utiliza de *blockchain* para gerar um controle descentralizado de acesso aos dados de saúde por meio de concessões e revogações registradas pelo paciente. Por meio desta solução, a tecnologia *blockchain* pôde ser utilizada para autenticação e auditabilidade do controle de acesso aos dados. As *blockchains* permitem o armazenamento seguro e imutável de dados, com aplicação direta na resolução de problemas de segurança e privacidade no cenário da saúde. Utilizamos os contratos inteligentes como base das regras de negócio, o que permite o uso destes por inúmeras aplicações desenvolvidas com o objetivo de atender tanto ao paciente quanto aos médicos e instituições de saúde. Diferentemente dos trabalhos existentes, nossa estrutura é capaz de registrar na *blockchain* autorizações de acesso a dados e revogá-las, garantindo assim rastreabilidade de acesso aos dados e mantendo o

[1] `https://gdpr-info.eu/`

[2] `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm`

controle de acesso centrado no paciente.

A utilização de *blockchain* em aspectos de segurança e privacidade de dados disponibilizados no setor de saúde são constantemente citados como direcionamento de pesquisa [Litvin et al. 2019]. Nesse sentido, analisamos as possíveis implicações da união entre as tecnologias *blockchain* e EHR, considerando suas características de segurança e privacidade. Baseado nesses requisitos é que este trabalho foi desenvolvido. Em nossa estrutura, propusemos a validação do uso de *blockchain* com a finalidade de controle de acesso aos dados proporcionando uma possibilidade de interoperabilidade de autorização e revogação de acesso entre aplicações. No entanto, é necessário prover formas confiáveis para a disponibilização destes recursos, e nossa solução auxilia favorecendo a adesão pela utilização de *blockchain* no intuito de melhorar a segurança e privacidade do usuário em relação aos seus dados de saúde.

O restante deste trabalho está organizado da seguinte forma. Na seção 2 são apresentados os conceitos básicos para o entendimento deste trabalho, quais sejam, os registros médicos, a tecnologia *blockchain*, contratos inteligentes e plataformas *blockchain*, junto aos trabalhos relacionados encontrados na literatura. Na seção 3 é apresentada a proposta deste trabalho, contendo o modelo de arquitetura e os contratos inteligentes desenvolvidos. Na seção 4 é detalhada a implementação dos contratos inteligentes, incluindo a configuração da *blockchain*. Na seção 5 estão descritas e discutidas as avaliações dos resultados. Por fim, na seção 6 é apresentada a conclusão, limitações e trabalhos futuros.

2. Referencial Teórico

2.1. Registros Eletrônicos de Saúde

O Registro Eletrônico de Saúde (*Electronic Health Records* – EHR) é um padrão de informações de saúde para serem armazenadas eletronicamente em formato digital. Normalmente são utilizados por uma variedade de aplicações com foco nos cuidados da saúde. São referidos e encontrados na literatura com algumas ramificações como *Personal Health Record* (PHR) e *Eletronic Medical Record* (EMR). O PHR é uma utilização específica do registro eletrônico de saúde pelo qual os pacientes são os responsáveis por controlar o acesso às informações, gerenciando e rastreando os seus próprios cuidados de saúde [Zhang et al. 2018].

As aplicações EHRs podem fornecer vários benefícios, porém é eminente o aumento do risco de exposição de dados, uma vez que são suscetíveis a ameaças de segurança e privacidade. Sendo a segurança e a privacidade quesitos importantes para este tipo de aplicação, elas demandam mecanismos eficientes para o controle e validação de acesso, integridade e interoperabilidade de dados. As implementações que utilizam os Registros Eletrônicos de Saúde são encontradas na maioria das vezes utilizando uma forma centralizada para armazenamento dos dados. Em estudos com referência ao termo PHR são utilizadas abordagens centrada no paciente. A utilização de Registros Eletrônicos de Saúde ainda enfrenta desafios relacionados aos princípios de segurança e que podem ser superados com o uso da tecnologia *blockchain*, considerando que a *blockchain* foi desenvolvida com base em criação de transações de forma segura e sem a necessidade de um terceiro confiável [Siyal et al. 2019].

2.2. Blockchain

Blockchain é uma tecnologia que armazena registros de transações de forma distribuída, composta por inúmeros participantes, e que não há necessidade de um controle centralizado. As informações ficam organizadas em blocos encadeados por meio de *hashes* criptográficos [Nakamoto and Bitcoin 2008]. Esses blocos contêm cabeçalho e uma lista de transações conforme ilustra a Figura 1.

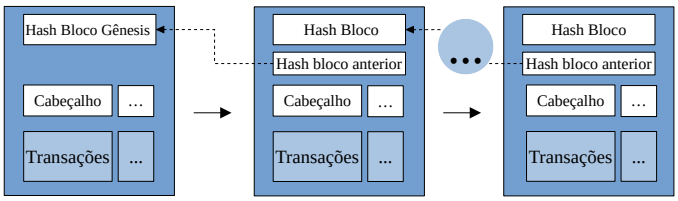


Figura 1. Cadeia de blocos.

