MEDICHAIN: Um *framework* para o compartilhamento seguro de mídias médicas utilizando *blockchain*

Anselmo L. E. Battisti[1], **Gabriel Carrara**[1]

[1]Instituto de Computação – Universidade Federal Fluminense (UFF)

Resumo. *O uso de mídias médicas para a tomada de decisões críticas durante o tratamento de um paciente é realidade há alguns anos. Com o aumento do uso deste tipo de mídia diversos tipos de ataques vem sendo praticados com o objetivo de roubar ou adulterar dados sensíveis de pacientes. No presente trabalho propomos um framework chamado MEDICHAIN. Ele é um modelo teórico cujo objetivo é garantir que uma determinada mídia produzida a partir de exame de algum paciente não seja adulterada ao longo da sua vida útil, garantindo assim integridade física e lógica do arquivo gerado. Para validar o modelo proposto também foi desenvolvida uma blockchain utilizando a plataforma Multichain cujos dados são armazenados e consumidos a partir de uma aplicação escrita em Python.*

Abstract. *Medical data files are used constantly to make decisions to choose the best approach about patient's health. In this scenario, it's very dangerous when someone manipulate this data. To prevent this kind of threat we propouse MEDICHAIN. It's a framework who promove the fisical and logic integrit to medical data files. To test this idea we developd a blockchain using Multichain. To store and retrieve the data our script is in Python.*

1. Introdução

As tecnologias da informação (TI) nas últimas décadas têm ganhado destaque na área médica, como aponta [Millar et al. 2000]. Diversos equipamentos operam de maneira autônoma no processo de geração de mídias digitais. Essas mídias podem ser imagens 2D; vídeos; representações 3D, etc. Médicos têm pautado suas decisões de acordo com dados coletados a partir de análises realizadas nessas mídias. Desta forma, é importante que existam mecanismos de proteção para que a mídia que esteja sendo analisada pelo médico realmente corresponda à mídia gerada a partir dos dados coletados no paciente, e mais, que a mídia que está sendo analisada seja realmente do paciente em questão.

Os sistemas para criação e consumo de mídias médicas são diversificados e heterogêneos em suas tecnologias de desenvolvimento. Essa heterogeneidade gera uma maior complexidade para gestores de TI em oferecer garantias de que todas as mídias produzidas e consumidas dentro de uma instituição médica tenham validade física e lógica. Além disso, mutias vezes a mídia é produzida em uma instituição diferente, como por exemplo laboratórios e centros de análises clínicas. Assim, garantir a integridade das mídias torna-se uma tarefa ainda mais complexa. Preocupações com relação a segurança e confiabilidade de mídias médicas já foram apontadas em diversos trabalhos acadêmicos, tais como [Barrows C. Randolph, Jr 1996], [Pan et al. 2010] e [Yue et al. 2016].

O objetivo deste trabalho é apresentar um *framework* conceitual que possibilita o compartilhamento seguro de mídias médicas entre os diversos *stakeholders* envolvidos

em seu processo de produção e consumo, de tal forma que o receptor da mídia tenha a certeza de que aquela mídia não foi de alguma forma adulterada seja durante o processo de transmissão ou mesmo no processo de armazenamento.

O presente trabalho está estruturado da seguinte forma. Na Seção 2 de referencial teórico, será apresentada uma visão geral sobre as principais tecnologias envolvidas na estruturação do MEDICHAIN, bem como uma visão geral sobre alguns trabalhos relacionados ao tema. Em seguida na Seção 3, será apresentada a estrutura do *framework*. Na Seção 4 sobre as discussões apresentaremos vantagens e desvantagens do *framework*, bem como dos detalhes de sua prova de conceito. Ao final, serão apresentadas as considerações finais do trabalho e possíveis extensões que o mesmo pode receber.

2. Referencial Teórico

Nessa seção, será apresentada uma visão geral sobre as principais tecnologias que fazem parte da estrutura do *framework* MEDICHAIN. Os principais temas abordados são: integridade de dados; mídias médicas, *blockchain* e *Multichain*. Também apresentaremos nessa seção algumas tecnologias já propostas com o objetivos similares ou complementares aos do MEDICHAIN.

2.1. Integridade de Dados

A integridade de dados é um dos principais requisitos para que uma mídia médica possa ser utilizada. Nessa seção, apresentaremos a definição adotada neste trabalho para integridade de dados. Além disso, apresentaremos algumas implicações potencialmente perigosas quanto ao uso de mídias cuja integridade tenha sido violada.

