Unificação de Dados de Saúde Através do Uso de Blockchain e Smart Contracts

Bruno Machado Agostinho[1], Geomar André Schreiner[1], Fernanda Oliveira Gomes[1], Alex Sandro Roschildt Pinto[1], Mario Antônio Ribeiro Dantas[2]

[1]Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil

[2]Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Juiz de Fora (UFJF)
Juiz de Fora – MG – Brasil

{bruno.agostinho,schreiner.geomar,fernanda.gomes}@posgrad.ufsc.br

a.r.pinto@ufsc.br, mario.dantas@ice.ufjf.br

Abstract. *In recent years there have been several proposals aimed at centralizing and manipulating health data, such as the electronic medical records. Because this type of data are highly sensitive, issues as how to ensure data confidentiality have always been a chalenge. The emergence of technologies such as blockchains and smart contracts has brought new approaches to the manipulation of these data. This paper proposes the use of blockchain in conjunction with smart contracts for centralization and sharing of health data. Preliminary experiments demonstrated the feasibility of securely storing and retrieving data through the use of two pairs of asymmetric keys*

Resumo. *Nos últimos anos houveram diversas propostas visando a centralização e manipulação de dados de saúde, como prontuário eletrônico do cidadão. Por se tratarem de dados altamente sigiloso, problemas de como garantir a confidencialidade dos dados sempre foram um entrave. O surgimento de tecnologias como blockchains e smart contracts vem trazendo novas abordagens possíveis na manipulação desses dados. Este trabalho apresenta uma proposta de utilização de blockchain em conjunto com smart contracts para centralização e compartilhamento de dados de saúde. Experimentos preliminares demonstraram a viabilidade do armazenamento e recuperação dos dados de forma segura, através da utilização de dois pares de chaves assimétricas.*

1. Introdução

Tem-se verificado nos últimos anos uma discussão sobre as diversas formas de manusear e compartilhar dados de saúde [Kluge 2007], como por exemplo o prontuário eletrônico dos cidadãos. Estes dados devem ser acessadas em diversas esferas do atendimento por diferentes profissionais ou pelo próprio paciente. Como estas informações podem possuir diversas fontes distintas (hospitais, unidades básicas de saúde, UPAs e etc) é pertinente que hajam soluções de interoperabilidade que sejam capazes de concentrar os dados referentes ao paciente e seus respectivos atendimentos e procedimentos.

Porém, dados na área de saúde demandam uma atenção especial no que diz respeito à privacidade, pois toda informação gerada em consultas e procedimentos possui um sigilo entre o agente de saúde (médico, enfermeiro, entre outros) e paciente. Além disso, problemas como troca de informações entre médicos e quais pacientes os agentes devem ter acesso trazem ainda mais complexidade para o cenário. Recentemente, uma nova abordagem vem chamando a atenção para aplicações na área de saúde e interoperabilidade de dados, a utilização de *blockchains*.

A *blockchain* é uma tecnologia que lida com informações em aplicações *Peer-to-peer* [Nakamoto 2008]. Cada nodo pertencente a rede é uma ferramenta de armazenamento e validação dos dados. Os nodos validam as informações e entram em um consenso sobre quais dados devem ser inseridos na *blockchain*. Aliado ao crescimento da *blockchain* temos a ascensão dos *smart contracts*. Proposto pela primeira vez por *Nick Szabo* [Szabo 1997], os *smart contracts* ganharam popularidade com o lançamento da *crypto-moeda* Ethereum[1]. Eles consistem na construção de contratos que podem ser utilizados e validados por uma ou mais partes a fim de estabelecer troca de recursos de maneira segura.

Durante muito tempo diversas restrições envolvendo a manipulação de dados médicos foram consideradas entraves para a aplicações desse tipo. A ascensão do conceito de *blockchain* vem trazendo novas perspectivas e abordagens a antigos problemas de pesquisa. A unificação de dados de saúde é apenas um deles. A forma de utilização de dados proposta no contexto de *blockchain*, assim como os conceitos de *smart contracts*, traz uma nova gama de possibilidades de aplicações para utilização e troca de dados.