A aplicação da tecnologia *blockchain* é diversificada e pode atingir inúmeras soluções de problemas como a validação de acesso, integridade e interoperabilidade de dados [Gordon and Catalini 2018]. Em relação à registros de saúde, a *blockchain* pode oferecer maior transparência, controle de acesso e segurança das suas transações.

A utilização do conceito de contratos inteligentes pela tecnologia *blockchain* aumenta as possibilidades de uso e seu funcionamento. Os contratos são implementados em uma determinada linguagem de programação por meio de scripts e armazenados na rede. As regras dos contratos são executadas pela rede da forma como foram estabelecidos.

Os tipos de *blockchains* são classificados basicamente de acordo com a forma de acesso e proteção das transações armazenadas. Os tipos encontrados são as públicas, privadas e de consórcio. As especificações de protocolo de consenso, proteção de acesso às informações e controle da forma de distribuição diferenciam os tipos de *blockchain*.

Em uma *blockchain* privada as respostas são mais rápidas e seguras, porém o controle é exercido por um proprietário específico e os nós precisam de permissão para ingressarem na rede. A *blockchain* privada é mais rápida, eficiente e segura. Na *blockchain* pública, por sua vez, a rede é totalmente descentralizada e pode conter vários nós e qualquer nó pode ingressar à rede. Porém, apenas nós sincronizados são utilizados para consenso. Uma *blockchain* de consórcio é composta por nós de organizações específicas que se unem e controlam quem pode ter acesso à rede. A rede resultante do consórcio é parcialmente descentralizada [Rouhani and Deters 2017] [Wang et al. 2018].

2.3. Contratos Inteligentes

Contratos Inteligentes (*Smart Contracts*) são programas auto executáveis e auto impositivos que funcionam de acordo com condições previamente acordadas [Hewa et al. 2021]. Esses contratos são capazes de implementar determinadas operações dentro da *blockchain* e funcionam como aplicações decentralizadas. Entre os benefícios da utilização de contratos inteligentes apontados por [Hewa et al. 2021] estão a eliminação da necessidade de um terceiro confiável para efetuar transações, a integridade e a transparência das transações e a autonomia de execução e a precisão dos contratos, uma vez que são imutáveis e são executados quando as pré condições são atendidas.

Devido ao caráter complementar que os contratos possuem em relação à *blockchain*, eles se tornaram parte essencial das *blockchains* que surgiram após o Bitcoin, proposto por [Nakamoto and Bitcoin 2008]. Com a utilização desses contratos, as *blockchains* tiveram sua capacidade de armazenamento aprimoradas. Um contrato permite definir um comportamento para um determinado estado e atender necessidades de aplicações diversas. Nesse sentido, os contratos inteligentes são capazes de executar transações muito mais complexas dentro da *blockchain* do que simplesmente a troca de moeda.

A partir dessas características, inúmeras aplicações podem ser desenvolvidas baseadas no uso de contratos inteligentes como, por exemplo, aplicações financeiras (gerenciamento de moeda, serviço de garantia, procedimentos de auditoria, empréstimo), aplicações médicas (gestão de informações de saúde, proteção de dados de pesquisa clínica, monitoramento e tratamento automatizado de pacientes, gerenciamento de identidade e controle de acesso, proteção de dados de identidade), aplicações imobiliárias, aplicações de acordos contratuais, aplicações de internet das coisas, aplicações de serviços de telecomunicações, aplicações de gestão de logística, além de aplicações entre diferentes indústrias [Hewa et al. 2021].

2.4. Trabalhos Relacionados

A aplicação da *blockchain* em diversos segmentos vem mostrando que, cada vez mais, a tecnologia está sendo sugerida e aceita em áreas que exigem segurança das informações e interoperabilidade facilitada. A *blockchain* pode ser usada para armazenar e compartilhar dados que podem ser facilmente verificados para confirmação de sua autenticidade. Segundo [Kshetri 2018], ela pode fornecer transparência através da imutabilidade das transações, o que gera rastreabilidade e aumenta a confiança dos participantes. Os trabalhos apresentados nesta Seção envolvem a criação de redes blockchain e a utilização de contratos inteligentes para resolver os problemas como os de interoperabilidade e segurança relacionados aos dados de saúde.

A rede desenvolvida por [Azaria et al. 2016], nomeada MedRec envolve a utilização da *blockchain Ethereum* como base de armazenamento de identidades e relacionamentos entre prestadores de serviço e pacientes, além de banco de dados externo para o armazenamento definitivo dos dados de saúde. A rede proposta requer a existência de um nó provedor e um nó do cliente, com funções diferentes, permitindo que o nó do cliente seja mais leve e armazene menos informações. Apesar de similar à nossa proposta, a rede MedRec é muito mais complexa, considera a existência de nós com funcionalidades diferentes na rede, algo não comum à *blockchain Ethereum*, além de requerer a existência de um nó pertencente ao paciente. Nossa aplicação se diferencia ao apresentar uma infraestrutura mais simples e direta, oferecendo garantias semelhantes à apresentada pela rede MedRec.

