Registros Médicos Eletrônicos com Banco de dados Blockchain

Tiago Leoratto[1], **Marcelo de Paiva Guimarães**[1,2]

[1]Programa de Mestrado em Ciências da Computação
Centro Universitário Campo Limpo Paulista (UNIFACCAMP)
R. Guatemala 167 – 13.231-230 – Campo Limpo Paulista – SP – Brasil

[2]Universidade Federal de São Paulo (Unifesp/Reitoria-UAB)
Rua Sena Madureira, 15 - São Paulo - SP - Brasil

Abstract. *Blockchain-based applications are characterized by the decentralization of processing and management, and the possibility of the user being the manager of their data. Therefore, the use of this technology has aroused interest in the health area, especially for the development of electronic medical records. This work aims to present a model for electronic records based on blockchain integrated with a document-oriented database (noSQL). The model aims to give patients the management of their own medical records and access, as long as I allowed it, by any service provider.*

Resumo. *Aplicações baseadas em blockchain possuem como características a descentralização do processamento e do gerenciamento, e a possibilidade do usuário ser o próprio gestor dos seus dados. Por isso, o uso desta tecnologia tem despertado o interesse na área da saúde, em especial, para o desenvolvimento de prontuários eletrônicos. Este trabalho tem como objetivo apresentar um modelo para prontuários eletrônicos baseados em blockchain integrado com um banco de dados orientado a documentos (noSQL). O modelo visa atribuir aos pacientes a gestão dos seus próprios prontuários e o acesso, desde que permitido, por qualquer prestador de serviço.*

1. Introdução

Os prontuários médicos inicialmente eram registrados em papel e ficavam disponíveis somente para um profissional ao mesmo tempo, possuíam baixa mobilidade e estavam sujeitos a ilegibilidade, ambiguidade, possíveis perdas de informação, falta de padronização e dificuldades de pesquisas coletivas. Para guardar exigiam grandes espaços para arquivamento, pois os atendimentos podem gerar quantidades expressivas de informações sobre o paciente [CFM and SBIS 2012] . Com o intuito de minimizar as limitações dos registros médicos em papel, os computadores foram incorporados nas rotinas das instituições médicas. Desde então, inúmeras instituições têm desenvolvido diferentes modelos de registros médicos eletrônicos [Hyppönen et al. 2013].

Apesar do uso da tecnologia auxiliar em diversos pontos a geração e armazenamento dos prontuários médicos, os mesmos geralmente ficam em posse somente dos profissionais que os criam. Com o objetivo de possibilitar que os prontuários estejam disponíveis para mais de um profissional e que as informações sejam de propriedade do paciente, as características da blockchain vêm despertando interesse na área da saúde.

Como a blockchain é uma solução distribuída e que permite que o próprio usuário seja o gestor de seus dados, então é uma abordagem promissora como base para os prontuários eletrônicos. Além disso, agrega a garantia de privacidade e a possibilidade dos pesquisadores se beneficiarem da disponibilidade de um amplo conjunto de dados médicos [Karafiloski and Mishev 2017].

Este trabalho tem como objetivo mostrar um modelo de prontuários eletrônicos baseados em blockchain, que terá com caraterísticas a descentralização da informação, privacidade, controle dos ativos[1] pelo proprietário e armazenar as informações em um banco de dados orientado a documento e escalável. O modelo apresentado neste projeto utiliza a solução BigchainDB em uma rede privada, onde os participantes são conhecidos. Existem alguns prontuários na literatura que também usam blockchain, contudo elas são baseadas em criptomoedas e banco de dados relacionais, como por exemplo, Medrec [Ekblaw et al. 2016], Ancile [Dagher et al. 2018], UniRec [Quaini et al.], Zhealth [zhe], MediChain [Rouhani et al. 2018] e Medblocks [Ramesh].

O restante desse trabalho esta divido da seguinte forma: a seção 2 apresenta a fundamentação, a seção 3 expõe o projeto e por fim, a seção 4 relata as conclusões.

2. Fundamentos

Os primeiros estudos que originaram o conceito blockchain ocorreram no início da década de 90. Foi inspirado no algoritmo de ordenação de data e hora, e usado para impedir a violação de documentos. A definição original foi criada em 2008 com a publicação do artigo ”Bitcoin: A Peer-to-Peer Electronic Cash System”publicado por Satoshi Nakamoto[Nakamoto 2008].