Sendo assim, este trabalho tem como objetivo apresentar uma nova solução para o problema de interoperabilidade de dados de saúde utilizando *blockchain* como meio de armazenamento e *smart sontracts* para o compartilhamento destas informações de maneira segura.

O restante deste artigo está organizado conforme segue. A Seção 2 apresentando alguns conceitos relacionados para o melhor entendimento da proposta. Na Seção 3 serão apresentados alguns trabalhos relacionados utilizados para comparação e validação da proposta. Já a Seção 4 apresentada a proposta de aplicação para centralização dos dados de saúde, tendo seus resultados experimentais apresentados na Seção 5. A Seção 6 apresenta as conclusões preliminares e trabalhos futuros.

2. Preliminares

Nesta Seção são apresentados os principais conceitos envolvidos no trabalho. Inicialmente é apresentada, de maneira breve, a arquitetura da *blockchain* e como esta opera. Então são apresentados os algoritmos de consenso utilizados para verificação da confiabilidade dos nodos e dos dados.

2.1. Blockchain

Segundo [Tasatanattakool and Techapanupreeda 2018], *blockchain* é uma forma de armazenamento de dados não centralizada, confiável e difícil de utilizar para fins fraudulentos. Já para [Saraf and Sabadra 2018], pode ser definida como um livro-razão distribuído, em

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

uma arquitetura *peer-to-peer*, onde todos os nodos conectados possuem uma cópia dos dados, sem precisar de um banco de dados centralizado. Sendo desenvolvida em uma arquitetura distribuída,a *blockchain* pode ser considerada um sistema puramente *peer-to-peer* [Tama et al. 2017].

O funcionamento de uma *blockchain* acontece através de um conjunto de blocos conectados de maneira imutável. Caso haja uma tentativa de alteração nos dados de um bloco, todos os blocos a partir deste passam a ser inválidos. Isso ocorre pois cada bloco aponta para seu anterior através de um *HASH*. Para a geração deste *hash*, o bloco utiliza o conteúdo do bloco anterior em conjunto com o seu, gerando uma chave onde qualquer alteração pode fazer os blocos invalidarem a ligação. Uma vez que existe a premissa de que um nodo não pode confiar nos demais, os blocos são adicionados à cadeia através dos algoritmos de consenso. Estes foram projetados para que os mineradores da rede não consigam ou não tenham vantagens em manipular dados. Mineração é o processo de introduzir um novo bloco na *blockchain*. Cada nó utiliza a cadeia para verificar se a transação é legítima e se não utiliza *tokens* já gastos [Tama et al. 2017]. Algumas arquiteturas de *blockchain* podem fornecer recompensa ao nodo que inseriu o bloco na rede. Outras pagam apenas para os nodos que ajudaram a validar as transações. Essas recompensas podem ser chamadas de camada de incentivo [Yuan and Wang 2018].

Existe ainda, um tipo de específico de aplicação dentro do contexto de *blockchain* que vem ganhando destaque. Tendo sido baseados na proposta de [Szabo 1997], os *smart contracts* consistem em uma camada acima das *blockchains* convencionais. Funcionando como classes estáticas, os contratos podem ser executados por usuários para diversas funções além de transferência de ativos. Estes possuem recursos próprios para controle de acesso, invalidação do contrato, controle de saldo entre outras funcionalidades.

2.2. Algoritmos de Consenso

Para resolver o problema de falta de confiança entra os nodos de uma *blockchain*, foram desenvolvidos algoritmos de consenso para que apenas um bloco seja inserido por vez na cadeia. Segundo [Watanabe et al. 2015] um algoritmo de consenso é um conjunto de regras que permite que os usuários cheguem a um acordo mútuo. Atualmente o algoritmo mais utilizado em *blockchains* é chamado de *Proof-of-Work* (POW).

