Concessão de Permissão a Dados de Saúde Baseada em *Blockchain*

Natália R. Junqueira, Gabriel A. da Silva, Sergio T. de Carvalho

Instituto de Informática (INF) – Universidade Federal de Goiás (UFG)
Câmpus Samambaia – Goiânia – GO – Brasil

nattaliarj2016@gmail.com, gabriel.gbss@gmail.com, sergio@inf.ufg.br

Abstract. *Technological advances have led to the emergence of wearable devices that allow people to monitor their own health status. There has also been a growth in people's interest in controlling their own health, including tracking and analysis of personal health data. In this way, a patient can not only track this data, but effectively decide who may or may not have access to it. One of the pillars for this to be possible is privacy. This work focuses on data privacy to provide a greater degree of trust for digital health systems. The purpose of this paper is to develop a blockchain-based architectural solution for granting access permission to patient health data collected by a Remote Patient Monitoring System (SMRP), ensuring the privacy of this data.*

Resumo. *Com os avanços tecnológicos tem ocorrido o surgimento de dispositivos vestíveis que permitem às pessoas o monitoramento do seu próprio estado de saúde. Tem havido ainda um crescimento no interesse das pessoas pelo controle da própria saúde, incluindo o rastreamento e a análise dos dados pessoais de saúde. Desse modo, um paciente pode não só acompanhar esses dados, mas efetivamente decidir quem pode, ou não, ter acesso a eles. Um dos pilares para que isso seja possível é a privacidade. Esse trabalho tem como foco a privacidade dos dados, no sentido de proporcionar um maior grau de confiança aos sistemas de saúde digital. A proposta deste trabalho é desenvolver uma solução arquitetural baseada em blockchain para concessão de permissão de acesso aos dados de saúde do paciente coletados por um Sistema de Monitoramento Remoto de Pacientes (SMRP), garantindo a privacidade desses dados.*

1. Introdução

O uso de dispositivos vestíveis e sensores permite o acompanhamento do estado de saúde por meio de aplicativos que se comunicam com esses dispositivos [Fantoni 2016]. Nesse contexto, tem crescido o interesse das pessoas pelo controle, rastreamento, análise e compartilhamento de seus dados pessoais de saúde [Rettberg 2014, Ribeiro et al. 2017].

Para garantir a privacidade é essencial, no entanto, que o poder de decisão de quem acessa ou não os dados fique a cargo do próprio paciente [Fernández-Alemán et al. 2013, Reis et al. 2008, Røstad 2008, van der Linden et al. 2009, Daglish and Archer 2009, Lovis et al. 2007, Testa et al. 2011]. Além disso, é necessário que esse paciente tenha a garantia de que somente pessoas autorizadas por ele poderão obter acesso. A questão, portanto, é: como conceder acesso a esses dados sem comprometer a privacidade?

Uma tecnologia em potencial para realizar isso é a *blockchain*. Embora *blockchain* tenha surgido no contexto da realização de transações financeiras na Internet sem a necessidade de um terceiro de confiança, como, por exemplo, um banco, tem sido bastante investigado o seu uso para a área de saúde [Hoy 2017, Esposito et al. 2018].

Este é um trabalho que faz parte de um Projeto de Pesquisa "Aplicação de Técnicas de Computação Ubíqua, Arquitetura de Software e Inteligência Computacional no Contexto do Monitoramento de Pacientes Domiciliares" do Instituto de Informática - UFG, no qual já foram desenvolvidos diversos trabalhos, proporcionando assim um contexto para o qual este artigo está dando continuidade. O grupo tem trabalhado na área de Sistemas de Monitoramento Remoto de Pacientes (SMRP) que envolvem a coleta de dados de saúde por meio de sensores [Battisti and Carvalho 2016], um plano de cuidados ubíquo [Germano et al. 2016] que emite notificações para esse paciente conforme as prescrições e orientações, e uma rede social [Ribeiro et al. 2017] para gerenciar os relacionamentos entre as entidades desse SMRP. A rede social dissemina as notificações sobre o estado de saúde desse paciente para as pessoas com as quais esse paciente possui um relacionamento.

O objetivo desse artigo é apresentar uma solução arquitetural para a concessão de permissão de acesso a dados pessoais de saúde coletados por um SMRP, com base na tecnologia *blockchain*. Um paciente, no contexto desse trabalho, pode ser uma pessoa com alguma doença crônica ou que apenas tenha interesse em monitorar sua saúde de forma contínua.

O artigo está organizado em mais 3 seções. A Seção 2 traz a fundamentação teórica. A Seção 3 apresenta a proposta de solução arquitetural e uma prova de conceito desenvolvida utilizando contratos inteligentes em uma rede blockchain. A Seção 4 apresenta as considerações finais.

2. Fundamentação Teórica

Essa seção apresenta os conceitos de SMRP, de Redes Sociais, Princípios de Segurança da Informação, Tecnologia Blockchain em conjunto com Contratos Inteligentes. A união de todos esses conceitos forma a base para a abordagem de concessão de permissão proposta neste trabalho.