O termo integridade é utilizado na computação de diversas formas e em diversos contextos. Em contextos diferentes, o termo pode assumir significados diferentes. Por esta razão, é importante apresentar uma definição formal sobre o que é integridade dos dados no contexto MEDICHAIN.

- **Integridade física**: é utilizada para verificar se o conteúdo de uma mídia sofreu alguma alteração após a sua criação e distribuição;
- **Integridade lógica**: é utilizada para verificar se a mídia que está sendo acessada realmente pertence ao paciente do qual ela foi gerada.

A validade da integridade física de uma mídia é fundamental para que o médico possa tomar a melhor decisão com base em dados reais coletados do paciente. Um atacante malicioso ao modificar uma mídia de um paciente pode ter interesses variados, como por exemplo: induzir um médico a fornecer um tratamento inadequado a um paciente; gerar evidências para que um determinado procedimento não seja executado removendo elementos da mídia que implicariam na sua utilização; causar traumas psicológicos em pacientes.

A validade da integridade lógica por sua vez previne problemas inerentes a troca intencional ou não de mídias entre pacientes. Nesse cenário a mídia de um paciente pode ser inadvertidamente utilizada para tomada de decisão em outro paciente. Nesse caso o erro médico poderia ter sido evitado com a validação lógica da mídia.

Atacantes podem explorar tanto a integridade física como a integridade lógica de uma mídia para alcançar seus objetivos. O uso do *framework* MEDICHAIN garante aos

seus usuários tanto a validade física como a validade lógica de uma mídia. Essas garantias são alcançadas utilizando o consenso distribuído em uma rede *blockchain*.

2.2. Mídias Médicas

Mídias médicas são arquivos digitais gerados a partir de exames ou procedimentos médicos. Em geral esses tipos de arquivos devido a sua natureza são volumosos e possuem grande valor comercial. O armazenamento adequado deste tipo de dado é fundamental para uma instituição médica.

Na arquitetura do MEDICHAIN a mídia médica não é armazenada dentro da **blockchain**. Essa estratégia de arquitetura da aplicação foi tomada pois, em muitos casos, o tamanho em bits de uma mídia médica pode ser grande, dessa forma, manter uma cópia distribuída em cada um dos nós da rede poderia gerar desperdícios de recursos de armazenamento. Por essa razão, dentro da blockchain, é armazenado apenas o *hash* criptografado da mídia.

2.3. Blockchain

A *Blockchain* é um livro razão par-a-par (P2P, do Inglês *peer-to-peer*) usado como registro de transações [Antonopoulos 2014]. Para seus usuários realizarem transações, é utilizada criptografia assimétrica onde cada participante possui uma chave privada que é utilizada para assinar suas transações e uma chave pública que pode ser utilizada como endereço para recebimento das mesmas. O uso de chaves assimétricas garante que as identidades reais dos usuários sejam mantidas ocultas para a rede, sendo assim um forma de pseudonimização.

Uma transação representa a transferência da posse de um ativo entre usuários. Essa transação contém entradas que são endereços dos proprietários atuais desses ativos e a saída contém o endereço que receberá a posse do ativo. Algumas plataformas de *blockchain*, como o Bitcoin [Nakamoto 2008], permitem que múltiplas entradas e saídas sejam inseridas em cada transação. Nesse caso, cada entrada deve ser assinada com a chave privada de seu dono para provar a posse dela.

Após ser criada e assinada, a transação é transmitida para rede, onde nós chamados de mineradores, a coletam e validam. Depois de validada, a transação é então adicionada junto com outras na estrutura do bloco. Para garantir que um bloco seja criado de maneira correta e sem fraudes, as plataformas de *blockchain* implementam mecanismos de consenso para que fraudes sejam impedidas.

Para que um minerador consiga gerar um bloco válido que seja aceito pelos outros nós da rede, ele deve cumprir uma tarefa computacional. No caso da rede Bitcoin essa tarefa consiste em resolver um quebra-cabeça computacionalmente difícil conhecido como prova de trabalho (do Inglês *Proof-of-Work*, ou PoW). Porém existem outros mecanismos de consenso que são menos custosos utilizados por outras plataformas como a prova de autoridade (do Inglês *Proof-of-Authority*, ou PoA) utilizada pelo Multichain [Greenspan 2015]. [Zheng et al. 2017] cita outros mecanismos de consenso utilizados por outras plataformas de *blockchain* com diferentes propostas, são eles *Proof-of-Stake* (PoS), *Practical byzantine fault tolerance* (PBFT), *Delegated proof of stake* (DPoS) e *Ripple* e *Tendermint*. Porém com o crescimento do número de plataformas para desenvolvimento de aplicações com *blockchain* é esperado que surjam novas propostas de mecanismos.

