



Escalabilidade no contexto de Prontuário Eletrônico do Paciente baseado em Blockchain: Um Estudo Experimental sobre Armazenamento Off-chain

Pamella Soares (UECE - PPGCC), Allysson Allex Araújo (UFC - GESID),
Raphael Saraiva (UECE - PPGCC), Jerffeson Souza (UECE - PPGCC)



UNIVERSIDADE
ESTADUAL DO CEARÁ



Programa de Pós-Graduação
em Ciência da Computação



UNIVERSIDADE
FEDERAL DO CEARÁ



Agenda

- 1. Introdução**
- 2. Modelagem Arquitetural Preliminar**
- 3. Estudo Experimental**
- 4. Considerações Finais e Trabalhos Futuros**

01. Introdução

INTRODUÇÃO

PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)

É uma estrutura para manutenção da informação eletrônica sobre a saúde do indivíduo e os cuidados recebidos durante sua vida.

[Massad et al. 2003]

FINALIDADES

- ❖ Armazenamento
- ❖ Comunicação
- ❖ Garantir a continuidade do cuidado ao paciente
- ❖ Interoperabilidade
- ❖ Privacidade [Ricarte et al. 2017]

Lei Geral de Proteção de Dados

Prover acesso a dados sensíveis de modo seguro e que preserve a privacidade e anonimidade dos pacientes [da Conceição et al. 2018].

Massad, E., Marin, H. d. F., and Azevedo Neto, R. S. d. (2003). O prontuário eletrônico do paciente na assistência, informação e conhecimento médico. Pages 1-202
Ricarte, I. L. (2019). Sistemas nacionais de prontuários eletrônicos frente à privacidade de dados.*E-prints in library information science*. Disponível em:<http://eprints.rclis.org/33929/>.
da Conceição, A. F., da Silva, F. S. C., Rocha, V., Locoro, A., and Barguil, J. M. (2018). Eletronic health records using blockchain technology.*arXiv preprint arXiv:1804.10078*.

INTRODUÇÃO

BLOCKCHAIN

A tecnologia blockchain se demonstra promissora por sua viabilização de que **partes anônimas** e que **não confiam entre si** formem uma rede que armazena informações **confiáveis**, garantindo a **auditabilidade, disponibilidade e integridade** das transações armazenadas.

Um banco de dados distribuído, protegido por criptografia e governado por um mecanismo de consenso, ou seja, um registro de eventos transparente, seguro e resiliente.

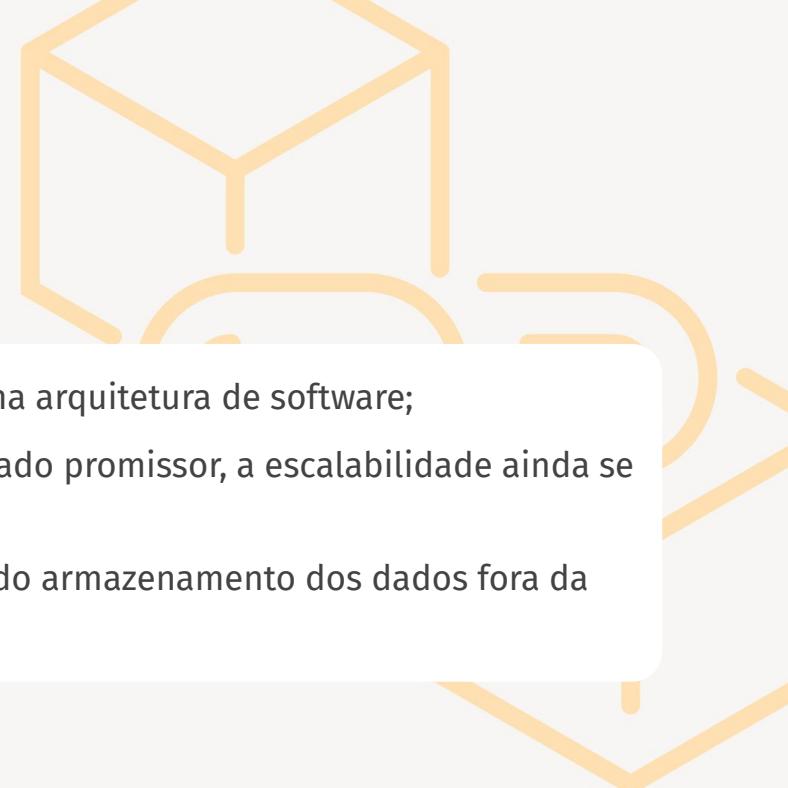
[Beck et al. 2017]