Blockchain consiste em uma cadeia ordenada e consistente de blocos. Os blocos têm informações para controle e as informações propriamente ditas do contexto que a blockchain esta inserida. A Figura 1 demonstra a estrutura de blocos encadeados. Nela é possível verificar que cada bloco (B) tem um apontador H(B) para o bloco anterior. Outra característica é a de que a estrutura de blocos é replicada em uma rede peer-to-peer. Dessa forma, a informação é descentralizada evitando que uma entidade central ou absoluta tenha o poder sobre ela. Quando um novo bloco tem sua criação submetida, ele é enviado para todos os participantes[2] da blockchain. Os participantes, através de mecanismos de consenso, determinam quando um bloco é válido e o acrescentam na blockchain.

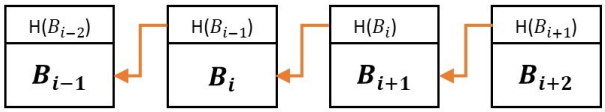

Figura 1. Cadeia de blocos na blockchain

A blockchain também garante a privacidade das transações que são realizadas de forma anônima, evitando que terceiros conheçam exatamente as pessoas envolvidas na

[1]Um ativo pode representar qualquer objeto físico ou digital. O ativo no contexto deste trabalho representa os prontuários médicos e as regras de acesso para os mesmos. Cada ativo é associado a proprietários, que são responsáveis pela sua criação.

[2]Em uma blockchain pública todos participantes têm o mesmo direito de verificação. Já em uma blockchain privada, um grupo pré-definido de participantes controlam o processo de verificação.

transação. Também na blockchain ocorre o controle de propriedade dos ativos, a qual somente o proprietário, ou proprietários, possuem um conjunto específico de chaves privadas que validam a propriedade de um ativo específico.

2.1. BigchainDB

O BigchainDB[3] foi anunciado em 2016 e é chamado de banco de dados blockchain, por possuir propriedades de um banco de dados tradicional e ter características de uma blockchain. A estrutura fundamental do BigchainDB é o *node*. Ele é formado pelo MongoDB[4], Tendermint[5].

O MongoDB é o banco de dados de código aberto que opera utilizando a linguagem de consulta NoSQL. Ele é o responsável pelo armazenamento dos dados oriundos do BigchainDB e fornece as características de banco de dados ao ambiente. O ponto positivo do MongoDB é sua flexibilidade. Sua estrutura orientada a documentos permite gravar os dados da forma que for melhor para a aplicação [MongoDB 2017].

Tendermint é um protocolo composto por duas partes, algortimo de consenso e protocolo de rede ponto a ponto. O Tendermint funciona mesmo que até 1/3 das máquinas falhem de maneira arbitrária. A adição de um bloco novo na cadeia ocorre através de rodadas (*rounds*) no Tendermint. Em cada rodada o bloco pode ter alguns estados possíveis que também são chamados de passo (*step*). Um bloco a ser validado esta em uma determinada altura, rodada e passo. Um bloco é dito efetivado pelo Tendermint quando assinado e difundido por mais de 2/3 do poder de votação dos validadores [Kwon 2014]. É o Tendermint que adiciona as características de uma blockchain ao sistema BigchainDB.

A Figura 2 ilustra um exemplo de registro de consulta de um paciente. Um usuário da blockchain, através de uma aplicação desenvolvida, por exemplo, na linguagem Python[6], submete uma transação ao BigchainDB (1). O BigchainDB fornece os métodos de criptografia necessária e também faz algumas validações iniciais para as transações. A transação contendo o registro da consulta é enviada para o Tendermint realizar o processo de consenso. Como parte desse consenso, são empacotadas as transações submetidas em um bloco e esse bloco sofre uma votação para avaliar sua validade (2). Quando é alcançado um consenso, é enviada uma confirmação do bloco criado (3). Com o bloco criado, é enviado ao banco de dados MongoDB (4), em seguida o banco de dados envia a confirmação do bloco armazenado (5). Logo após é enviado para a aplicação a confirmação de todo o processo ao usuário (6).

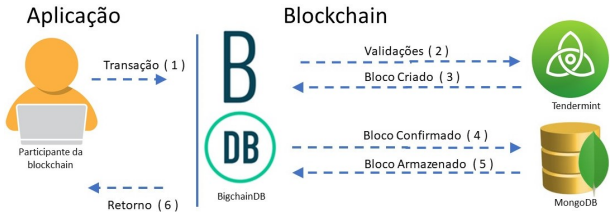

Figura 2. Fluxo de transação BigchainDB.