2.1. SMRP e Redes Sociais

Um SMRP é uma especialização de um sistema sensível ao contexto[Ribeiro et al. 2016], ou seja, um sistema capaz de prover serviços e informações baseados no contexto. De acordo com Dey e Abowd, contexto se refere a "qualquer informação que pode ser usada para caracterizar a situação de uma entidade. Uma entidade é uma pessoa, um local ou um objeto relevante para a interação entre o usuário e a aplicação, incluindo os próprios usuários e aplicações" [Abowd et al. 1999]. Um SMRP é aquele que utiliza dispositivos (sejam vestíveis, sensores, ou algo do tipo) para coletar dados remotamente, enviá-los para uma central de diagnósticos, onde após processados geram resultados (e.g., detecção de arritmia cardíaca[Doering et al. 2012], indicação de anomalias no índice glicêmico[Zhu 2011], detecção de queda[Karantonis et al. 2006]) .

Um modo de aperfeiçoar os sistemas de monitoramento remoto de pacientes é o envolvimento das pessoas em torno do indivíduo que necessita de cuidados. Essas pessoas, sejam elas cuidadores formais (profissionais de saúde) ou cuidadores informais (familiares e amigos), formam uma rede de cuidadores [Khorakhun and Bhatti 2015] ou comunidade de interesse [Ayubi and Parmanto 2012]. Espera-se que essa comunidade auxilie o paciente no que diz respeito ao seu tratamento como uma rede de amparo àquela pessoa. Além disso, estas comunidades possuem o potencial de conscientizar-se sobre condições de saúde.

Uma forma de permitir a manutenção dessa rede de cuidadores é a integração de serviços de redes sociais a sistemas de monitoramento remoto de pacientes [Ribeiro et al. 2016,

Ribeiro et al. 2017]. Os relacionamentos definidos no serviço de rede social podem ser usados para direcionar a rede de cuidadores e as notificações referentes ao estado de saúde de um paciente.

A abordagem proposta por [Ribeiro et al. 2017] é que os dados sejam compartilhados por meio de notificações em uma rede social específica de saúde, onde os relacionamentos entre os usuários dessa rede social são interpretados como informações contextuais. O relacionamento na rede social é, portanto, utilizado como uma forma de descrever uma interação entre os usuários.

O relacionamento entre um profissional de saúde e um paciente significa que o profissional possui interesse em receber dados daquele paciente, e, ao mesmo tempo, significa que o paciente concede àquele profissional de saúde o acesso aos seus dados. Essa solução, porém, tem o seu foco na proveniência de dados sem levar em consideração aspectos de segurança da informação, em especial a privacidade.

Privacidade é a propriedade das informações pertencerem a uma pessoa [ISO 2009]. Uma das formas de garantir a privacidade é permitindo ao dono da informação decidir como, quando e por quem seus dados serão manipulados.Além disso, deve ser fornecida ao dono detalhes sobre quais informações estão sendo coletadas e como esses dados estão sendo tratados e armazenados. Uma informação pode ser privada e não confidencial, mas quem decide a confidencialidade dessa informação é a pessoa a qual ela pertence.

2.2. Tecnologia *Blockchain*

Blockchain em português significa cadeia de blocos. O termo surgiu em 2008 quando um artigo foi transmitido para uma lista de e-mails divulgando uma criptomoeda denominada *Bitcoin*[Nakamoto 2008]. O *blockchain* do *Bitcoin* é um livro contábil (ledger) distribuído público do qual toda a rede *Bitcoin* depende. Este livro contábil é onde são registradas as transações, de forma ”timestampada”, o que significa que são registradas na ordem em que ocorreram, formando um histórico de todas as transações que resultaram no estado atual da rede *blockchain*. Outra característica de *blockchain* é que cada nó da rede possui uma cópia desse livro contábil distribuído, eliminando assim a possibilidade de um único ponto de falha[Nakamoto 2008, Greve et al. 2018].

A Figura 1 apresenta em um alto nível de abstração o funcionamento de um *blockchain*, desde a solicitação de uma transação até o seu término. No passo 1 alguém solicita uma transação; no passo 2, a transação é representada como um bloco; no passo 3, esse bloco é disseminado por todos os nós da rede; no passo 4, os nós que compõem a rede aprovam a transação; no passo 5, o novo bloco é adicionado na cadeia de blocos de forma permanente e imutável; e no passo 6, a transação está completa. Em um *blockchain* como o do *Bitcoin*, o fluxo de uma transação é um pouco diferente do apresentado pois requer mais passos, sendo portanto mais complexo. Nele, um bloco é um conjunto de transações criado através do processo de mineração executado por nós denominados mineradores que competem entre si através de um mecanismo de consenso para determinar quais nós terão suas transações publicadas no *blockchain*. Após a criação de um novo bloco, ele é disseminado para todos os nós da rede, os quais devem executar a verificação do bloco para validá-lo. Caso mais da metade da rede aprove o bloco como válido, o bloco é validado e adicionado à cadeia de blocos já existente[Allen].