Assim que um bloco é formado por um minerador, ele o transmite para a rede, e se for válido, é anexado ao último bloco da *blockchain*. Cada bloco contém uma referência ao seu anterior, formando assim uma estrutura de encadeamento entre cada bloco.

Depois de armazenado por algum tempo na *blokchain*, outro blocos são anexados após ele e cada bloco pode ser considerado como uma confirmação dos seus antecessores. Blocos confirmados possuem pouca ou nenhuma chance de serem modificados ou removidos da cadeia no futuro, e conforme o tempo passa, a chance de ser modificado é reduzida.

As redes de *Blockchain* podem ser caracterizadas segundo seus critérios de privacidade e atribuição de papéis na rede. Segundo [Oliveira et al. 2018], as redes podem ser classificadas em redes públicas não permissionadas, redes públicas permissionadas, redes privadas não permissionadas e redes privadas permissionadas.

Em **redes públicas não permissionadas**, há desconfiança mútua entre os usuários da rede e, por isso, os mecanismos de consenso são rígidos. A fim de evitar ataques de personificação, o consenso em redes públicas não permissionadas é oneroso, exigindo-se a resolução de um desafio computacional como prova da participação no consenso e, assim, evitando que um nó apresente diversas identidades. O incentivo aos nós a participarem desse mecanismo de consenso consiste em um incentivo econômico dado aos nós mineradores na forma de criptomoeda.

Isso é justificável pelas características principais de uma rede pública não permissionada, tais como conteúdo aberto e igualdade entre os nós. Todo nó pode ingressar e sair da rede. O participante da rede gera um par de chaves criptográficas para assinar e realizar transações quando ingressa pela primeira vez na rede. Além disso, qualquer nó pode ser um minerador e fazer parte do mecanismo de consenso da rede.

Os problemas associados às redes públicas não permissionadas estão relacionados à escalabilidade e ao tempo efetivo desde a emissão da transação até a execução na cadeia. Essas redes constituem ambientes colaborativos e, portanto, dependem do comportamento benigno dos nós. Além disso, a competição entre os nós mineradores pelas recompensas da geração do bloco torna o processo mais lento e custoso.

As **redes públicas permissionadas** foram desenvolvidas para aplicação de mecanismos de consenso menos custosos em redes públicas. A diferença entre as redes públicas não permissionadas e as permissionadas é a desigualdade de atuação dos nós na rede. Em uma rede pública permissionada, todos os dados são disponíveis para auditoria pública e não se restringem a entrada de novos nós. Contudo, um nó só participa da rede após a verificação adequada de sua identidade e, assim, alocam-se as permissões que determinam quais atividades o nó pode executar na rede.

Este tipo de rede é utilizada para gerenciar transações entre empresas ou em processos que envolvem várias entidades, permitindo que somente alguns nós de cada entidade fiquem responsáveis pela geração de blocos, aplicando mecanismos de consenso mais eficientes e escaláveis.

As **redes privadas não permissionadas** se diferenciam das redes púbicas por restringirem a entrada de nós e, portanto, só fornecem a réplica da cadeia a nós identificados por uma chave pública autorizada. Nestas redes, existe uma ou um conjunto de

instituições que determinam quem são os nós autorizados a participar da rede. Destaca-se que o conceito de rede privada se delimita ao controle de acesso aos dados da cadeia. Os nós que participam da rede têm funções iguais e exercem a mesma importância na rede, pois não se determinam permissões diferenciadas aos nós da rede. Uma vez autorizado a participar da rede, o nó pode gerar transações, gerar blocos e participar do consenso.

Esta característica é interessante às aplicações em que nós, mesmo autorizados a participar da rede, oferecem um comportamento hostil. Nesses casos, empregam-se mecanismos de consenso tolerantes a falhas Bizantinas (*Byzantine-Fault Tolerant* - BFT), exigindo que todos os nós participem do consenso.