Em [Griggs et al. 2018], os autores criam contratos e os implementam para a *blockchain* privada *Ethereum*. Por eles, são controladas as comunicações entre sensores e dispositivos que registram os dados de eventos de monitoramento de pacientes na *blockchain*. Apesar de afirmarem que os registros de saúde do paciente são mantidos em privacidade, o sistema apenas mantém um histórico de acessos e modificações dos dados, o que coloca nosso trabalho com vantagens em relação ao controle consciente e auditabilidade de acesso aos dados.

O estudo feito por [Zhuang et al. 2020] propõe a utilização da tecnologia *blockchain* em um modelo para enfrentar os desafios de controle de registros médicos. O modelo consiste em implantar uma *blockchain* que garanta o acesso autorizado a informações da rede e manter o controle de usuários para pacientes. Neste modelo os pacientes têm controle sobre quem pode acessar seus registros de saúde por meio de uma lista. Os autores realizaram uma simulação com base na *blockchain Ethereum*, contratos inteligentes e um conjunto de dados. Foram computados e analisados o tempo para recebimento de permissão, os dados criptografados e a chave de descriptografia e o número de solicitações envolvidas. O maior desafio relatado e enfrentado no trabalho foi a escalabilidade do modelo uma vez que cada participante deve prover a infraestrutura do nó de conexão com a rede e a instituição. Portanto, nossa aplicação oferece os recursos apresentados nesse trabalho e ainda simplifica o acesso a rede blockchain, uma vez que os participantes apenas usufruem de uma rede pública.

[Huang et al. 2021] projetou e implementou uma proposta de *blockchain* para possibilitar a auditabilidade em manipulação de registros médicos. Cada manipulação realizada nos dados é gravada na *blockchain* como uma transação, se tornando um armazenamento permanente. As manipulações de dados são rastreadas e não sofrem alterações por meio das próprias características da *blockchain*. Algumas características presentes em nossa solução não são incorporadas neste trabalho, como o um controle dos acessos aos registros garantidos pela *blockchain* e a garantia que este controle seja centrado no paciente.

Foram apresentados trabalhos relacionados ao tratamento de registros médicos com o uso blockchain. Esses estudos apresentam abordagens diferentes daquela desenvolvida para a metodologia proposta pelo presente trabalho. Enquanto os trabalhos encontrados mantêm o foco sobre a elaboração de técnicas para garantir a imutabilidade, segurança e privacidade dos dados, nosso trabalho possibilita que todas essas garantias sejam controladas pelo paciente e alcance os requisitos de uma aplicação centrada no paciente. Nossa solução ainda é adaptável às diferentes aplicações, em termos de dados médicos, de acordo com suas funcionalidades e requisitos.

3. Modelo arquitetural

Neste trabalho é proposto uma estrutura de controle de concessões e revogações de acesso aos registros de saúde compartilhados usando a tecnologia *blockchain*. Esta estrutura permite aos indivíduos controlarem o acesso aos seus próprios registros de saúde, concedendo e revogando acesso a partes interessadas nos registros. O modelo foi construído para permitir que os acessos aos registros médicos sejam realizados a partir da verificação de permissões alocadas em uma blockchain. A aplicação cliente, também chamada de *decentralized application (dApp)* ou aplicação descentralizada, é responsável em verificar as permissões registradas na blockchain para assim prover o recurso solicitado. Por outro lado temos a blockchain que persiste os dados das permissões de forma imutável e atende as requisições das *dApps*.

A Figura 2 apresenta o modelo de controle de acesso aos registros médicos compartilhados por *blockchain* e que foi utilizado para o desenvolvimento da solução deste trabalho. Existem quatro tipos de atores externos que atuarão diretamente com as funcionalidades para o andamento da estrutura. São eles o Paciente, o Pesquisador, a Emergência

e outras instituições de saúde, que neste modelo foram representadas pelos hospitais e farmácias. Os atores interagem com a estrutura modelada nas formas cabíveis a cada um e que são relacionadas numericamente na Figura 2.