O *blockchain* utiliza uma estrutura de dados similar a de uma lista encadeada para a construção da cadeia de blocos, com cada bloco contendo um hash do bloco anterior em seu cabeçalho, como apresentado na Figura 2, formando assim uma cadeia de blocos imutável que

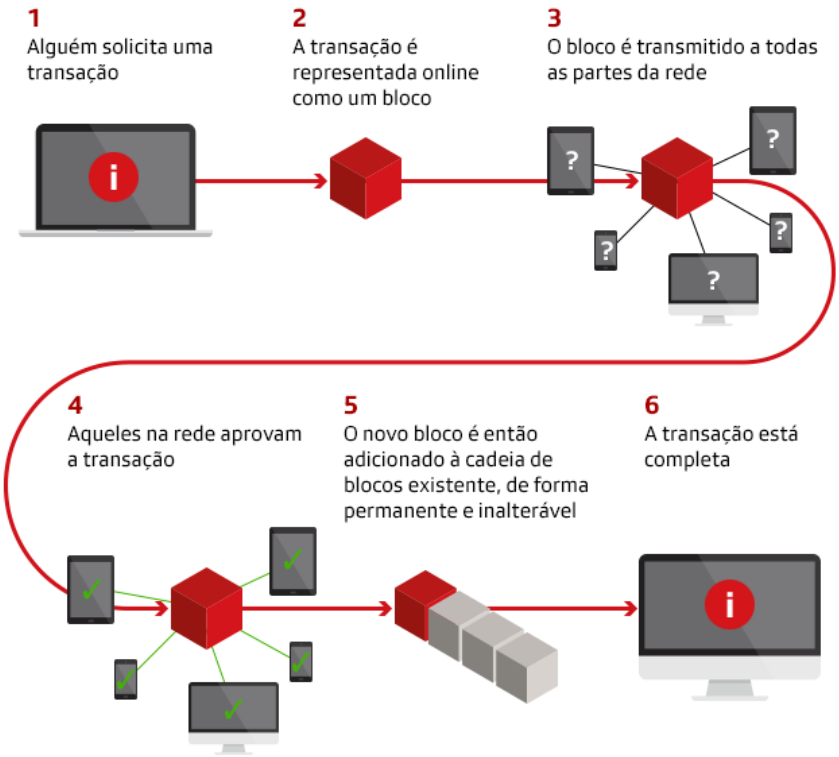

Figura 1. Funcionamento de um *blockchain* em alto nível de abstração [Allen]

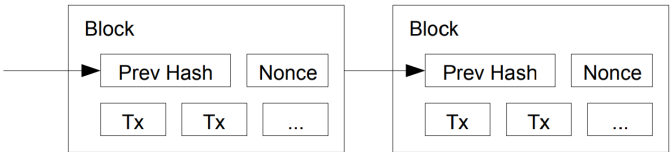

Figura 2. *Blockchain* - Adaptada de [Nakamoto 2008]

tem início no bloco gênesis (o primeiro bloco da cadeia) até o mais recentemente adicionado. Sempre que um novo bloco de transações é criado torna-se necessário atualizar todos os outros nós da rede com aquele novo bloco de transações. Esse processo é realizado através de um algoritmo de consenso que, no caso do *Bitcoin* é o algoritmo de prova de trabalho (PoW) [Nakamoto 2008, Greve et al. 2018].

O algoritmo PoW (Proof of Work), inicialmente proposto por Adam Back [Back et al. 2002], tem como ideia principal desmotivar ataques cibernéticos. Para atingir este objetivo, o usuário deve provar por meio de uma prova de trabalho que gastou um certo tempo para encontrar uma resposta que satisfaça a um requisito. A tarefa de encontrar a resposta é baseada em dois princípios: a prova de trabalho tem que ser difícil e trabalhosa, mas não impossível; e a verificação da prova de trabalho dessa prova deve ser rápida e fácil de ser realizada. Os nós responsáveis por realizar essa prova de trabalho, com o intuito de validar aquele conjunto de transações e provar que foi o primeiro a resolver esse problema computacionalmente difícil, são denominados mineradores (miners), os quais competem para realizar o trabalho de mineração de um novo bloco [Back et al. 2002].

O minerador que conseguir realizar o trabalho de mineração mais rápido ganha um prêmio, em geral, uma certa quantidade de criptomoeda como incentivo para continuar mine-

rando. O minerador é responsável também por informar aos outros nós que foi criado um novo bloco com determinado conjunto de transações válidas e adicionar o bloco à cadeia. O consenso ocorre nesse momento através da escolha da cadeia mais longa como sendo a verdadeira [Back et al. 2002].

Em um nível de abstração mais alto, a tecnologia *blockchain* utiliza mecanismos conhecidos da ciência da computação como listas encadeadas e redes distribuídas; reúne primitivas criptográficas como hashing, assinaturas digitais, chaves públicas/privadas; e combina conceitos financeiros tais como ledgers.

2.2.1. Contratos Inteligentes

A tecnologia *blockchain* também utiliza o conceito de contratos inteligentes, que são implementados na forma de *scripts* escritos em uma determinada linguagem de programação e armazenados na rede *blockchain*. As regras descritas no contrato inteligente funcionam de forma similar a uma lei, pois uma rede *blockchain* é praticamente imutável e os contratos armazenados nela herdam essa característica. Em outras palavras, o que for acordado em um contrato é exatamente o que será executado pela rede [Nakamoto 2008, Greve et al. 2018, Yaga et al. 2018].