O algoritmo de consenso *POW* foi proposto por [Nakamoto 2008] como uma função de custo baseado no trabalho de [Back 2002]. Sua proposta visa gerar um esforço computacional através da geração de *HASHs* onde o *HASH* gerado seja menor que a função de custo da rede. Para isso, um número aleatório, normalmente chamado de *nonce*, tem que ser gerado por diversas tentativas e utilizado em conjunto com os dados do conteúdo do bloco atual e do *HASH* do bloco anterior. O sistema redimensiona a função de custo para que cada bloco da rede proposta (*Bitcoin*) seja inserido a cada 10 minutos aproximadamente. Essa abordagem também evita problemas de nodos mal intencionados, pois dificilmente o mesmo nodo conseguirá inserir dois blocos simultâneos na rede, tendo um bloco malicioso desconsiderado em alguma tentativa de manipulação.

Devido ao alto custo computacional requerido para utilização do protocolo *POW*, alternativas tem sido propostas visando a diminuição do uso de recursos. A alternativa ao *POW* mais utilizada atualmente é o protocolo *Proof-of-Stake*, que se baseia na ideia

de aplicar “um voto por unidade de participação no sistema” na escolha do nodo que vai inserir o próximo bloco, onde a participação pode ser medida pela quantidade de unidades (*tokens*, criptomoedas) pertencentes a um nodo específico [Bentov 2016]. Dessa maneira, nodos que possuem mais *tokens* tendem a ter preferência na inserção de novos blocos.

3. Trabalhos Relacionados

Do ponto de vista acadêmico, a utilização de dados médicos para troca de informações dentro da internet não pode ser considerado algo recente. Embora sempre tenham existidos obstáculos, na maioria das vezes devido ao sigilo dos dados, diversas propostas têm sido desenvolvidas com o passar dos anos. *Chen*, em [Chen et al. 2012] propôs a utilização de uma integração de *clouds* públicas e privadas para troca de informações de prontuários eletrônicos. Em [Sucurovic 2007] foi detalhado o sistema *MEDIS* para centralização de dados de saúde, assim como as abordagens de segurança no acesso ao sistema. Em um sistema utilizando *blockchain*, [Azaria et al. 2016] propôs a utilização de contratos para mapeamento de dados, permissões e transição de estados, em uma *blockchain* que funciona como um ponteiro para bancos de dados descentralizados. *Yue*, em [Yue et al. 2016] propôs o armazenamento dos dados médicos em uma *blockchain*, e o desenvolvimento de *gateways* utilizados por usuários para o acesso a troca de informações.

O trabalho proposto por [Sucurovic 2007] teve um foco na junção de dados de sistemas de diversas instâncias de unidades de saúde. Visando a segurança, o trabalho foi voltado para políticas de acesso aos dados e ao sistema. Embora seja parte importante, não foi mencionado nenhuma prática que impedisse a manipulação dos dados uma vez que uma pessoa consiga ter acesso ao banco de dados por meio de ataques.

No trabalho de [Chen et al. 2012], foi criada uma integração entre *clouds* públicas e privadas para troca de informações. Embora tenha sido pensada em uma estrutura onde os dados ficam armazenados de maneira sigilosa, esta proposta apresentou um primeiro ponto de vulnerabilidade ao inserir uma forma de acessar as informações de um paciente como válvula de escape para emergências. Embora existam algumas regras para que isso aconteça, isso pode vir a se tornar o foco de atacantes para ter acesso a informações sigilosas. Outro ponto crítico é o acesso ao banco de dados. Uma vez que um atacante consiga acessar uma das estruturas em nuvem ele pode conseguir manipular os dados mesmo sem conseguir ler os mesmo.

Em [Azaria et al. 2016], foi proposta a utilização de *blockchains* em conjunto com *smart contracts* para gerenciamento de acessos e ponteiros para os dados médicos. Assim como os trabalhos citados anteriormente, no caso de um acesso direto a um dos servidores de BD os dados poderiam ser manipulados, estando cifrados ou não.

O trabalho de [Yue et al. 2016] apresenta muitas semelhanças com esta proposta. Em uma estrutura que parece garantir disponibilidade, confidencialidade, autenticidade e integridade dos dados, os autores propuseram o armazenamento de dados em *blockchain* e o desenvolvimento de *gateways* para leitura e troca de dados, utilizando chaves para cifrar e decifrar os dados. Embora existam semelhanças, os autores deixaram a desejar nas especificações da estrutura de troca de dados. Após sugerir a utilização de uma tabela única para inserir os dados compartilhados, as poucas informações do desenvolvimento não deixam realmente claro como o sistema faz a manipulação dos dados.

