

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

Anselmo Battisti  
Gabriel Carrara

Universidade Federal Fluminense

Dezembro de 2018

- O Problema;
- Tecnologias, Conceitos;
- Soluções já Propostas;
- Nossa solução: Medichain;
- Avaliações e Resultados;
- Considerações finais.

- Mídias médicas são valiosas;
- Mídias médicas são constantemente compartilhadas entre produtores e consumidores;

O problema!

Como garantir integridade física e lógica deste ativo?

- **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.

- **Blockchain:** Distribuição dos dados através da rede par-a-par;
  - Imutabilidade e integridade dos dados presentes na cadeia;
  - Fácil disseminação dos dados;
  - Múltiplas replicas permitem recuperação das informações;

## Pseudo-anonimização

Informações relacionadas à endereços públicos ao invés de identidades.

- **Redes permissionadas:**

- Não há administração da rede;
- Qualquer pessoa pode fazer parte da rede;
- Usuários maliciosos podem acessar dados sensíveis;

- **Redes não permissionadas:**

- Rede possui administrador;
- Admissão de novos membros controlada por administrador;
- Possibilidade de identificar usuários pela chave pública.

- Plataforma para desenvolvimento de aplicações baseadas em *blockchain*;
- Permite criação de redes permissionadas;
- **Canais:** Nível adicional de isolamento dos dados;
  - Divisão da rede em partições menores;
  - Podem ser criadas por usuários;
  - Criadores possuem privilégios administrativos sobre seus canais;

- Uso de marca d'água invisível;
- Uso de blockchain:
  - Armazena a mídia dentro da *blockchain*;
  - Garante apenas integridade física.



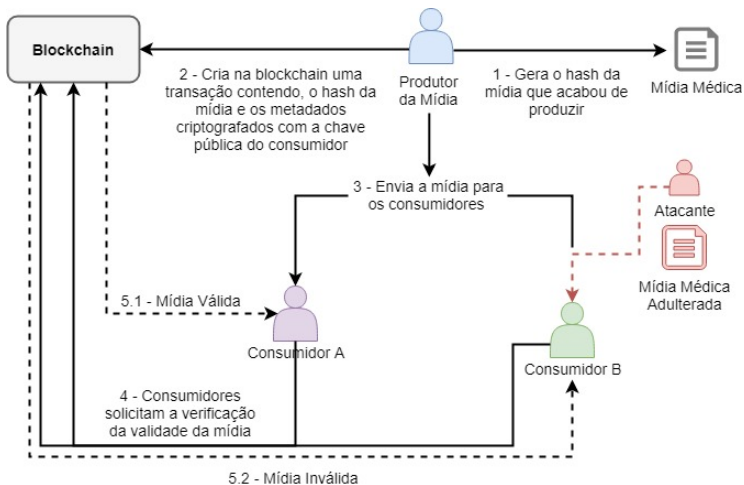


Figure 1: Modelo esquemático do *framework* MEDIACHAIN

- *Multichain*;
- Python;
- Clientes e servidores em ambiente Windows e Linux.

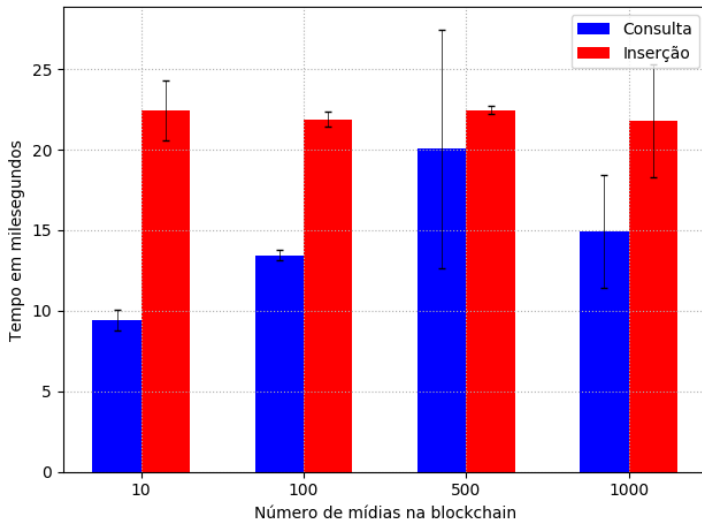


Figure 2: Relação entre o número de médias na *blockchain* e o tempo das

- A arquitetura prove validade física e lógica para mídias médicas;
- O tempo de inserção e consulta são aceitáveis, abaixo de 1 segundo;
- Uma mesma mídia não pode ser compartilhada para mais de um consumidor.