Em [Yaga et al. 2018] um contrato inteligente é definido como uma coleção de código e de dados que é implantado em uma rede *blockchain*, por exemplo, *Ethereum*[1], *Hyperledger Fabric*[2], dentre outros. A cada transação enviada para o *blockchain*, dados podem ser enviados para os métodos públicos oferecidos pelo contrato inteligente. O contrato executa o método apropriado com os dados do usuário fornecidos para executar um serviço. O código, sendo implantado no *blockchain*, é imutável e, portanto, utilizado como um terceiro de confiança para transações, como por exemplo, uma transação financeira. Um contrato inteligente pode executar cálculos, armazenar informações e enviar automaticamente fundos para outras contas. Isso não significa necessariamente ter que executar uma função financeira. Os contratos inteligentes podem ser usados como uma forma de personalizar o funcionamento da rede *blockchain*. Esse artigo utiliza contratos inteligentes para identificar usuários, rastrear dados e conceder acesso.

2.3. Blockchains disponíveis para implementação de contratos inteligentes

Uma rede *blockchain* pode ser categorizada com base em seu modelo de permissão, que determina quem pode mantê-la (por exemplo, publicar blocos). Há duas categorias: sem permissão e com permissão. Uma rede blockchain sem permissão ou pública é aquela onde qualquer pessoa pode publicar um novo bloco (por exemplo, *Bitcoin*, *Ethereum*). A rede blockchain com permissão ou privada é onde apenas usuários específicos podem publicar blocos (como a *Hyperledger Fabric*). Em termos simples, uma rede *blockchain* com permissão é como uma intranet corporativa controlada, enquanto uma rede *blockchain* sem permissão é como a Internet pública, onde qualquer pessoa pode participar. Redes de *blockchain* com permissões são frequentemente implantadas para um grupo de organizações e indivíduos, tipicamente referido como um consórcio.

Ethereum foi a primeira plataforma blockchain para desenvolvimento de contratos inteligentes. Nela os contratos são escritos na linguagem de programação Solidity e implantados em um blockchain sem permissão. Ela usa como algoritmo de consenso a PoW em suas pri-

[1]https://www.ethereum.org

[2]https://hyperledger-fabric.readthedocs.io/en/release-1.4/

meiras versões, e tanto os contratos inteligentes como os dados armazenados são, por padrão, públicos, e, portanto, sem privacidade alguma [Wood 2014].

Hyperledger Fabric é também uma plataforma blockchain que permite o desenvolvimento de contratos inteligentes, que podem ser escritos nas linguagens de programação Go, Java ou Node JS, e são implantados em um blockchain com permissão modular. Um blockchain modular tem suas características representadas em módulos como, por exemplo, os mecanismos de consenso que no caso do *Hyperledger Fabric* podem ser acoplados a ele. Tanto os contratos como os dados armazenados são também públicos aos participantes da rede, porém causam um impacto menor quanto à privacidade por se tratar de um blockchain com permissão [Androulaki et al. 2018].

Uma plataforma blockchain que traz a solução para essa falta de privacidade nos contratos inteligentes é a *Enigma*[3]. A rede *blockchain* da *Enigma* permite realizar computação em dados criptografados sem a necessidade de descriptografar, tornando possível a criação de contratos secretos que com base nessa propriedade não violam a privacidade dos dados que armazenam. Esses contratos secretos são desenvolvidos na linguagem de programação RUST [Zyskind et al. 2015].

2.4. Trabalhos Relacionados

Essa Seção apresenta alguns trabalhos relacionados os quais também utilizam a tecnologia *blockchain* para um contexto parecido com o nosso.

Os autores do trabalho [Azaria et al. 2016] tem como objetivo apresentar um protótipo denominado MedRec que busca oferecer aos pacientes um registro abrangente, imutável e de fácil acesso a suas informações médicas em ”provedores”de tratamento (provedores são terceiros que armazenam informações médicas de diversos pacientes, por exemplo um Hospital). O MedRec gerencia a autenticação, a confidencialidade, a responsabilidade e o compartilhamento de dados. A implementação proposta por eles aborda três problemas relacionados a Registros Médicos Eletrônicos sendo eles a fragmentação dos dados, a falta de interoperabilidade e a falta de gerência do paciente sobre seus dados. Para isso eles reuniram referências a dados médicos diferentes e codificaram em um *blockchain*, de modo que estas referências fossem organizadas para formar um histórico para a história médica.

No *blockchain* do [Azaria et al. 2016] o conteúdo do bloco representa permissões de propriedade, visualização de dados compartilhados por membros de uma rede privada, referência para os dados em um banco de dados externo e um hash dos dados visando garantir a integridade dos mesmos . Ele foi implementado utilizando uma instância do *blockchain* da *Ethereum*, portanto, é um *blockchain* sem permissão onde todas as transações são públicas e todos que pertencem àquela rede podem participar. No *blockchain* do MedRec os contratos inteligentes são utilizados para monitorar mudanças de estado dos dados, como mudanças nos direitos de audiência ou nascimento de um novo registro. Além disso, os contratos inteligentes também são utilizados para estabelecer relacionamentos entre pacientes e os provedores que associam os registros médicos eletrônicos com bancos de dados externos.