As **redes privadas permissionadas** oferecem a oportunidade de aplicações de mecanismos de consenso mais eficientes e menos custoso em termos de processamento. A característica privada limita a entrada e permanência de nós indesejáveis na rede. As permissões possibilitam configurar diferentes papéis para os nós participantes da rede como, por exemplo, oferecer flexibilidade para aplicações permitirem que apenas alguns nós façam parte do processo de consenso e apenas um subconjunto desses nós possam gerar o próximo bloco.

Todas as características citadas anteriormente tornam a *blockchain* uma tecnologia promissora e capaz de despertar o interesse de diversos áreas de aplicação. Contudo, a aplicação de *blockchain* deve ser feita com cautela pois nestas mesmas áreas já existem outras tecnologias que podem ser utilizadas de maneira mais eficiente que a *blockchain*. Em [Wüst and Gervais 2017] pode-se encontrar diversos cenários onde o uso de *blockchain* traz reais benefícios em relação a outras tecnologias.

No contexto deste trabalho, a tecnologia da *blockchain* será aplicada para auxiliar na criação e verificação de mídias médicas de maneira que a integridade e propriedade destas mídias sejam garantidas através do armazenamento de dados referentes a elas na cadeia [Mettler 2016]. Assim também é possível verificar essas informações que estão disponibilizadas de maneira pública aos usuário da rede sem a necessidade de revelar seu conteúdo na integra para desconhecidos [Macdonald et al. 2017].

2.4. *Multichain*

A MultiChain [Greenspan 2015] é uma plataforma para desenvolvimento de aplicações utilizando cadeias de blocos, cujo projeto foi desenvolvido baseado na implementação da Bitcoin [Nakamoto 2008]. A plataforma é totalmente compatível com o protocolo e capaz de funcionar como um nó da rede Bitcoin. A MultiChain permite a criação de redes privadas permissionadas [Greenspan 2015], o que exige a participação de um administrador na rede, que é responsável por permitir a entrada e gerenciar as permissões dadas aos nós. As permissões variam desde capacidade de executar buscas na cadeia, até permissão para um nó ser minerador ou tornar outro nó administrador. O papel de administrador é concedido ao nó responsável por criar o bloco *gênesis* da rede. Sempre que um administrador concede ou revoga uma permissão de um nó, esse evento fica registrado na cadeia através de uma transação especial. Dessa forma, todos os demais nós são capazes de verificar quais permissões estão vinculadas a cada chave pública da rede.

Usuários de uma rede MultiChain são capazes de criar e gerenciar seus próprios ativos, através de uma transação especial, chamada ”Transação Gênesis”, que contém os metadados necessários para registrar o canal na cadeia de blocos [Greenspan 2015]. Para

tanto, o usuário deve possuir a permissão concedida por um administrador da rede. Após a criação do canal, o criador assume o papel de administrador, podendo decidir quem pode enviar, receber e criar novos ativos naquele canal. A criação de canais privados permite que apenas os usuários que tenham interesse em um certo tipo de ativo obtenham acesso ao canal e às informações presentes na cadeia relativa ao ativo.

Ao contrário da plataforma Bitcoin, a MultiChain não possui suporte à implementação de regras. Logo, um usuário é apenas capaz de enviar e receber ativos pela rede. No entanto, quando utilizada para se conectar à rede Bitcoin, a plataforma fornece suporte à criação de regras através da linguagem *Script*. O mecanismo de consenso oferecido pela MultiChain permite que, através da configuração de parâmetros no momento da criação da rede, o consenso funcione como uma prova de trabalho ou que cada minerador alterne na criação de um novo bloco, sem a necessidade de haver competição. Isso permite que haja maior flexibilidade na criação de novas redes e elimina os altos custos computacionais da prova de trabalho. A manutenção da prova de trabalho permite a retrocompatibilidade com a rede Bitcoin.

Esta plataforma foi escolhida para implementação devido a sua praticidade e versatilidade. Com essas características em conta o esforço de implementar a arquitetura proposta nesse trabalho pôde ser focado na integração das mídias à plataforma, uma vez que ela não possui suporte nativo para esse tipo de dados. Assim os resultados puderam ser obtidos de maneira rápida e sem grandes exigências de recursos.

2.5. Trabalhos Relacionados

Nesta seção serão apresentados algumas propostas já desenvolvidas utilizando diversas tecnologias com o objetivo de garantir a integridade de mídias médicas. Buscamos não apenas trabalhos que utilizam validação distribuída de consenso em sua estrutura, mas também, alternativas locais que visam validar a integridade de um determinado arquivo.

