Transação segura de informações médicas usando BigchainDB

Aldair C. D. Klein, Cleiton S. Baloneker, Matheus C. Pelegrino, Nilson M. Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

{camargoterabyte,cleitonbaloneker,matheuscastroweb,nilsonmori}@gmail.com

Abstract. *The use of BigchainDB in healthcare applications can enable decentralization and facilitate access control. This article presents a model for medical data transactions, using security techniques, aiming to guarantee privacy and access control. Threrefore, in addition to the immutability of data guaranteed by the blockchain, it is possible to guarantee access only to the patient and the professionals authorized by him.*

Resumo. *O uso do BigchainDB em aplicações de saúde pode possibilitar a descentralização e facilitar o controle de acesso. Este trabalho apresenta uma proposta para transação de dados médicos, utilizando técnicas de segurança, visando garantir a privacidade e o controle de acesso. Dessa forma, além da imutabilidade dos dados garantido pela blockchain, é possível a garantir o acesso somente ao paciente e aos profissionais por ele autorizados.*

1. Introdução

Blockchain é uma sequência de blocos onde cada um deles contém um determinado número de transações, dessa forma ela funciona como um registro público de todas as movimentações realizadas e qualquer um pode checar a legitimidade de uma transação. Cada bloco é dividido em duas partes: *cabeçalho* e *dado*. No campo *cabeçalho* são armazenados os metadados da transferência, tais como o identificador da transferência do bloco anterior; No campo *dado* são armazenados os dados de transferência que foi efetuada [da Conceição et al. 2019].

O BigchainDB é um banco de dados que simula o comportamento da blockchain, sendo parte de suas características, tais como: controle descentralizado, imutabilidade, criação e transferências digitais. Além disso, características como a escalabilidade, velocidade de escrita e leitura e capacidade de extração de dados através de linguagens de *query* utilizando o MongoDB estão presentes. Ele se difere de banco de dados tradicionais por algumas características citadas acima, além de não existirem operações como *delete* e *update*, sendo possível apenas criar ou transferir um registro [McConaghy et al. 2016].

Este trabalho apresenta uma proposta de transação de dados, através de uma carteira baseada em blockchain, uma tecnologia que vem sendo cada vez mais utilizada como uma solução de garantia de segurança aos dados. O objetivo da proposta é tornar o usuário o próprio gestor do acesso aos seus dados médicos, permitindo que o paciente conceda acesso ao profissional de saúde diretamente através da blockchain. Para tal, utilizaremos um banco de dados orientado a documentos com características da blockchain, o BigchainDB, banco de dados que oferece descentralização, imutabilidade e transferências de ativos digitais.

2. Trabalhos Relacionados

Em [Lavina 2018] é apresentado um estudo para validação do uso da blockchain para o tráfego de dados médicos, concluindo que a blockchain pode ajudar no compartilhamento de informações entre diversas entidades, fazendo que o paciente tenha em mãos todas as informações do seu histórico médico auxiliando os profissionais da saúde a tomar decisões mais assertivas.

Em [Leoratto and Guimarães 2020] é apresentado um modelo de prontuários eletrônicos baseado em blockchain, no qual qualquer transação é chamada de ativo. No ativo *paciente* são armazenados: chave pública; identificador; dados do paciente e dos responsáveis. Esses ativos possuem o identificador do cliente e só podem ser criados com a chave privada do paciente. No ativo *instituição* são registradas as informações das entidades de saúde e também sua chave pública, além do ativo administrador para acesso de emergência. No ativo denominado *prontuário* são armazenados os dados médicos, sendo assinado com a chave privada do paciente. Por fim, no ativo denominado *acesso* estão armazenados o identificador do prontuário e as chaves públicas dos responsáveis, instituição, administradora e paciente. A solução funciona de maneira com que o paciente crie o *prontuário*, cifrado com uma chave simétrica e armazenado no banco de dados. A chave simétrica utilizada é criptografada utilizando todas as chaves públicas dos proprietários do prontuário, criando assim o ativo acesso.