Nesse artigo o intuito é armazenar um hash dos dados na cadeia de blocos; partindo do pressuposto que os dados são do paciente, sendo, portanto dados privados e cabe a ele decidir quanto ao seu grau de confidencialidade e a quem conceder acesso. Vamos utilizar os contratos também para monitorar o estado dos dados, o que o [Azaria et al. 2016] chama de direitos de

[3]https://enigma.co

audiência, onde permissões concedidas pelo paciente cria uma transação para atualizar o estado atualizando o hash dos dados para manter a integridade. Nossa proposta utiliza uma forma similar. Os dados que ele trata são também dados de saúde, mas estão mais voltados para dados produzidos em um ambiente hospitalar como prontuários eletrônicos e exames. Os dados que estão sendo trabalhos nesse artigo são de um ambiente domiciliar coletados por um SMRP.

Em [Xia et al. 2017], os autores projetam uma solução para o compartilhamento de dados entre provedores de serviços em nuvem, oferecendo controle de acesso a dados, procedência e auditoria. Eles consideram que não existe confiança entre os nós que participam do *blockchain*. A arquitetura da rede *blockchain* deles foi projetada como uma cadeia de blocos multi-chain que além da cadeia normal também possui blocos laterais que fazem parte de cada elemento individual da cadeia principal e utiliza triggers para intermediar a comunicação no sistema com bancos de dados externos onde ficam os dados. Os blocos desse *blockchain* armazenam diferentes instâncias de solicitações de acesso aos dados feitas por um determinado solicitante, onde na cadeia principal estão os solicitantes e na lateral as solicitações de cada. Já os contratos inteligentes foram utilizados com o intuito de garantir a obtenção de dados, a auditoria desses dados de forma confiável, além de serem responsáveis por monitorar de perto todas as ações realizadas nos dados, relatar todas as ações realizadas por um solicitante em dados de um proprietário e caso haja alguma violação de permissão o acesso aos dados também é revogado por um contrato inteligente.

Algo comum entre a solução que está sendo proposta nesse artigo e as apresentadas no MedRec e no MedShare é a aplicação de contratos inteligentes para monitorar os dados e todas as ações que alteram seu estado. Além disso, há um interesse em controlar quem pode ter acesso aos dados de saúde. Mas o diferencial da solução deste trabalho é em se tratar de um ambiente domiciliar e o paciente ter o poder de conceder, ou não, acesso aos seus dados diretamente para outra pessoa usando relacionamentos em uma rede social como forma de conceder permissão de acesso a seus dados.

3. Proposta de Solução Arquitetural

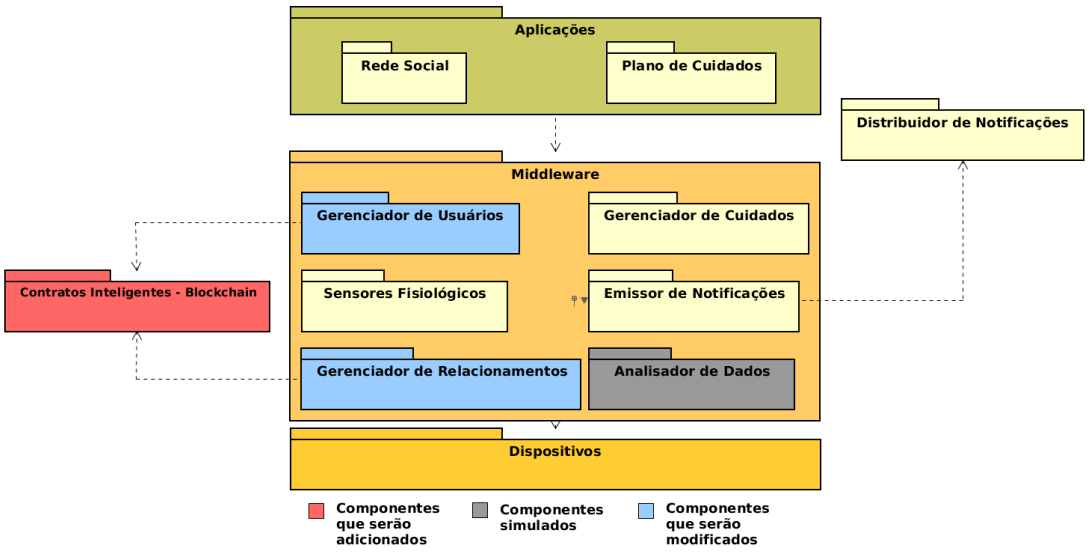

Figura 3. Solução Arquitetural de Concessão de Permissão de Acesso baseada em *Blockchain*.

Essa seção apresenta a proposta deste trabalho que consiste em desenvolver uma solução arquitetural que utilize a tecnologia *blockchain* em conjunto com os contratos inteligentes para garantir a privacidade dos dados de saúde de um paciente coletados por um SMRP. Nesse contexto, os pacientes manifestam o desejo de conceder acesso aos seus dados, e os demais manifestam o interesse de receber os dados desse paciente, por meio de relacionamentos em uma rede social específica. Isso possibilita aos pacientes ter um maior controle dos seus dados de saúde, dando a eles a escolha de a quem conceder acesso a esses dados.

A Figura 3 apresenta a proposta de solução arquitetural de concessão de permissão a dados de saúde baseada em *blockchain*. Os módulos de Gerência de Usuários e de Gerência de Relacionamentos possuem em sua estruturação contratos inteligentes construídos com o objetivo de preservar a privacidade do paciente que está sendo monitorado, e conceder permissão de acesso a seus dados de saúde a quem ele desejar com a confiança de que apenas quem ele autorizar terá o acesso.