4. Proposta

Para o desenvolvimento da proposta de centralização de dados de saúde utilizando *blockchain*, foram utilizadas como modelo as camadas propostas no trabalho de [Yuan and Wang 2018]. Neste trabalho, os autores propuseram uma formalização no desenvolvimento de *blockchains*, dividindo e esclarecendo o funcionamento de cada uma das camadas, como pode ser visto na Figura 1. Embora tenham sido propostas 6 diferentes camadas (Dados, Rede, Consenso, Incentivo, Contrato e Aplicação), a esta proposta utilizou apenas 4, deixando de fora as camadas de Incentivo e Consenso. A camada de Consenso deve ser especificada e desenvolvida posteriormente enquanto a camada de Incentivo deve ser analisada para ver sua pode ser adequada a este tipo de rede.

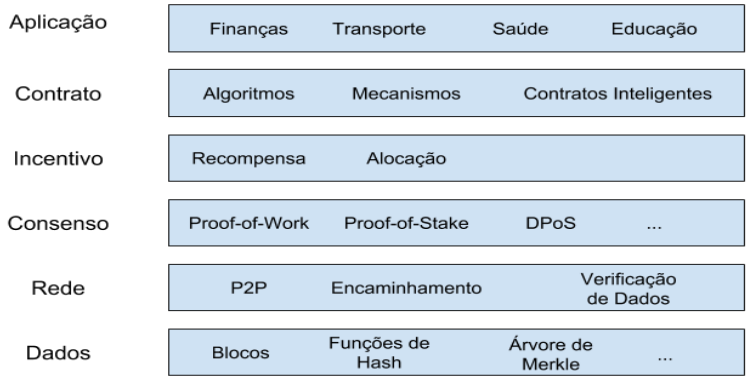

Figura 1. Camadas propostas por [Yuan and Wang 2018].

4.1. Camada de Dados

Nesta camada ficarão armazenados todos os dados gerados por qualquer tipo de interação entra pacientes, médicos, enfermeiros, procedimentos e até aparelhos hospitalares. Essas interações serão tratadas como transações, sendo armazenadas inicialmente com o status de não confirmadas. Como se tratam de dados sensíveis, o conteúdo armazenado de todas as transações é cifrado através de criptografia assimétrica, podendo serem lidas apenas pela entidade originadora da transação.

Sempre que uma interação entre paciente e agentes de saúdes ocorrer, os resultados devem ser inseridos como transações. Cada interação pode gerar até 3 transações. A primeira delas tendo como origem o paciente, a segunda o agente de saúde e a terceira para uma base de análise de dados pública. Na primeira e segunda transação, os conteúdos são cifrados pelas chaves das entidades originadoras antes de serem inseridos. A terceira transação tem como objetivo publicar dados para análise de maneira pública e é gerada utilizando apenas dados que não sejam sensíveis. Não deve ser possível identificar o paciente ou médico relacionado a essa interação. A Figura 2 demonstra como será estruturada os dados dentro da *blockchain*. Cada bloco pode alocar até N transações, variando de acordo com o tamanho máximo configurado para os blocos. Uma transação consiste nos dados de uma interação, que permanecem cifrados, e em uma assinatura digital, que visa garantir a integridade dos dados inseridos.

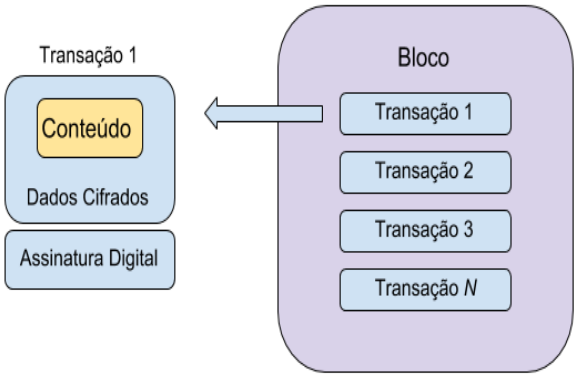

Figura 2. Bloco e Transações.