Em [Lamblet et al. 2020] é apresentada uma arquitetura para compartilhamento de dados entre médico e paciente através de criptografia ponta a ponta, é utilizado o algoritmo Diffie-Hellman em combinação ao AES (*Advanced Encryption Standard*) para proteção dos dados e uma API (*Application Programming Interface*) para integração de outras plataformas. A solução consiste em usuários se cadastrarem na plataforma por meio da geração de um par de chaves assíncronas. A chave pública é armazenada no banco de dados e a chave privada é cifrada com AES, utilizando a senha do usuário, e devolvida para ele. Para a transferência de dados é gerado um *token* com a chave privada do usuário e a pública do destinatário utilizando Diffie-Hellman, o arquivo é convertido para base64 e cifrado utilizando o *token* gerado. Para a recuperação, um profissional da saúde deve informar sua chave privada e a chave pública do paciente, derivando o *token* com Diffie-Hellman, permitindo a decifragem e a decodificação.

Este trabalho busca promover transação segura e centralização de dados médicos, de forma que o paciente tenha total controle. Diferentemente de [Lamblet et al. 2020], a solução apresentada realiza a transação dos dados utilizando o BigchainDB, tornado o usuário o único dono, permitindo o compartilhamento por tempo limitado, mas não permitindo que outro usuário possa transferir esse dado para um terceiro. Nesta proposta é possível que outros sistemas se integrem, diferente de [Leoratto and Guimarães 2020] e de [Lavina 2018], provendo uma centralização dos dados médicos do paciente.

3. Proposta

Com a utilização de um banco de dados baseado na Blockchain, junto com a utilização de criptografia simétrica e criptografia assimétrica é possível que essa centralização seja feita de forma segura. Com o BigchainDB é possível garantir rastreabilidade, imutabilidade e permitir a criação e transferências digitais. O modelo proposto conta com três ativos: *Paciente, Registro e Permissão*:

Paciente: armazena os dados de acesso à plataforma dos pacientes, profissionais da saúde e entidades médicas, tais como: nome, CPF/CNPJ, senha e a chave pública;

Registro: armazena a *chave de acesso*, gerada aleatoriamente e cifrada utilizando o algoritmo RSA (*Rivest–Shamir–Adleman*) com a chave pública do paciente, uma identificação do dono do registro e os dados médicos (cifrados com o algoritmo AES, utilizando a chave aleatória);

Permissão: armazena a *chave de acesso* (cifrada utilizando o algoritmo RSA com a chave pública do profissional de saúde), identificador do registro, identificador do usuário que terá acesso e uma data de validade.

Durante o cadastro de um usuário é gerado um um par de chaves assimétricas, a chave pública é armazenada no ativo *Paciente* bem como as outras informações de acesso do usuário, como CPF/CNPJ, senha e nome.

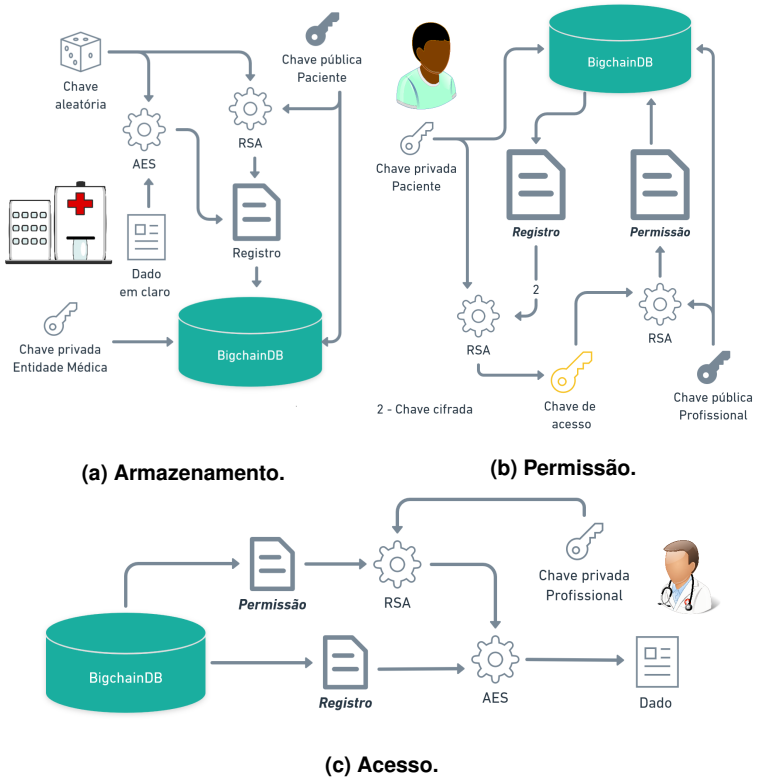

Figura 1. Funcionamento do modelo com o BigchainDB.