O componente Contratos Inteligentes - *Blockchain* está abstraindo todo o conjunto de contratos necessários para realizar as funções de armazenamento dos dados, relacionamento entre as entidades, perfis de usuários, níveis de acesso de cada perfil, restrições determinadas pelo próprio paciente sobre os seus dados, entre outros. Um contrato determina um paciente e os seus respectivos dados monitorados. As atualizações são feitas por meio de chamadas aos métodos *set* definidos no contrato inteligente, os quais criam uma transação para armazenar as informações vindas dos sensores e do analisador de dados, atualizando o estado atual do *blockchain*. Por se tratar de um *blockchain*, as informações anteriores não são apagadas, sendo possível, portanto, manter um histórico completo dos dados nele armazenados.

3.1. Concessão de permissão de acesso através de Contratos Inteligentes

Para realizar a concessão de permissão de acesso é necessário responder às seguintes questões: Quem é o dono dos dados? Quais são esses dados? Para quem o acesso será concedido? Quais são as restrições para esse acesso? Essas questões são respondidas nessa solução por meio de três tipos de contratos inteligentes: o contrato de identificação, o contrato de rastreamento dos dados e o contrato de concessão de permissão de acesso aos dados.

O contrato de identificação de usuário identifica o paciente, familiar, profissional de saúde ou responsável legal. A política de controle de acesso é implementada com base nesses papéis que os usuários podem assumir no sistema. Para cada papel um conjunto de informações é requisitado para criar e validar a identidade do usuário no sistema. Esse contrato é invocado pela rede social para realizar o cadastro de novos usuários no blockchain, por meio de uma chamada ao método do contrato de identificação responsável por criar novas identidades na rede.

Usuários com o papel de paciente devem fornecer informações pessoais, como, por exemplo, nome, RG, CPF. Aqueles usuários com o papel de familiar fazem seu cadastro de dados pessoais e informações sobre a qual paciente está vinculado, comprovando esse vínculo com o anexo de um documento comprobatório no sistema. Essa relação de vínculo não permite a esse familiar o acesso aos dados de um paciente. Para efetivar esse acesso, é necessário que haja um contrato de concessão permissão de acesso aos dados entre o paciente e o familiar. O usuário com o papel de profissional de saúde, além de realizar o cadastro dos seus dados pessoais, também deve inserir seus dados de registros profissionais, como, por exemplo, a identificação junto ao respectivo conselho profissional. Por fim, outro papel possível para usuários é o de responsável legal, para os casos em que o paciente seja incapaz.

O contrato de rastreamento dos dados está vinculado a um usuário com o papel de paciente. Esse contrato mantém uma referência ao banco de dados do SMRP em conjunto com o seu hash. Além disso, todas as operações de leitura e escrita relacionadas aos dados do paciente são chamadas pelos métodos deste contrato deixando assim um histórico completo e auditável sobre a manipulação desses dados, para só então transmitir essas requisições ao banco para serem executadas. Antes que as chamadas aos métodos desse contrato sejam processadas, consultas são realizadas para verificar se há um contrato de concessão de permissão entre o paciente dono dos dados e o interessado. O contrato de rastreamento dos dados é invocado pela rede social durante o cadastro de um usuário com o papel paciente para armazenar os dados relacionados a ele, mas também é invocado sempre que um usuário desejar o acesso aos dados de um paciente ou quando for necessária a atualização dos dados vindos do SMRP (e.g., dados de saúde coletados por sensores).

O contrato de concessão de permissão de acesso aos dados está vinculado a um paciente e a um contrato de rastreamento dos dados. Nele, o paciente registra para qual usuário ele está concedendo permissões de acesso a seus dados, especificando as restrições que desejar, tanto em relação ao nível de permissão de acesso quanto a quais dados específicos. A rede social invoca esse contrato sempre que um novo relacionamento é criado entre os usuários, e realiza consultas para verificar se existe um contrato concedendo permissão antes de fornecer o acesso aos dados de um outro usuário.

A rede social deixa transparente para os seus usuários a utilização da tecnologia blockchain e a invocação dos contratos para o seu funcionamento. Os contratos são utilizados no sentido de garantir que as políticas de acesso e de funcionamento da rede sejam executadas da mesma forma que foram programadas. Contratos inteligentes e a tecnologia blockchain ficam no *back-end* da rede social auxiliando no seu funcionamento, no sentido de garantir a privacidade dos dados.

3.2. Prova de Conceito

A prova de conceito desse trabalho está sendo realizada por meio da implementação de contratos inteligentes implantados na plataforma Hyperledger. A implementação armazena um hash e a referência dos dados produzidos por um SMRP.

A Figura 4 apresenta o diagrama de atividades da UML de identificação de um paciente na rede social. É realizada uma verificação para identificar se aquele paciente já está cadastrado, e, na sequência, se o paciente não é incapaz e então, é invocado o Contrato de Identificação de Usuário para criar a nova identidade na rede. A rede social solicita os dados de acesso ao SMRP para o paciente, que os cadastra, para, por fim, a Rede Social invocar o contrato de Rastreamento dos dados para cadastrar essas informações.