A abordagem adotada por [Guo and Zhuang 2009] e [Shao et al. 2015] utiliza em sua estrutura o conceito de marca d'água sem perda de qualidade ou inclusão da marca d'água em regiões da imagem cujo conteúdo não afeta o entendimento da imagem original. Em ambas as propostas bits são incluídos na imagem que garantem a integridade física da mesma em função da marca d'água invisível.

Um modelo cujo objetivo é atender a uma gama maior de requisitos foi proposto por [Patel 2018]. Sua proposta apresenta um *framework* que utiliza a tecnologia blockchain para garantir que apenas pessoas autorizadas tenham acesso aos registros médicos de um determinado paciente. Essa abordagem garante tanto a integridade física como a integridade lógica das mídias, entretanto, a viabilidade técnica da implementação do framework devido a complexidade do mesmo pode limitar a sua utilização.

A proposta apresentada por [Yue et al. 2016] mostra uma alternativa para um *gateway* onde os pacientes têm uma visão geral sobre os seus dados médicos, de tal forma que é possível definir quais médicos terão acesso aos seus dados. Na proposta apresentada a mídia médica é armazenada dentro da *blockchain*. Nós acreditamos que essa não é a melhor abordagem pois essas mídias são volumosas, sendo assim, o crescimento da *blockchain* pode ser exponencial, inviabilizando a participação de nós com um poder computacional pequeno.

A utilização de marcas d'água e *blockchain* como forma de garantir a integridade física de uma mídia foi proposta por [Bhowmik and Feng 2017]. O trabalho apresenta um esquema que permite não apenas a detecção de modificações como também a identificação das regiões modificadas. Essa proposta garante a integridade física mas não a integridade lógica da mesma.

Com base em nossos esforços de pesquisa não conseguimos encontrar uma solução distribuída que garantisse a validade lógica e física de uma mídia média.Assim, propomos o *Framework* MEDICHAIN. Na próxima sessão serão apresentados os detalhes do mesmo.

3. *Framework* MEDICHAIN

Nessa seção é apresetnado de forma conceitual o *framework* MEDICHAIN. Serão detalhados quais são os agentes envolvidos e, de que maneira eles estão relacionados. Podemos descrever em linhas gerais o *Framework* MEDICHAIN como uma plataforma que utiliza uma *blockchain* de forma que os usuários de uma mídia médica tenha um banco de dados distribuído para confirmar a sua integridade física lógica. Uma imagem esquemática do *framework* pode ser vista na Figura 1.

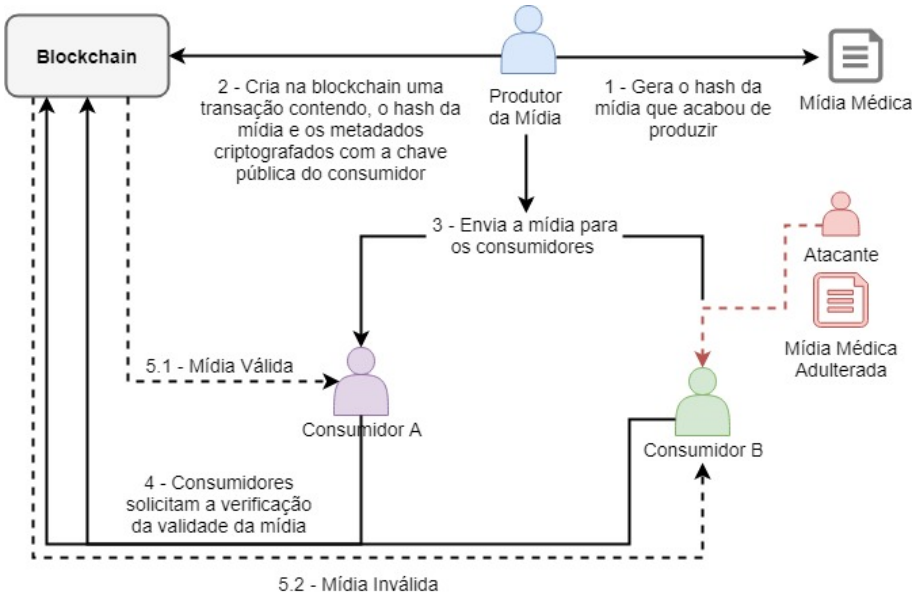

Figure 1. Modelo esquemático do *framework* MEDIACHAIN

Os agentes envolvidos no *framework* MEDICHAIN são **produtor da mídia** e o **consumidor da mídia**. É importante observar que uma mesma pessoa ou entidade pode desempenhar tanto o papel de produtor como consumidor da mídia. Essa divisão conceitual apresenta apenas a responsabilidade de cada um dos agentes no processo que garante a integridade das mídias.