4.2. Camada de Rede

Uma vez que esta proposta pode ser aplicada para dados de saúde do país inteiro e que deve ser realizada de maneira a manter não só o sigilo, mas também evitando a propagação de falsas informações, esta deve possuir permissões. Apenas alguns nodos pertencentes à rede devem poder inserir os blocos e transações. Assim sendo, os tipos de integrantes dessa camada foram divididos em quatro perfis:

4.2.1. Usuários

O perfil de usuário na rede será utilizado pelos pacientes e agentes de saúde. Cada usuário será cadastrado em uma *blockchain* secundária tendo um identificador único (CPF) vinculado á uma chave pública que será utilizada para assinar as transações. O usuário também deverá portar um dispositivo inteligente (*token*, *smart card*) contendo duas chaves. A primeira é a chave privada correspondente à chave pública que está localizada na *blockchain* secundária. A segunda é uma chave pública que será utilizada para cifrar os dados referentes às interações entre usuários. O usuário ainda terá guardada a respectiva chave privada que pode ser utilizada para decifrar estes dados. O fluxo de uma interação entre usuários acontece da seguinte maneira:

1. Os dados da interação são gerados por um dispositivo da entidade de saúde.
2. O usuário utiliza o dispositivo inteligente.
3. Os dados da interação são cifrados utilizando a chave pública do dispositivo.
4. O dispositivo gera um *hash* dos dados cifrados e utilizada a chave privada do dispositivo para cifrar o *hash*
5. O dispositivo inteligente devolve os dados no formato de transação.
6. A transação é enviada para a lista de transações não confirmadas

Esse fluxo será repetido para cada usuário pertencente a interação, mantendo cópias da transação com acesso restrito a cada um.

4.2.2. Entidades de Saúde

As entidades de saúde serão os responsáveis pela inserção de transações não confirmadas na *blockchain*. Uma entidade de saúde pode ser um hospital, clínica, uma ambulância ou

qualquer outra entidade que esteja apta a prestar atendimento a um cidadão. Possuindo um identificador único para a entidade, deve ser possível a configuração de diversos dispositivos pertencentes a ela. Todos eles devem realizar as transações como se fossem um só, utilizando o mesmo identificador.

As entidades também são responsáveis pela geração das transações com dados da interação que não identificam o cidadão. Cada tipo de interação permitida deve ter um modelo de dados previamente cadastrado onde ficam marcados quais deles são confidenciais e quais podem ser enviados de maneira aberta.

4.2.3. Supervisor de Rede

Os nodos supervisores de rede ficam responsáveis pelas confirmações de transações e inserção de novos blocos na cadeia. Por ser uma *blockchain* do tipo permissionada, apenas nodos confiáveis, e normalmente pré-selecionados, são autorizados. O número mínimo de nodos de redes disponíveis para o funcionamento da proposta é dois. Isso acontece pois um nodo sempre ficará aguardando um número mínimo de transações confirmadas para geração de um novo bloco enquanto os outros ficam responsáveis pelas confirmações.

4.2.4. Armazenamento

O armazenamento dos dados de transações e blocos da cadeia é realizado em nodos específicos para isso. Assim como os supervisores de rede, a camada de armazenamento fica sob responsabilidade dos administradores *blockchain*. Por se tratar de uma grande quantidade de dados em um cenário onde todos os nodos possuem uma cópia exata da cadeia, os dispositivos utilizados para o armazenamento necessitam de uma configuração apropriada, não contendo riscos de limitação por espaço.

4.3. Camadas de Contrato e Aplicação

A camada de contrato será utilizada como um sistema de troca de informações entre usuários da camada de rede. Uma vez que médicos pode ter a necessidade de trocar prontuários de pacientes ou até mesmo um paciente que deseje um segundo parecer médico, o sistema deve permitir que tais dados sejam manuseados de maneira sigilosa.

O sistema para troca de informações será desenvolvido como uma aplicação descentralizada, que ficará hospedada nos nodos de dados. Os usuários terão livre acesso a seus dados, que continuarão cifrados a menos que seja utilizada a chave privada.