Contratos Inteligentes

INTRODUÇÃO

ESCALABILIDADE EM BLOCKCHAIN

- ❖ Escalabilidade é um atributo de qualidade essencial em uma arquitetura de software;
- ❖ Apesar do blockchain atrelado ao uso de PEPs ser considerado promissor, a escalabilidade ainda se demonstra um **desafio**;
- ❖ **Estratégias off-chain**, que está relacionada à terceirização do armazenamento dos dados fora da blockchain.



OBJETIVO



Como parte de um **estudo em desenvolvimento**, este artigo objetiva discutir um **estudo experimental**, a partir de uma **modelagem arquitetural preliminar**, o qual busca avaliar o uso de uma **estratégia off-chain** para lidar com o desafio da **escalabilidade** no contexto de PEP baseada em blockchain. Contribui-se, assim, ao discutir possíveis caminhos para **adoção de blockchain para PEP**, sendo estes importantes sistemas intensivos.

02. Modelagem Arquitetural Preliminar

ARQUITETURA DE SOFTWARE PRELIMINAR

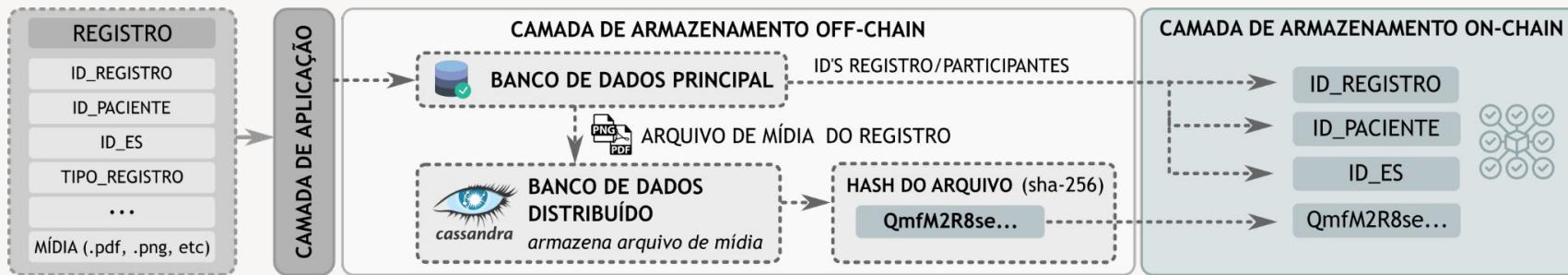


Realiza a comunicação entre as camadas e usuários.

Referente ao armazenamento de dados brutos em bancos de dados externos.

Referente aos dados adicionados dentro da blockchain:
Os ponteiros ou identificadores (IDs) e hash advindos dos registros nos bancos de dados que compõem a Camada de Armazenamento Off-chain.