Os produtores são todas as instituições e profissionais que produzem mídias médicas. Laboratórios de análise, clínicas de radiologia entre outros são alguns exemplos. Eles são os responsáveis por, após a geração da mídia, registrar a mesma na *blockchain*. O processo de registro da mídia consiste nas seguintes etapas, como pode ser visto no Algoritmo 1.

Algoritmo 1 Registrar mídia na *blockchain*

1: Abrir o arquivo como leitura;
2: Gerar o *hash* do arquivo;
3: Gerar os metadados da imagem;
4: Assinar os metadados da mídia com a chave pública do destinatário da mídia (essa é uma etapa opcional);
5: Estabelecer a conexão com a *blockchain*;
6: Criar uma transação cuja chave seja o *hash* da imagem e o *payload* sejam os metadados.

É importante observar que a mídia em si não é armazenada na *blockchain*. Na *blockchain* serão armazenados apenas o *hash* e os metadados associados à mídia. O *hash* será utilizado para validar a integridade física, já os metadados serão utilizados para validar a integridade lógica da mídia.

O *hash* da mídia possui um outro papel de grande relevância dentro da arquitetura, ele será usado como chave de busca. Na abstração proposta, durante a abertura da mídia médica o sistema fará uma consulta na **blockchain** pelo hash do arquivo que está sendo aberto. Duas situações podem acontecer, ou existe uma transação cujo índice é o *hash* ou, não existe uma transação. Caso exista a transação, então, a integridade física da mídia está mantida. Caso não exista isso significa ou que a mídia não foi vinculada na **blockchain** ou ocorreu uma violação na mídia. Em ambos os casos, não pode-se atestar a integridade física da mídia.

Os consumidores são todos as instituições e profissionais que necessitam da mídia para realizar algum procedimento referente ao paciente gerador da mídia. Os consumidores são responsáveis por utilizar a estrutura proposta com o objetivo de garantir a integridade física e lógica da mídia médica. O processo de validação de uma mídia consiste nas seguintes etapas, como pode ser visto no Algoritmo 2.:

Algoritmo 2 Registrar mídia na *blockchain*

1: Abrir o arquivo como leitura;
2: Gerar o *hash* do arquivo;
3: Consultar na *blockchain* se existe uma transação cujo id é *hash*;
4: A *blockchain* retorna a transação caso ela exista, caso contrário um erro será gerado;
5: Se a transação existir E existirem metadados então eles devem ser descriptografados com a chave privada do consumidor da mídia.

A *blockchain* proposta para o MEDIACHAIN possui uma estrutura híbrida. Nela, os produtores têm permissão para inserção de novas transações na *blockchain*, ao passo que os consumidores poderão apenas realizar consultas de verificação de integridade de uma mídia. A participação como consumidor na *blockchain* é pública, ou seja, qualquer pessoa poderá participar dela, porém, para a participação como produtor de mídia será necessária a solicitação da autorização de uma entidade centralizadora.

A integridade lógica da mídia médica é alcançada a partir dos metadados da mídia que estão armazenados na *blockchain*. Esse tipo de integridade pode ser utilizado ou não, como descrito anteriormente. Caso o produtor da mídia opte por incluir elementos para a

validação lógica da mídia, então o produtor irá assinar os metadados com a chave pública do destinatário da mídia médica. A validação lógica ocorrerá no ato da solicitação da validade física da mídia, nesse momento, caso exista uma transação associada ao *hash* da mídia que está sendo aberta, esses metadados criptografados são entregues ao cliente que usará sua chave privada para ler os dados. Caso o cliente consiga abrir os metadados então a mídia realmente era destinada para ele.

Uma observação importante sobre os metadados utilizados no MEDICHAIN, é que não foi proposta uma uma sintaxe, ou mesmo padrão de metadados. A escolha sobre quais metadados serão incluídos na *blockchain* deverão ser previamente acordados entre o produtor e o consumidor da mídia. Isso é importante, pois o framework é genérico e, caso fosse definido um conjunto mesmo que mínimo de dados para serem incluídos nos metadados poderia-se assim limitar a implantação dessa arquitetura.