[3]https://www.bigchaindb.com/
[4]https://www.mongodb.com/
[5]https://tendermint.com/
[6]https://github.com/bigchaindb/bigchaindb-driver

O BigchainDB utiliza o conceito de ativo para qualquer transação e esse será armazenado no banco de dados. Os ativos podem ser qualquer tipo de informação, como por exemplo uma anotação de um atendimento médico a um paciente. Esses ativos são criados através da transação *create* e também associa o proprietário. O proprietário do ativo é identificado por uma chave pública criptografada e é inserido no ativo criado. Além da chave pública, uma chave privada também é assinada no ativo. Assim, se o par de chaves não pertencer ao mesmo usuário, o ativo não será criado. Quando o ativo é criado um identificador é gerado. Com o identificador único, posteriormente o ativo será referenciado para consultas e até mesmo transferidos para outros usuários. A transferência do ativo ocorre através da transação *transfer*, onde é necessário informar a chave privada do proprietário aprovando a transferência.

3. Projeto

Neste projeto tudo será tratado como ativo, assim serão criados alguns tipos de ativos com características distintas. A Figura 3 mostra a abordagem proposta com os ativos que poderão ser criados e como são relacionados entre si. O ativo do tipo paciente terá uma chave pública e o seu identificador único. No ativo de dados do paciente estarão suas informações pessoais, como peso, altura e tipo sanguíneo. Já no ativo de responsáveis será informado os responsáveis do paciente, por exemplo, parentes ou cuidadores. Esses ativos terão a informação do identificador do paciente. Para que a criação desses ativos ocorra deverão ser assinados pela chave privada do paciente.

As instituições de saúde e de pesquisa são criadas no ativo de instituição, que também terão suas chaves públicas. O ativo do tipo *admin* será utilizado para casos de visualização de emergência, com sua respectiva chave pública. O registro médico será criado no ativo prontuário. Na criação do ativo prontuário é assinado com a chave privada do paciente que está criando este ativo. Por fim, o ativo do tipo acesso, esse terá o identificador do prontuário e as chaves públicas dos responsáveis, instituição, *admin* e do paciente.

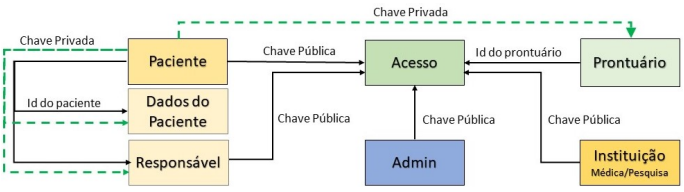

Figura 3. Abordagem proposta

Quando o paciente efetuar seu cadastro no mínimo um ativo é criado, ativo do tipo paciente. O identificador do ativo paciente é utilizado para inserir nos demais ativos que o paciente criar. Um paciente pode ter mais de um ativo de dados e responsáveis em sua história. Sendo assim, para esses ativos sempre são utilizado os mais atuais armazenados na blockchain. Por exemplo, um paciente pode ter seus dados como peso e altura alterados ao longo da vida, sendo necessário ”alterar”essas informações no seu ativo de dados do paciente. O mesmo pode ocorrer para o ativo de responsáveis.

O ativo de prontuário seguirá a abordagem utilizada para a confecção de um registro médico orientado ao problema. Nessa abordagem os prontuários médicos são armazenados na estrutura SOAP [da Costa 2001]. A Figura 4 mostra o prontuário na estrutura

SOAP em um documento que é armazenado no banco de dados MongoDB. Além da estrutura é informado um cabeçalho ao documento para que seja utilizado em buscas efetuadas no banco de dados. No item *Subjective* é informado os sintomas do paciente. O *Objective* serve para o especialista inserir os sinais observados. O *Assessment* é o item de concretização dos diagnósticos efetuados. Já *Plan* é feito a proposta de tratamento ao cliente.

```
Cabecalho : COVID-19,
Prontuario : {
        Subjective   : sintomas do paciente,
        Objective    : sinais observados pelo médico,
        Assessment : resultado de exames e conclusoes, diagnostico,
        Plan         : conduta, um tratamento por exemplo
}
```

Figura 4. Prontuário estruturado

A Figura 5 ilustra a visão geral proposta para contemplar a solução de prontuário médico. O paciente (1) armazenado no BigchainDB cria o prontuário (2). O prontuário é criptografado com uma chave simétrica e armazenado no banco de dados (3). Após a chave utilizada é criptografada de forma assimétrica utilizando as chaves públicas de todos os proprietários do prontuário, criando o ativo de acesso (4). Caso seja solicitado visualização (5) por uma nova instituição já armazenada no BigchainDB (6), é necessário criar um novo ativo do tipo acesso (7). No novo ativo de acesso será adicionado chave pública do solicitante juntamente com a chave assimétrica para decifrar o prontuário.