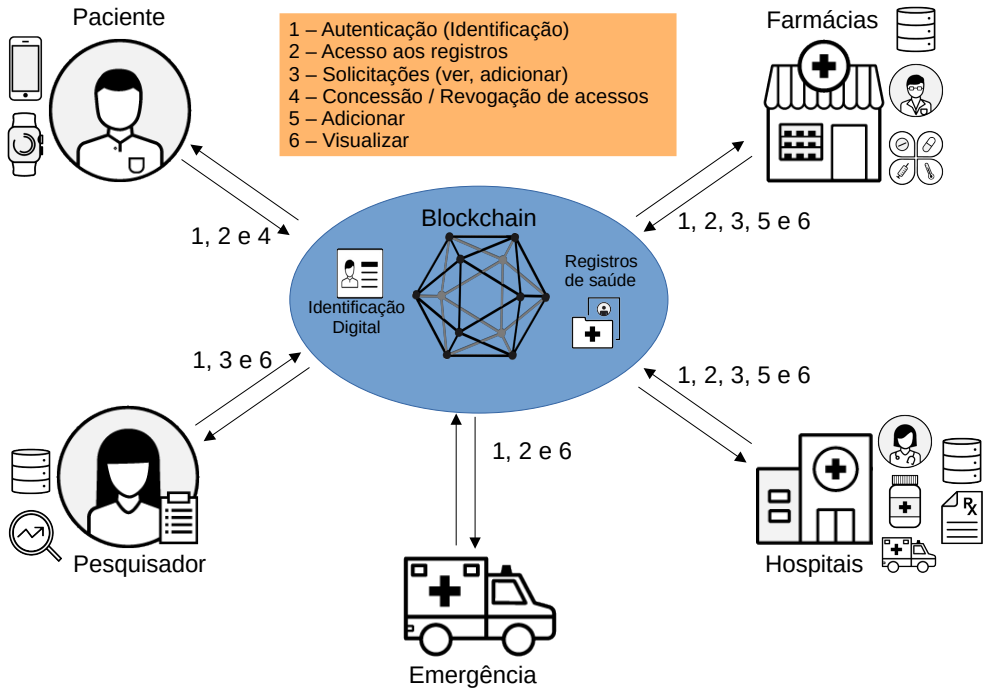


Figura 2. Controle de registros médicos compartilhados em *blockchain*.

Para o ator Paciente são dadas as opções de interação por meio da autenticação, acesso aos registros e a concessão e revogação de acessos. Estas opções os permitem se identificar para o acesso às outras funcionalidades, acessar os seus próprios registros e conceder ou revogar permissões de acesso. As concessões e revogações são detalhadas conforme o diagrama de sequência da Figura 4. Note que a Concessão/Revogação de acessos é dada apenas ao Paciente, isto é, o proprietários dos dados. Assumimos que a identificação é realizada pelo usuário por meio de uma credencial confiável fornecida por uma *self-sovereign identity - (SSI)* implementado em blockchain [Kondova and Erbguth 2020].

Ao ator Pesquisador são dadas as possibilidades de autenticação, solicitações para ver e visualizar, onde, após se identificar, ele poderá realizar solicitações de acesso do tipo "Ver", e caso obtiver autorização, visualizar os registros concedidos. Este ator Pesquisador foi incluído com o objetivo de criar a possibilidade de acesso aos registros por aplicações com a finalidade de utilização de técnicas de Inteligência Artificial na geração de conhecimento sobre os dados.

O ator Emergência é um tipo especial de ator que, ao ser identificado como tal, obtém as credenciais para acessar os registros e visualizá-los sem a necessidade de realizar solicitações e aguardar a concessão. Por meio deste recurso, os pacientes em estado de emergência podem receber atendimento personalizado e com maior agilidade em relação ao acesso aos seus dados, uma vez que o tempo para apenas visualizar um dado sem a necessidade de autorização cai drasticamente. As instituições de saúde são atores que

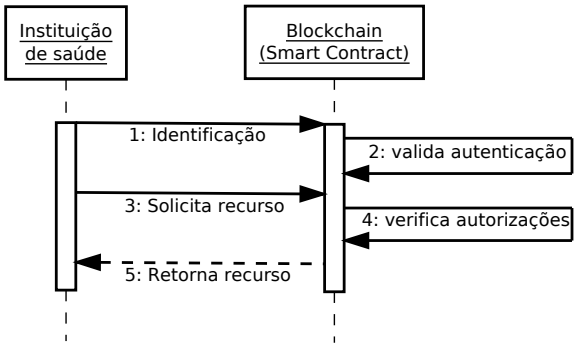


Figura 3. Diagrama de acesso aos dados dos pacientes.

interagem com as funcionalidades de autenticação, acesso, solicitações, adicionar e visualizar os registros com acessos concedidos. Assim como todos os atores, as instituições também precisam primeiramente se identificar. No diagrama de sequência apresentado na Figura 3 é observado os passos para acesso aos registros uma vez que já existe autorização para acesso aos mesmos. As solicitações de acesso feitas por esse ator podem ser dos tipos "Ver" e "Adicionar". Ao receber a concessão para ver os dados referentes ao paciente, a Instituição será capaz de visualizar os dados autorizados, e a concessão de adicionar dará permissão para criar um dado referente ao paciente.

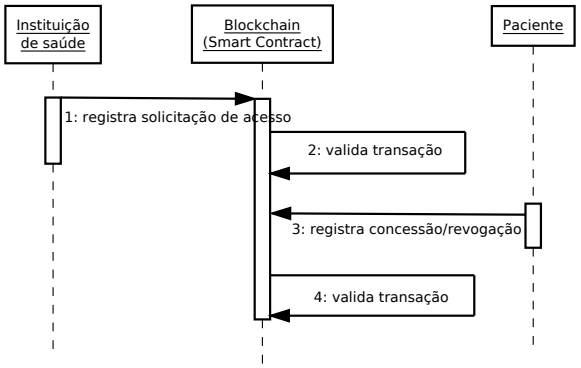


Figura 4. Diagrama de solicitações e concessão e revogação de permissões.