Para realizar o armazenamento de informações médicas, uma entidade deverá informar o paciente destinatário e o dado médico. Dessa forma, uma *chave de acesso* é gerada aleatoriamente e é utilizada para cifrar o dado médico, através do algoritmo AES. A *chave de acesso* é cifrada, utilizando o algoritmo RSA com a chave pública do paciente, e é armazenada no ativo *Registro*, além da identificação do paciente e o dado médico cifrado. Para criar a transação no BigchainDB a entidade médica precisa de sua chave privada para assinar a transação e a chave pública do destinatário para referenciá-lo como dono. O processo de armazenamento é apresentado na Figura 1a.

Para conceder acesso de determinado dado médico para um profissional de saúde, o paciente primeiramente deve fazer com que o destinatário possa decifrar o registro. Para

isso, o paciente informa sua chave privada para que o sistema possa decifrar e em seguida cifrar a *chave de acesso* com a chave pública do profissional de saúde e armazenando no ativo *Permissão*, juntamente com a identificação do profissional de saúde, a identificação do registro médico e uma data de validade. Agora, de posse dessas informações, é criado o ativo *Permissão*, com a chave pública do destinatário e a privada do paciente para assinar a transação. A atribuição de permissão é apresentada na Figura 1b.

Para que um profissional de saúde possa acessar um dado médico, ele deve selecionar qual dado quer acessar, através do ativo *Permissão*. Posteriormente é verificada a validade do acesso, a identificação do *Registro* e é solicitada a chave privada do profissional de saúde para decifrar a *chave de acesso*. Por fim, o *Registro* é decifrado com a *chave de acesso* e o profissional de saúde pode ler o dado médico. O processo de acesso é apresentado na Figura 1c.

4. Conclusão

A utilização de blockchain pode trazer benefícios para sistemas de informação aplicados à saúde, permitindo o compartilhamento entre diversas entidades, facilitando o acesso ao histórico médico e auxiliando na tomada de decisões mais assertivas [Lavina 2018].

Este trabalho apresentou uma proposta, baseado no BigchainDB, para transação de informações médicas através da blockchain, buscando facilitar o acesso e o controle de dados médicos de forma centralizada no paciente, de maneira que ele consiga acessar todos os seus dados em um só local, não precisando acessar diversos sistemas de entidades de saúde, para assim reunir todo seu histórico médico.

Trabalhos futuros poderão ser apresentados, visando a implementação da proposta para validação da mesma, análise do desempenho do modelo proposto, bem como comparar com outros modelos, tais como [Lamblet et al. 2020] e [Leoratto and Guimarães 2020].

Referências

da Conceição, A. F., Rocha, V. M., and de Paula, R. F. (2019). Blockchain e Aplicações em Saúde. In *Livro de Minicursos [do] 19o Simpósio Brasileiro de Computação Aplicada à Saúde, 11 a 14 de junho de 2019*. Sociedade Brasileira de Computação – SBC, Porto Alegre.

Lamblet, I., Sanglard, J. A. S., and Lazarin, N. M. (2020). Sigilo médico-paciente sobre criptografia ponta-a-ponta. In *Anais da XVIII Escola Regional de Redes de Computadores*, pages 161–167, Porto Alegre, RS, Brasil. SBC.

Lavina, M. E. (2018). Validação do uso da tecnologia Blockchain para o tráfego seguro de dados na área da saúde. *Gestão da Segurança da Informação-Unisul Virtual*.

Leoratto, T. and Guimarães, M. d. P. (2020). Registros Médicos Eletrônicos com Banco de dados Blockchain. *Anais do Workshop de Computação da UNIFACCAMP (WCF)*, v. 7 - XVI WCF.

McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., and Granzotto, A. (2016). Bigchaindb: a scalable blockchain database. *white paper, BigChainDB*.