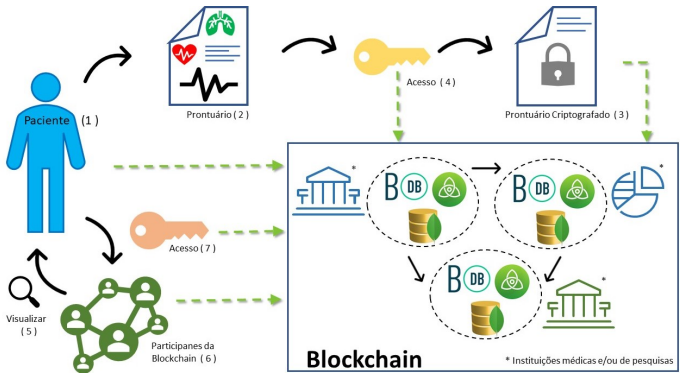

Figura 5. Visão geral do modelo proposto

4. Conclusão

A blockchain possibilita o compartilhamento das informações dos prontuários entre profissionais da saúde e empossa o paciente das informações desse documento. Também os pacientes podem controlar os acessos aos seus dados e com isso, o controle passa a ser de propriedade do paciente. Este trabalho apresenta a utilização de uma alternativa para armazenar prontuários médicos em um cenário de uso da blockchain. Apesar de algumas soluções já terem demonstrado ser promissor, na sua maioria utilizam blockchains que são suportadas por criptomoedas ou necessitam de pagamentos de taxas. Aqui foi proposto a utilização de uma solução que utiliza um banco de dados orientado a documentos e um mecanismo de consenso através de votação. Além disso, é abordado uma ideia de utilizar um prontuário estruturado e também sugere a criptografia dos dados mesmo que a solução esteja em um blockchain privada. Assim, os dados serão visualizados somente pelos participantes que os proprietários permitirem.

Referências

Zhealth soluções blockchain para o setor da saúde. http://zhealth.com.br/. Acessado: 2020-03-16.

CFM and SBIS (2012). A certificação de sistemas de registro eletrônico de saúde. In *Cartilha sobre Prontuário Eletrônico*.

da Costa, C. G. A. (2001). *Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenharia de Software*. PhD thesis, UNIVERSIDADE ESTADUAL DE CAMPINAS.

Dagher, G. G., Mohler, J., Milojkovic, M., and Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39:283 – 297.

Ekblaw, A., Halamka, A. A. J. D., and Lippman, M. A. (2016). A case study for blockchain in healthcare: m̈edrecp̈rototype for electronic health records and medical research data. Technical report, MIT Media Lab, Beth Israel Deaconess Medical Center.

Hyppönen, H., Saranto, K., Vuokko, R., Mäkelä-Bengs, P., Doupi, P., Lindqvist, M., and Mäkelä, M. (2013). Impacts of structuring the electronic health record: A systematic review protocol and results of previous reviews. *International journal of medical informatics*, 83.

Karafiloski, E. and Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, pages 763–768.

Kwon, J. (2014). Tendermint: Consensus without mining. *Tendermint*.

MongoDB (2017). Building enterprise-grade blockchain databases with mongodb. *A MongoDB White Paper*.

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

Quaini, T., Roehrs, A., da Costa, C. A., and da Rosa Righi, R. A model for blockchain-based distributed electronic health records. *IADIS International Journal*, 16:66 – 79.

Ramesh, S. Introducing medblocks - storing medical records securely on the interplanetary file system using blockchain technology. https://medium.com/medblocks/introducing-medblocks-storing-medical-records-securely-on-the-interplanetary-file-system-using-20f4e88c9bda. Accessed: 2020-05-11.

Rouhani, S., Butterworth, L., Simmons, A. D., Humphery, D. G., and Deters, R. (2018). Medichaintm: A secure decentralized medical data asset management system. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*.