A Figura 5 apresenta o diagrama de atividades da UML de concessão de permissão de acesso aos dados: paciente tem que selecionar para quem ele deseja conceder permissão de acesso, fazendo com que esse usuário participe da rede de interessados no paciente; paciente especifica as restrições para concessão desse acesso; interessado recebe uma notificação para ele aceitar ou não estabelecer esse relacionamento na rede social; rede social invoca o contrato de concessão de permissão para criar essa nova permissão de acesso na rede blockchain.

A Figura 6 apresenta o diagrama de atividades da UML de acesso aos dados de um paciente: o usuário solicita acesso e a rede social realiza uma chamada ao contrato de Rastreamento dos Dados para obter acesso; o contrato realiza uma consulta para verificar se existe alguma instância do contrato de Concessão de permissão concedendo acesso para esse usuário;

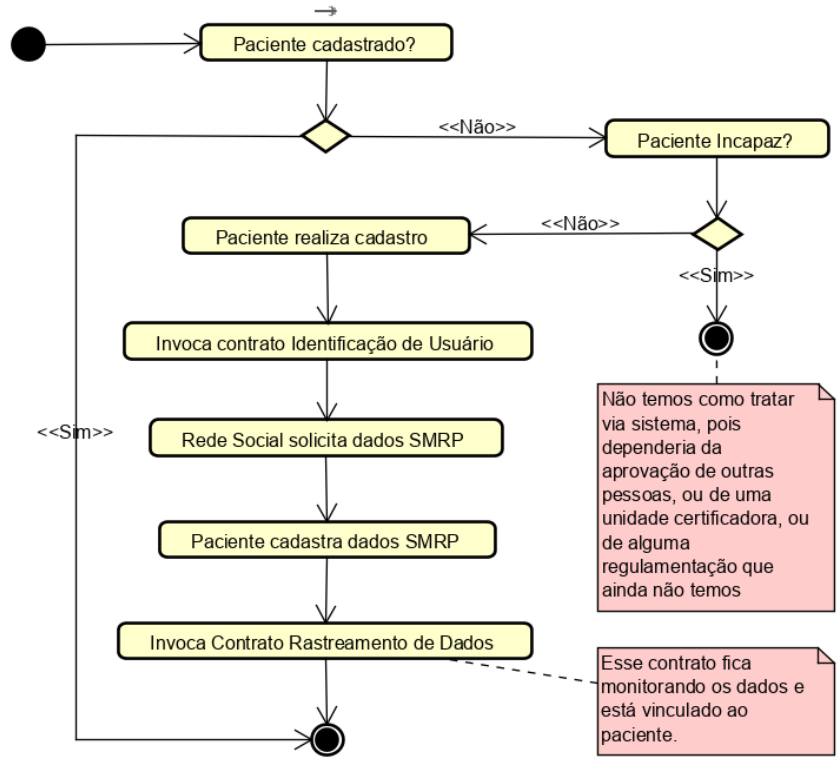

Figura 4. Diagrama de Atividades da UML - Identifica Paciente

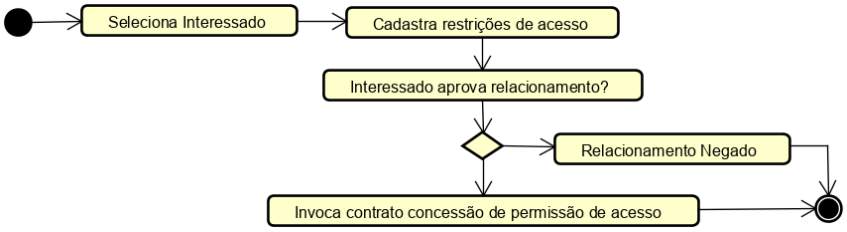

Figura 5. Diagrama de Atividades - Concede Permissão

caso exista, fornece os dados e registra o acesso no blockchain para manter um histórico de manipulação dos dados de um paciente.

Estes contratos estão sendo desenvolvidos para a plataforma *Hyperledger Fabric* sendo escritos na linguagem de programação Go, e para a plataforma *Enigma* usando a linguagem de programação Rust. Essas plataformas foram escolhidas por serem da categoria com permissão e permitirem o desenvolvimento de contratos em linguagens de programação de propósito geral.

A plataforma *Hyperledger Fabric*, por não garantir a privacidade dos seus contratos inteligentes e dados armazenados neles, necessita de um maior cuidado com a implementação, pois dados confidenciais necessitam ser criptografados antes de serem armazenados nesses contratos para evitar que pessoas sem autorização tenham acesso. A plataforma *Enigma*, por possuir contratos secretos, por padrão já garante a confidencialidade de seus contratos e dos dados contidos neles.

4. Considerações Finais

Esse artigo apresenta uma solução arquitetural de concessão de permissão de acesso a dados de saúde baseada em blockchain, onde os relacionamentos entre os usuários de uma rede social

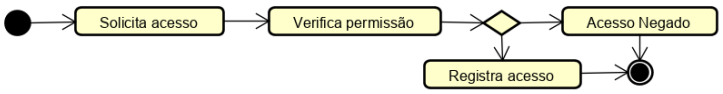

Figura 6. Diagrama de Atividades - Acessa Dados Paciente

específica de saúde são mapeados em contratos inteligentes com o intuito de conceder permissão de acesso aos dados de saúde de um paciente, garantindo a privacidade desses dados, os quais são coletados através de um SMRP que utiliza essa rede social para disseminar os resultados obtidos por ele.