ARQUITETURA DE SOFTWARE PRELIMINAR

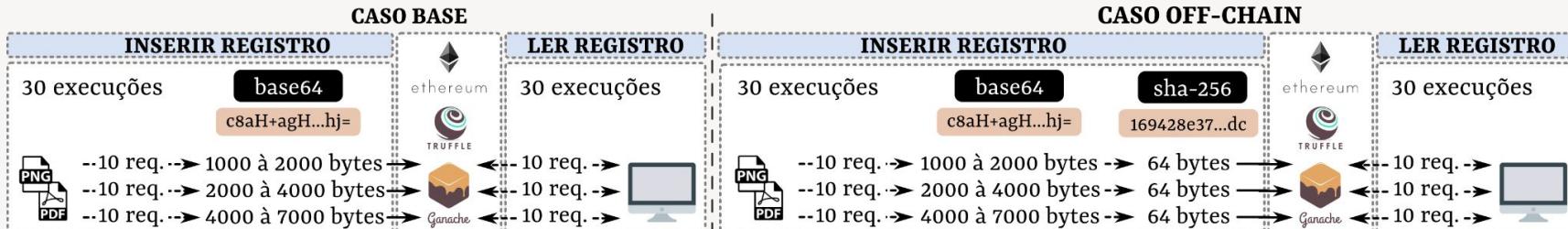


03. Estudo Experimental

AVALIAÇÃO DE DESEMPENHO

CONFIGURAÇÃO DO EXPERIMENTO COMPUTACIONAL

- ❖ Implementação da Prova de Conceito de um dApp;
 - ❖ Simulador de blockchain Ganache.
 - ❖ Testes aplicados sobre duas funções do contrato inteligente:
 - inserirRegistro;
 - lerRegistro.
 - ❖ Para fins de comparação foram criados dois tipos de casos:
 - Caso Base;
 - Caso Off-chain.
- ❖ Métricas analisadas:
 - Tempo de Publicação;
 - Tempo de Busca.
 - ❖ Testes estatísticos de Wilcoxon e Vargha-Delaney;



04. Resultados e Análises

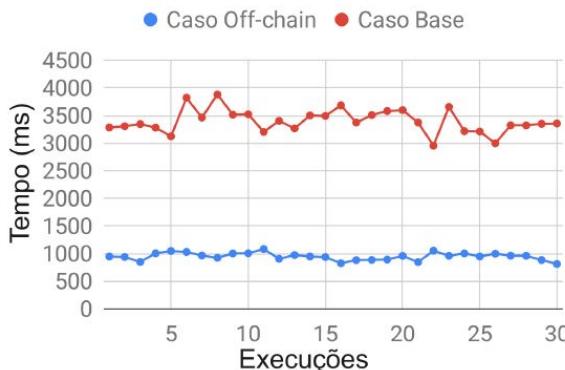
AVALIAÇÃO DE DESEMPENHO

RESULTADOS

TEMPO DE PUBLICAÇÃO

- Para todas as situações, existem evidências estatísticas que mostram que o tempo de publicação do Caso Base é显著mente maior que o do Caso Off-chain em 100% das execuções para todos os tamanhos de arquivos.