Uma vez que o paciente deve ser capaz de identificar quem acessa seus dados, o controle inicia com a exigência de identificação de cada participante por meio de uma identidade digital. A partir desta identificação é possível que cada participante registre solicitações ao sistema de acesso aos dados registrados do paciente. O paciente por sua vez irá registrar as concessões e revogações de solicitações de acesso aos dados.

Na Figura 3 apresentamos o diagrama que representa os passos de um acesso aos dados do paciente. Os passos incluem a identificação digital, a validação da identificação, a solicitação de acesso a um dados específico, a verificação de autorização de acesso e por fim o compartilhamento do dado caso haja autorização. No diagrama da Figura 4 apresentamos os passos para o registro de solicitação e concessão de acessos. As solicitações de acesso são inseridas por um médico, pesquisador ou uma instituição de saúde. A aplicação, por sua vez, realiza a mediação entre o registro da solicitação na Blockchain e o comunicado ao paciente. Por fim, o paciente registra a concessão ou revogação de

acesso aos dados em diferentes níveis de verificação. Isto quer dizer que a concessão é dada para cada parte dos seus registros.

4. Implementação

Baseado no conceito de proteção de dados implementado no Brasil pela Lei Geral de Proteção de Dados (LGPD) e também nas características dos registros eletrônicos de saúde (EHR), definimos uma estrutura que permite ao paciente ser o dono efetivo de suas informações e possa controlar o acesso por terceiros aos seus dados, assim como possa controlar quem poderá inserir informações ao seu respeito na rede. Para isso, utilizamos a tecnologia *blockchain Ethereum*. Nela, todas as transações são armazenadas de forma imutável. Além disso, é possível observar nessa rede todas as transações passadas e, assim, verificar a autorização para inserção ou visualização de dados, assim como verificar quem foi responsável por inserir cada dado sobre o paciente na rede. Isso garante a autenticidade e a origem da informação e também permite que o paciente tenha controle sobre todos os seus dados.

Assim, utilizamos a *blockchain Ethereum* para armazenar as informações a respeito do controle de acesso aos dados, enquanto os dados ficam armazenados de maneira criptografada em um banco de dados externo, uma vez que pode conter imagens, textos e vídeos a depender do exame que tenha sido realizado. Dessa forma, fica garantido que o crescimento da *blockchain* será limitado, uma vez que serão armazenados apenas as solicitações, autorizações e revogações de acesso, assim como a chave para descriptografar o dado presente no banco de dados externo.

4.1. Contratos Inteligentes

Para desenvolver a estrutura, utilizamos como base os contratos inteligentes. Esses contratos foram desenvolvidos em linguagem *Solidity*, linguagem de desenvolvimento de contratos para a rede *Ethereum*. Esses contratos são responsáveis por controlar todo o processo de permissão de acesso e inserção de dados. Fazendo uso deles, uma aplicação externa é responsável pela interface entre o paciente, o médico e a rede.

O contrato responsável pelo controle de acesso, nomeado ControleAcessoDados, possui as funções para solicitar ver informação (SV) e solicitar adicionar informação (SA), que são funções utilizadas pelos profissionais de saúde, e as funções autorizar ver informação (AV), revogar autorização para ver informação (RV), autorizar adicionar informações (AA) e revogar autorização para adicionar informações (RA), que são funções utilizadas pelo paciente. O contrato responsável por controlar os dados, por sua vez, nomeado ControleDados, possui as funções ver informação (VI) e adicionar informação (AI), além de funções especiais, denominadas modificadores, que controlam o acesso dos usuários a essas funções.

Cada função deverá ser executada por um usuário específico e, mesmo que um usuário qualquer da rede queira executar uma dessas funções, ele só conseguirá se possuir autorização. Assim, o médico fica responsável por solicitar a permissão ao paciente e também ver ou adicionar uma informação na rede. O paciente, por sua vez, fica responsável por conceder a autorização solicitada e também por revogá-la. Os contratos permitem que o paciente possa apenas conceder acesso a seus dados, assim como o médico só pode fazer solicitações em seu nome a pessoas específicas. Dessa forma, todo o processo de controle de acesso fica dentro da *blockchain*, sendo registrado de forma imutável.

As funções dos contratos desenvolvidos se relacionam ao processo de adicionar uma nova informação na rede. São elas as funções de solicitar permissão para adicionar, autorizar a inserção de uma nova informação, revogar a permissão para adicionar, verificar se há autorização, que é uma função interna, e adicionar informação. A invocação dessas funções deve ser feita de maneira ordenada, uma vez que o contrato irá barrar a inserção de uma informação caso não tenha sido concedida a permissão pelo paciente. Além disso, as funções implementadas com o objetivo de ver uma informação são similares às apresentadas e seguem um caminho idêntico ao apresentado para inserção de dados.