A arquitetura proposta pode ser considerada uma proposta progressiva pois, a implementação da validade física não necessariamente implica a obrigatoriedade da implantação da validade lógica. O MEDICHAIN foi planejado dessa forma para que a implantação possa ser realizada de forma gradativa. Ou seja, uma instituição pode iniciar o processo de implantação da validade física e posteriormente implantar a validade lógica sem que haja necessidade de se reescrever toda a *blockchain*

4. Avaliação e Resultados

Nesta seção serão discutidos aspectos referentes à implementação da prova de conceito do MEDICHAIN. Serão apresentadas também as tecnologias utilizadas e as correlações existentes entre elas. Além disso, serão apresentados dados referentes ao desempenho da arquitetura, tanto do tempo de inclusão de mídias como do tempo de validação das mesmas.

4.1. Tecnologia Utilizada

A fim de testar a viabilidade técnica do MEDICHAIN, foi realizada a implementação de uma prova de conceito da plataforma. É importante ressaltar que o modelo teórico é independente de plataforma de *blockchain* ou de linguagem de programação. De qualquer forma, alguns pré-requisitos existentes tanto para a linguagem de programação são:

1. A *blockchain* deve permitir a criação de uma cadeia híbrida, onde alguns membros podem inserir dados e outros apenas consultar;
2. A linguagem de programação deve ser capaz de realizar consultar e inserções de transações nessa *blockchain*.

Para a prova de conceito implementada optou-se pela linguagem de programação Python e pela *Multichain*. Essas duas tecnologia foram escolhidas pois a plataforma *Multichain* possui uma curva de aprendizado baixa, facilitando assim a sua utilização na implementação de provas de conceito. A linguagem Python foi escolhida pois a mesma já possui bibliotecas para a comunicação com a *Multichain*. Neste trabalho, foi utilizada a biblioteca Savoir https://github.com/DXMarkets/Savoir para a integração entre o Python e o *Multichain*.

4.2. Ambiente de Teste

Nessa seção, descreveremos de forma sucinta o ambiente de teste onde a prova de conceito foi desenvolvida. A fim de realizar simulações fidedignas como as utilizadas em um ambiente real optou-se pelas seguintes configurações de máquinas clientes e servidor.

1. Os nós servidores são máquinas que rodam Linux e estão alocadas em datacenters da DigitalOcean;
2. As máquinas cliente são máquinas Windows e Linux rodando localmente.

Tanto nos nós clientes, como nos nós servidores, roda uma instância do *Multichain*. A aplicação realiza a comunicação com a *blockchain*, a partir de conexão RPC. Durante o processo de inicialização da *blockchain* é necessário especificar parâmetros que definem qual será o usuário e senha para essas chamadas. Esse usuário e senha são apenas para o nó local que está sendo consultado pelo consumidor ou produtor da mídia. No *Multichain* para iniciar um nó habilitado para chamadas RPC é necessário executar o seguinte comando: ”Multichaind.exe chain1 -rpcuser=foo -rpcpassword=bar”.

4.3. Desempenho

A fim de validar o desempenho do modelo proposto, foram realizados testes para medir os tempos de inserção e de consulta de uma determinada mídia na *blockchain*. Os testes foram realizados utilizando como forma de controle o número de mídia inseridas previamente na *blockchain*. Os testes foram realizados da seguinte forma:

- A *blockchain* foi inicializada sem nenhum bloco;
- Foram geradas 1000 imagens aleatórias;
- Foi realizada a inserção de 10 imagens e depois foi realizada a consulta por cada uma das imagens inseridas e o tempo médio foi computado;
- O procedimento anterior foi repetido para 100, 500 e 1000 imagens.

Na Figura 2 podem ser vistos os resultados dos testes realizados. Os testes mostram que o tempo de inserção foi constante em relação ao número de mídias previamente armazenados na `blockchain`, ao passo que houve um aumento quase linear do tempo de consulta em relação ao número total de mídias previamente inseridas.

Outro teste que foi realizado foi a adulteração aleatória de mídias previamente inseridas na rede. Em 100% dos casos a imagem que sofreu a modificação foi identificada. Para que um atacante consiga realizar com sucesso um ataque desse tipo ele deve burlar a própria estrutura da *blockchain* para modificar o conteúdo do hash previamente inserido na rede.