Quando um usuário (médico, enfermeiro, paciente, etc...) desejar compartilhar determinados dados, este deverá escolher qual o usuário vai receber os dados. Após entrar com a chave privada para decifrar os dados a serem enviados, o sistema criará um novo par de chaves, cifrando a informação com a chave pública criada e assinando com a chave pública do usuário remetente. Essa informação ficará contida em um *smart contract* que só poderá ser acessado pelo usuário remetente e pelos usuários destinatários. Ainda assim, para dificultar qualquer acesso indesejado, a chave privada para decifrar os dados será enviada em outro contrato, este será cifrado com a chave pública do destinatário. No caso de mais de um destinatário, múltiplos contratos com a mesma chave serão criados.

Após a criação dos contratos, os usuários destinatários passam a ter acesso aos dados de ambos os contratos pelo sistema decentralizado. A intenção em separar os dados em contratos diferentes é de invalidar o uso de qualquer um dos dois de maneira isolada.

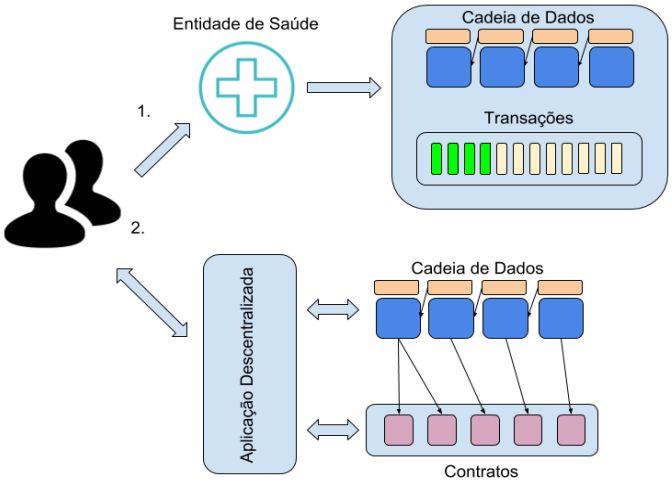

Figura 3. Arquitetura da Proposta.

A Figura 3 mostra uma visão geral sobre os possíveis fluxos de utilização de dados dentro da *blockchain* proposta. A primeira possibilidade mostra a iteração entre usuários gerando dados para uma entidade de saúde e esta inserindo novas transações na rede da *blockchain*. As transações vão sendo confirmadas e inseridas nos blocos que acabam na cadeia. No segundo fluxo é mostrada a relação entre usuários, sistema, *blockchain* e contratos.

5. Experimentos Preliminares

Para os primeiros testes de validação da proposta, foi desenvolvido um ambiente de simulação de uma *blockchain*. Os nodos da *blockchain* foram desenvolvidos em *Node.js* utilizando instâncias da biblioteca *Express*. A comunicação foi realizada através de serviços, simulando uma rede *peer-to-peer*. Cada nodo contém os serviços para listagem dos nodos da cadeia, inserção de novo nodo, verificar integridade, inserir, retornar dados e decifrar uma transação. Foram utilizados 4 instâncias para os testes. Para armazenamento, foi utilizado o Mongo DB. O objetivo dos primeiros testes foi validar a ideia de utilização de dois pares de chaves assimétricas para manipulação e garantia de confidencialidade dos dados. Para isso, cada instância foi criada com dois pares de chaves *RSA*, utilizando a biblioteca URSA. No BD, foram criadas duas coleções. A primeira foi utilizada para vincular uma chave pública a um identificador do usuário, que conforme a proposta utilizará o CPF. A Figura 4 mostra como ficaram armazenadas as chaves públicas no Mongo DB.

Para a validação do uso dos pares de chaves, foi desenvolvido um teste para inserção dos dados cifrados e assinados no BD. Antes de enviar os dados para os outros nodos, o conteúdo da transação de teste foi definido como “Esta transação não pode ser acessada.”. O conteúdo foi então cifrado pela chave pública do par 1. Para garantir a integridade, um *hash SHA1* foi calculado em cima do conteúdo cifrado e este *hash* foi cifrado utilizando a chave privada do par 2. A transação então foi enviada para o BD contendo as informações: ID, CPF, DADOS e ASSINATURA.