Para que uma informação seja adicionada na rede, primeiro deve ser chamada a função de solicitação, que emite um evento na rede indicando a solicitação. A partir desse momento, caso o paciente deseje autorizar a inserção de informações ele utilizará a função autorização, que inserirá o endereço do médico no *mapping* do cliente, permitindo então que esse médico adicione informações na rede. Esse mapping funciona como um vetor, armazenando o endereço do médico que poderá inserir dados relacionados àquele paciente. Além disso, será emitido um evento que indica essa autorização. O evento nada mais é que uma notificação no log da rede *Ethereum* que pode ser acessado pela aplicação e utilizado como informação para avisar aos envolvidos sobre o sucesso da ação.

A partir desse momento, enquanto possuir a permissão, o médico poderá inserir dados do paciente na rede por meio da função adicionar informação. Essa função fará uso da função verificar autorização para adicionar, que verifica se o endereço do médico está salvo no *mapping* daquele paciente e, caso esteja, retorna o valor indicando essa condição. Caso o médico esteja autorizado, a função para adicionar informação então inserirá a informação no *mapping* infos e armazenará seu endereço no *mapping* endereços. O médico poderá inserir quantos dados forem necessários enquanto possuir essa permissão.

A partir do momento que uma informação sobre um paciente é inserida na rede essa informação passa a ser do paciente. Nesse sentido, caso o médico necessite ver essa informação posteriormente ele terá que pedir a permissão para visualizar o dado ao cliente. Por fim, quando o paciente desejar revogar a autorização para determinado médico inserir informações ao seu respeito na rede, ele poderá utilizar a função revogação, que removerá o endereço do médico do *mapping* do paciente, efetivamente removendo sua permissão, e emitirá um evento indicando a remoção dessa permissão.

Quanto às funções responsáveis por controlar a visualização dos dados, o médico deve fazer requisições específicas a cada informação que ele queira ver a respeito do paciente. O paciente pode liberar o acesso individualmente a cada informação sua contida na rede, de forma a ter total controle sobre o que cada médico poderá ver a seu respeito.

4.2. Aplicações

Utilizando como base os contratos inteligentes desenvolvidos, inúmeras aplicações podem ser desenvolvidas com o objetivo de atender tanto ao cliente quanto ao médico. Essas aplicações podem ser páginas web que podem ser acessadas pela Internet por qualquer hospital ou clínica, assim como aplicativos mobile que permitam aos pacientes e médicos fazerem solicitações e acessar dados diretamente pelo *smartphone*.

De maneira geral, qualquer aplicação desenvolvida em cima do contrato proposto

deve seguir algumas regras de negócio para o seu correto funcionamento. O caminho a ser seguido pela aplicação é o seguinte. O médico faz a solicitação para acesso a determinado dado ou para inserção de uma informação. O paciente recebe essa solicitação e emite a autorização. O médico é notificado da autorização e pode solicitar para ver o dado ou inserir a informação desejada, de acordo com o que foi permitido. O paciente pode revogar a autorização concedida ao médico a qualquer momento. O médico deve fazer uma solicitação por vez. Caso ele deseje ver um dado e inserir outro, serão necessárias duas autorizações diferentes por parte do paciente. O médico poderá visualizar o dado ou inserir um dado a respeito daquele paciente enquanto possuir a permissão para isso. Por esse motivo o paciente pode revogar essa autorização a qualquer momento.

Dessa forma, os contratos desenvolvidos não se comprometem quanto à definição de quem é médico e quem é paciente, uma vez que o médico também pode ser paciente em outra circunstância. Assim, inicialmente, qualquer pessoa pode utilizar as funções destinadas aos médicos ou aos pacientes na rede, é a aplicação que ficará responsável em oferecer as funções corretas a cada um desses atores, limitando suas funcionalidades de acordo com seu login ou informações externas à blockchain.

5. Simulação, avaliação e resultados

O ambiente utilizado para a execução da arquitetura proposta foi criado a partir da configuração de um nó *Ethereum* privado, ou seja, foi criada uma nova instância da rede *Ethereum* sem conexão com a rede principal ou as redes de teste. Essa instância pode ser nomeada privada, pois não provê acesso público à sua implementação, sendo localizado em uma infraestrutura de rede local e apenas com o intuito da realização dos testes descritos a seguir. A utilização da rede pública Ethereum se justifica pelo fato dos testes realizados em uma rede não permissionada serem mais conclusivos do que uma rede permissionada que já faz um controle de quais participantes podem pertencer a rede. O ambiente de testes tem as seguinte configurações: Intel Core i5-3470U CPU 3.20GHz 4, 4 GB de memória RAM e sistema operacional Ubuntu 18.04.1 LTS 64 bits.