A solução arquitetural proposta precisa ser avaliada por meio de uma análise de desempenho, visando medir o quanto a aplicação da tecnologia *blockchain* e dos contratos inteligentes pode impactar no desempenho do SMRP. Além disso, é necessária uma avaliação relacionada ao seu grau de privacidade que essa arquitetura efetivamente garante.

Referências

(2009). *ISO 27000, "Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary"*. ISO.

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., and Steggles, P. (1999). Towards a better understanding of context and context-awareness. In *1st Int. Symp. on Handheld and Ubiq. Comp.*, pages 304–307, London, UK, UK. Springer-Verlag.

Allen, M. Como o blockchain pode afetar em breve a vida cotidiana. `https://bit.ly/2r4a6XN`. Acessado: 25/11/2018.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *13th EuroSys Conf.*, page 30. ACM.

Ayubi, S. U. and Parmanto, B. (2012). Persona: Persuasive social network for physical activity. In *2012 Int. Conf. IEEE Engineering in Medicine and Biology Society*, pages 2153–2157.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *2nd OBD*, pages 25–30. IEEE.

Back, A. et al. (2002). Hashcash-a denial of service counter-measure. `ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf`.

Battisti, D. and Carvalho, S. (2016). Aplicação do padrão ISO/IEEE 11073 no contexto da assistência domiciliar à saúde. pages 79–90. In: Anais da IV Escola Regional de Informática (ERIGO), 2016.

Daglish, D. and Archer, N. (2009). Electronic personal health record systems: a brief review of privacy, security, and architectural issues. In *Privacy, Security, Trust and the Management of e-Business*, pages 110–120. IEEE.

Doering, L. V., Hickey, K., Pickham, D., Chen, B., and Drew, B. J. (2012). Remote noninvasive allograft rejection monitoring for heart transplant recipients: study protocol for the novel evaluation with home electrocardiogram and remote transmission (new heart) study. *BMC cardiovascular disorders*, 12(1):14.

Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, 5(1):31–37.

Fantoni, A. (2016). Dispositivos wearable para o campo da saúde: reflexões acerca do monitoramento de dados do corpo humano. *Temática*, 12(01).

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *J. Biomedical informatics*, 46(3):541–562.

Germano, E., Battisti, D., Ribeiro, H., and Carvalho, S. (2016). Plano de cuidados ubíquo para acompanhamento domiciliar de pacientes. CBIS, p. 849-858.

Greve, F., Sampaio, L., Abijaude, J., Coutinho, A., Valcy, Í., and Queiroz, S. (2018). Blockchain e a revolução do consenso sob demanda. In: Minicursos do XXXVI SBRC.

Hoy, M. B. (2017). An Introduction to the Blockchain and Its Implications for Libraries and Medicine. *Medical Reference Services Quarterly*, 36(3):273–279.

Karantonis, D. M., Narayanan, M. R., Mathie, M., Lovell, N. H., and Celler, B. G. (2006). Implementation of a real-time human movement classifier using a triaxial accelerometer for ambulatory monitoring. *IEEE transactions on inf. tech. in biomedicine*, 10(1):156–167.

Khorakhun, C. and Bhatti, S. N. (2015). mhealth through quantified-self: a user study. In *2015 17th Int. Conf. on E-health Networking, Application & Services*, pages 329–335. IEEE.

Lovis, C., Spahni, S., Cassoni, N., and Geissbuhler, A. (2007). Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks. *Int. J.Medical Informatics*, 76(5-6):466–470.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *In: www.bitcoin.org/bitcoin.pdf. Acesso em 05/02/2019*.

Reis, F. F., Costa-Pereira, A., and Correia, M. E. (2008). Access and privacy rights using web security standards to increase patient empowerment. *Health tech. inf.*, 137:275–285.

Rettberg, J. W. (2014). *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves*. Palgrave Macmillan, Springer.

Ribeiro, H., Battisti, D., Germano, E., and Carvalho, S. (2016). Notificações de monitoramento remoto de pacientes usando redes sociais. CBIS,p. 859-868.

Ribeiro, H. A., Germano, E., Carvalho, S. T., and Albuquerque, E. S. (2017). Integrating social networks and remote patient monitoring systems to disseminate notifications. In *MEDINFO 2017*, volume 245, page 198. IOS Press.

Røstad, L. (2008). An initial model and a discussion of access control in patient controlled health records. In *Availability, Reliability and Security*, pages 935–942. IEEE.

Testa, M. G., de Azevedo Bragança, C. E. B., and Luciano, E. M. (2011). Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. *Revista Reuna*, 16(2):89–102.

van der Linden, H., Kalra, D., Hasman, A., and Talmon, J. (2009). Inter-organizational future proof ehr systems: a review of the security and privacy related issues. *Int. J. medical informatics*, 78(3):141–160.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., and Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access*, 5:14757–14767.

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018). Blockchain technology overview. *National Institute of Standards and Technology Internal Report – NISTIR*, 8202.

Zhu, Y. (2011). Automatic detection of anomalies in blood glucose using a machine learning approach. *Journal of Communications and Networks*, 13(2):125–131.

Zyskind, G., Nathan, O., and Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*.