5. Considerações Finais

Podemos concluir que os objetivos propostos neste trabalho foram alcançados uma vez que o MEDICHAIN oferece os recursos de validação da integridade física e lógica para mídias médicas. A integridade física foi obtida a partir da implementação da consulta do *hash* da mídia médica na *blockchain* e, a validade lógica foi obtida a partir da analise dos metadados armazenados pelo produtor da mídia na *blockchain*. Além disso, a prova de conceito desenvolvida mostrou que existe a viabilidade técnica para a implantação da arquitetura.

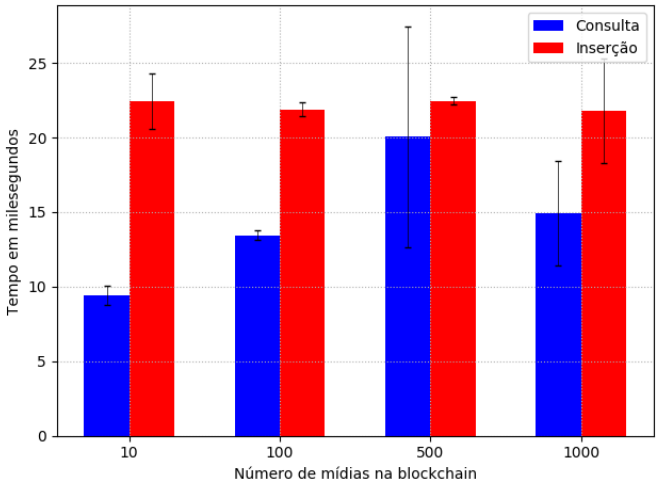

Figure 2. Relação entre o número de mídias na *blockchain* e o tempo das operações de consulta e inserção.

Uma das limitação observadas no MEDICHAIN está relacionada com a validade lógica de mídias que precisem ser compartilhadas por mais do que um consumidor. Caso dois ou mais consumidores precisem da mesma mídia, não será possível incluir elementos de integridade lógica pois o *hash* da mídia é único e portanto, não será possível incluir na *blockchain* duas transações com o mesmo *hash* contendo metadados criptografados com chaves diferentes. Uma possível solução para esse problema seria a incorporação de um controle de acesso mais elaborado onde os dados seriam criptografados com duas chaves públicas.

Como trabalho futuro, pretende-se desenvolver uma aplicação para que os usuários possam interagir com a *blockchain* de forma mais intuitiva. Além disso, será desenvolvida uma interface Web pra o gerenciamento de solicitações de entidades que tenham interesse em participar do MEDICHAIN.

Referências

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. ” O’Reilly Media, Inc.”.

Barrows C. Randolph, Jr, P. D. C. (1996). Privacy , Confidentiality : and Electronic Medical Records Abstract The enchanced Goals of Informantional Security In Health Care. *Journal of the American Medical Information Association*, 3(2):139–148.

Bhowmik, D. and Feng, T. (2017). The multimedia blockchain: A distributed and tamper-proof media transaction framework. *International Conference on Digital Signal Processing, DSP*, 2017-August(August).

Greenspan, G. (2015). Multichain private blockchain—white paper. *URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf*.

Guo, X. and Zhuang, T. G. (2009). A region-based lossless watermarking scheme for enhancing security of medical data. *Journal of Digital Imaging*, 22(1):53–64.

Macdonald, M., Liu-Thorrold, L., and Julien, R. (2017). The blockchain: A comparison of platforms and their uses beyond bitcoin. Technical report.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *Proc. of International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3.

Millar, G., Saks, A. M., and Tomlinson, G. (2000). The practice of. *Journal of the American Medical Informatics Association*, 7(1):1–20.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Oliveira, M. T., Carrara, G. R., Fernandes, N. C., Albuquerque, C. V., Carrano, R. C., Medeiros, D. S., Mattos, D. M., and Niterói, R. (2018). Uma avaliaç ao de desempenho de cadeias de blocos privadas permissionadas através de cargas de trabalho realısticas.

Pan, W., Coatrieux, G., Cuppens-Boulahia, N., Cuppens, F., and Roux, C. (2010). Medical image integrity control combining digital signature and lossless watermarking. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5939 LNCS:153–162.

Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*.

Shao, J., Lu, R., and Lin, X. (2015). Fine-grained data sharing in cloud computing for mobile devices. *Proceedings - IEEE INFOCOM*, 26:2677–2685.

Wüst, K. and Gervais, A. (2017). Do you need a blockchain? *IACR Cryptology ePrint Archive*, 2017:375.

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(10).

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proc. of International Congress on Big Data*, pages 557–564.