Os contratos inteligentes foram migrados para o nó da *blockchain* e a aplicação realizou a geração e inserção de usuários da rede representando pacientes, clínicas e médicos. Os dados dos pacientes, juntamente com as solicitações de acesso, visualização e inserção foram gerados de forma aleatória com a finalidade de serem computados e analisados. A aplicação desenvolvida para a execução dos testes ficou responsável por executar em ordem uma chamada de todas as funções previstas nos contratos de forma a observar sua correta execução. Conforme ilustrados pela Figura 2, existem vários tipos de solicitações de dados. Cada solicitação passa pela aprovação do paciente que controla todos os seus registros. Isto se faz necessário para centralizar o controle no paciente e abranger uma solução mais realista, conforme o que ocorre durante as etapas de uma aplicação centrada no paciente.

Para realizar a avaliação da solução proposta foram criadas três abordagens de execução dos experimentos. Em cada uma das abordagens foi utilizado um número diferente de *dApps* realizando solicitações simultaneamente, ou seja, em cada cenário a aplicação desenvolvida para testes foi executada paralelamente um número diferente de vezes. No **Experimento 1** foram utilizadas *dApps* realizando em média, 215 solicitações por minuto. No **Experimento 2** houve a utilização de *dApps* realizando, em média, 290

solicitações por minuto e por fim, no **Experimento 3** as *dApps* realizando, em média, 360 solicitações por minuto. A quantidade de solicitações foi obtida por meio da média da quantidade de transações realizadas durante toda a execução de cada experimento. Os dados capturados durante a execução dos experimentos foram o **Tempo da transação**, que é o tempo gasto para efetivar uma transação, o **Tamanho da fila**, que é o tamanho da fila de espera a cada inserção de transação e o **Tempo de espera por tipo** que é o tempo que cada tipo de solicitação presente na aplicação demora para ser efetivada na rede. Estes resultados serão apresentados na próxima subseção.

5.1. Resultados

A medição dos tempos tem o objetivo de demonstrar a viabilidade de utilização da blockchain para controle de permissões em registros médicos e não a performance comparativa de redes com tecnologia *blockchain*. Os resultados apresentados na Figura 5 representam o tempo de espera que uma transação levou para ser efetivamente gravada na *blockchain*. Os valores de média do tempo de espera para o experimento 1 é de 15,10 segundos e mediana é 11,13 segundos. Para o experimento 2, a média é de 24,47 segundos e a mediana de 17,63 segundos. No experimento 3 obtivemos a média de 31,05 e a mediana de 25,17 segundos. Os três cenários apresentam níveis crescentes em relação ao tempo de resposta uma vez que a demanda aumenta. Esses resultados nos mostram que o tempo de resposta apresentado é compatível com a necessidade de uma aplicação com finalidade de saúde em situações de não emergência. Em situação de emergência, os resultados obtidos de tempo de resposta poderiam se tornar um fator impactante se não houvessem o tratamento especializado para estes casos. Para essa finalidade houve a inserção de participantes especiais, denominados atores de Emergência, e com identificação certificada por uma SSI, que recebe o direito de realizar a visualização e atualização de dados de pacientes em uma ocorrência de emergência.

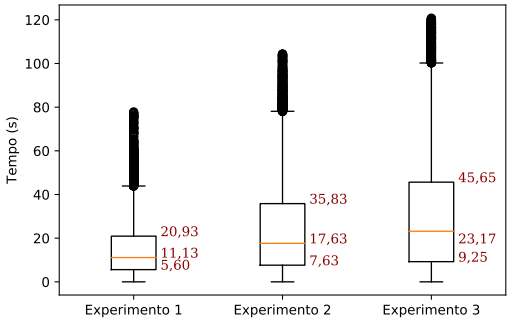


Figura 5. Tempo de espera.

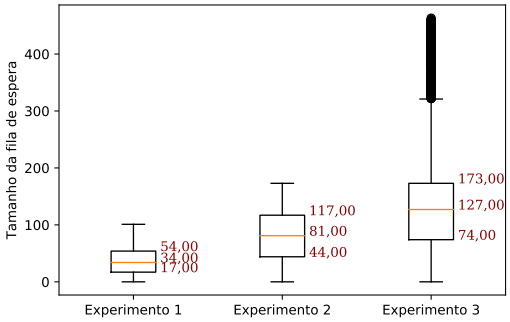
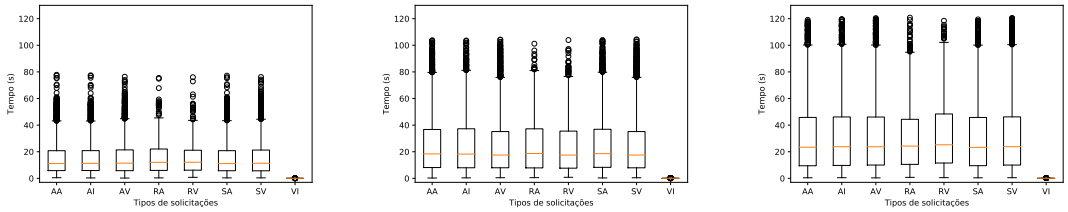


Figura 6. Tam. da fila de espera.