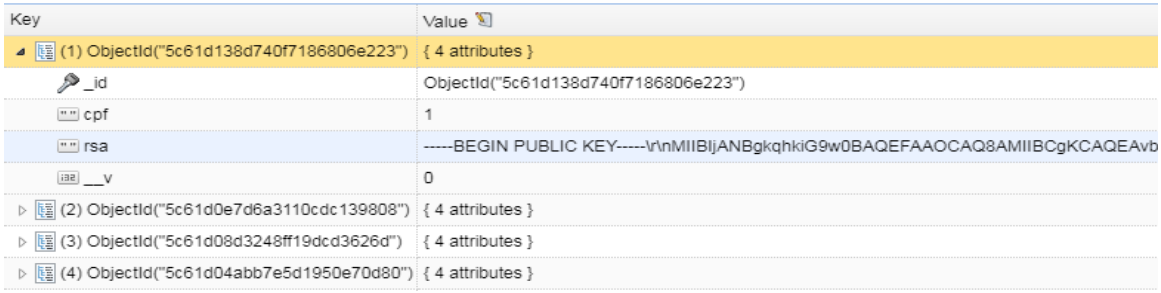

Figura 4. Armazenamento das chaves públicas.

Figura 5. Interface de validação.

Para o acesso às transações foram desenvolvidas algumas telas utilizando *HTML* para simular a parte correspondente a aplicação decentralizada da proposta. Utilizando o identificador o usuário pode baixar os dados da transação e decifra-los utilizando sua chave privada do par 1.

A Figura 5 apresenta um exemplo de utilização da funcionalidade de acesso aos dados. Na Figura 5 (A) foi utilizado o identificador da transação para baixar os dados da transação ainda cifrado. A Figura 5 (B) mostra os dados da transação após a utilização da chave privada. Conforme mencionado anteriormente, a transação de teste continha uma *string* de valor ”Esta transação não pode ser acessada”.

6. Conclusão e Trabalhos Futuros

O trabalho de pesquisa apresentado neste artigo sugere a utilização de *blockchains* em conjunto com *smart contracts* a fim de viabilizar a centralização e manipulação de dados médicos. Foram realizados experimentos iniciais em relação a validação da proposta de utilizar dois pares de chaves assimétricas para garantir a confidencialidade dos dados. Os resultados preliminares demonstraram a viabilidade o uso de pares e da utilização do formato de transação sugerido, com os dados cifrados por um par de chaves e assinado por outro.

Por se tratar de um trabalho em andamento, é necessária a implementação completa da proposta para a devida validação. São necessários testes utilizando uma *blockchain* real e não mais simulada. Uma hipótese a fim de otimizar o armazenamento é usar a *blockchain* apenas os dados de *hash* das transações mantendo os dados efetivos no *MongoDB* .

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.

Back, A. (2002). Hashcash - a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf. Acessado: 11/02/2019.

Bentov, Iddo; Pass, R. S. E. (2016). Snow white: Provably secure proofs of stake. https://eprint.iacr.org/2016/919.pdf. Acessado: 11/02/2019.

Chen, Y.-Y., Lu, J.-C., and Jan, J.-K. (2012). A secure ehr system based on hybrid clouds. *Journal of Medical Systems*, 36(5):3375–3384.

Kluge, E.-H. W. (2007). Secure e-health: Managing risks to patient health data. *International Journal of Medical Informatics*, 76(5):402 – 406.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Acessado: 11/02/2019.

Saraf, C. and Sabadra, S. (2018). Blockchain platforms: A compendium. In *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, pages 1–6.

Sucurovic, S. (2007). Implementing security in a distributed web-based ehcr. *International Journal of Medical Informatics*, 76(5):491 – 496.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).

Tama, B. A., Kweka, B. J., Park, Y., and Rhee, K. (2017). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, pages 109–113.

Tasatanattakool, P. and Techapanupreeda, C. (2018). Blockchain: Challenges and applications. In *2018 International Conference on Information Networking (ICOIN)*, pages 473–475.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., and Kishigami, J. J. (2015). Blockchain contract: A complete consensus using blockchain. In *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*, pages 577–578.

Yuan, Y. and Wang, F. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9):1421–1428.

Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40:218.