Na Figura 6 são apresentados, para os três experimentos, o tamanho da fila de espera, que é a fila que as transações enfrentam até que seja iniciado o seu processo de mineração. Os valores de média do tamanho da fila de espera para o experimento 1 é 37,11 e mediana 34. Para o experimento 2, a média é de 80,72 e mediana 81 e o experimento 3 obteve a média de 129,32 e mediana de 127. Os cenários apresentam filas de esperas que crescem de acordo com a demanda pelo recurso, o que afeta o desempenho em relação ao tempo da efetivação da transação.

Na Figura 7 são apresentados, para os três experimentos, o tempo de espera que uma solicitação de um tipo especifico gastou para ser concluída. Os tipos específicos de solicitações AA, AI, AV, RA, RV, SA, SV, conforme apresentados na Seção 4.1, obtiveram tempos médios aproximados. Os valores são 31,19; 31,59; 31,77; 31,42; 33,43; 31,24 e 31,76, respectivamente. O motivo desta proximidade de valores são devido a todas estas solicitações dependerem igualmente do consenso da rede e a efetivação da transação. As solicitações do tipo VI executam apenas consultas de autorizações e dados e obtiveram tempo de espera médio de 0,064 segundos. Estes valores de tempo de resposta são considerados baixos para este tipo de rede e foram alcançados por não dependerem do consenso da rede para as solicitações serem efetivadas. Nesse sentido, podemos observar que as solicitações do tipo VI, realizadas por uma unidade de emergência, serão prontamente atendidas e com tempo inferior a qualquer outro tipo de solicitação.



(a) Experimento 1 (b) Experimento 2 (c) Experimento 3

Figura 7. Tempo de espera por tipos de solicitações.

6. Considerações Finais

A *blockchain* é uma área de pesquisa de desenvolvimento recente, com grandes desafios a serem superados para que possa ser amplamente implementada e utilizada. As aplicações voltadas para o controle e compartilhamento de registros médicos são capazes de ofertar inúmeros benefícios para os usuários finais. Dentre as diversas questões de pesquisa relacionadas aos registros médicos está a segurança e privacidade dos dados, o qual está relacionado a este trabalho. Como contribuição para esta questão, apresentamos uma solução capaz de tratar concessão e revogação de acesso a registros eletrônicos de saúde baseada em *blockchain*. Os contratos inteligentes foram utilizados como solução para registrar as concessões e revogações de acesso em *blockchain*. A concessão e revogação de acessos foi elaborada de forma abrangente, resultando em uma estrutura capaz de oferecer suporte para qualquer aplicação desenvolvida para tal finalidade e que sigam as regras de negócio estabelecidas pelo contrato. A arquitetura consiste na integração de soluções definidas de maneira que o paciente possa ter o controle de acesso aos seus dados e atenda aos requisitos de aplicações centradas no paciente. Como trabalhos futuros pretendemos realizar testes na rede de teste Ropsten, dar continuidade no desenvolvimento da arquitetura para uma rede de consórcio e aprimorar a implementação em relação à possibilidade de interoperabilidade entre *blockchains* diferentes.

Referências

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. IEEE.

Gordon, W. J. and Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal*, 16:224 – 230.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7):1–7.

Hewa, T., Ylianttila, M., and Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 177:102857.

Hölbl, M., Kompara, M., Kamisalic, A., and Zlatolas, L. N. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, 10:470.

Huang, H., Sun, X., Xiao, F., Zhu, P., and Wang, W. (2021). Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. *Journal of Parallel and Distributed Computing*, 148:46–57.

Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., and Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare. *Journal of Medical Systems*, 43.

Kondova, G. and Erbguth, J. (2020). Self-sovereign identity on public blockchains and the gdpr. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 342–345.

Kshetri, N. (2018). 1 blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39:80–89.

Litvin, Korenev, S. V., Knyazeva, G., and Litvin, V. (2019). The possibilities of blockchain technology in medicine (Review). *Sovremennye Tehnologii v Medicine*, 11(4):191–199.

Nakamoto, S. and Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 4.

Rouhani, S. and Deters, R. (2017). Performance analysis of ethereum transactions in private blockchain. In *2017 8th IEEE(ICSESS)*, pages 70–74. IEEE.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., and Soursou, G. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography*, 3(1):3.

Wang, X., Feng, Q., and Chai, J. (2018). The research of consortium blockchain dynamic consensus based on data transaction evaluation. In *2018 11th International Symposium on Computational Intelligence and Design (ISCID)*, volume 2, pages 214–217. IEEE.

Zhang, P., Schmidt, D. C., White, J., and Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in computers*, volume 111, pages 1–41. Elsevier.

Zhuang, Y., Sheets, L. R., Chen, Y.-W., Shae, Z.-Y., Tsai, J. J., and Shyu, C.-R. (2020). A patient-centric health information exchange framework using blockchain technology. *IEEE journal of biomedical and health informatics*, 24(8):2169–2176.