(a) Arquivos de tamanho entre 1KB à 2KB



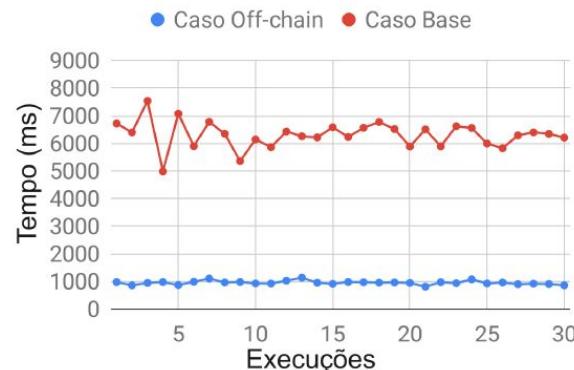
p-value (WC) = 4.5e-10

$\hat{A}_{12} = 0$

3397 ms

947 ms

(b) Arquivos de tamanho entre 2KB à 4KB



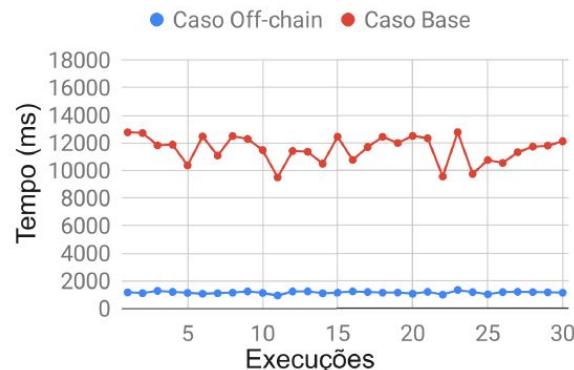
p-value (WC) = 4.5e-10

$\hat{A}_{12} = 0$

6307 ms

1133 ms

(c) Arquivos de tamanho entre 4KB à 7KB



p-value (WC) = 4.5e-10

$\hat{A}_{12} = 0$

11543 ms

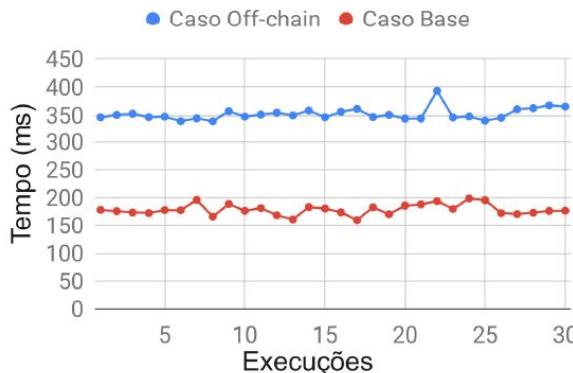
1141 ms

AVALIAÇÃO DE DESEMPENHO

RESULTADOS TEMPO DE BUSCA

- Nessas duas situações os casos são significativamente diferentes, com o Caso Off-chain tendo maiores valores de tempo de busca em 100% das execuções em relação ao Caso Base.
- Na Figura b, o Caso Off-chain obteve um tempo maior em 14% das execuções em relação ao Caso Base.

(a) Arquivos de tamanho entre 1KB à 2KB



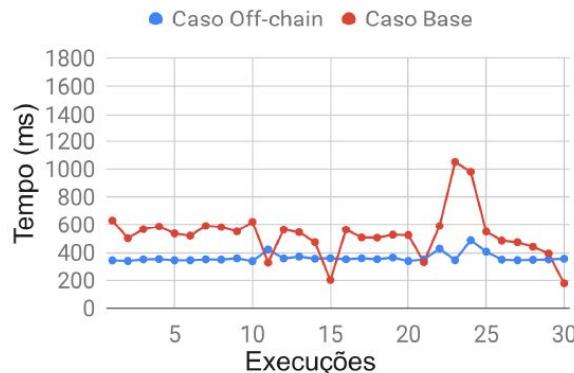
p-value (WC) = 4.4e-10

$\hat{A}_{12} = 1$

179 ms

352 ms

(b) Arquivos de tamanho entre 2KB à 4KB



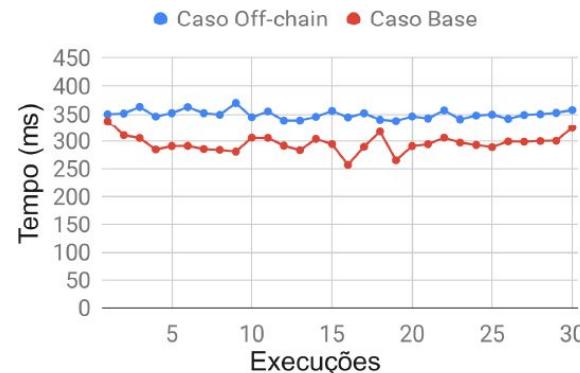
p-value (WC) = 3.0e-10

$\hat{A}_{12} = 0.14$

530 ms

362 ms

(c) Arquivos de tamanho entre 4KB à 7KB



p-value (WC) = 4.4e-10

$\hat{A}_{12} = 1$

296 ms

349 ms

05. Considerações Finais e Trabalhos Futuros

CONSIDERAÇÕES FINAIS

De maneira geral, os tempos de resposta das solicitações dos registros do paciente foram **reduzidos consideravelmente**. Dessa forma, concluiu-se que o uso de **estratégias de armazenamento off-chain** se demonstra proeminente para **lidar com o desafio da escalabilidade** no contexto de PEP.

TRABALHOS FUTUROS

- ❖ Evoluir este trabalho para uma modelagem de simulação detalhada considerando a construção de um modelo mais robusto;
- ❖ Configurar e validar uma modelagem computacional, inclusive, para facilitar a experimentação em situações extremas;
- ❖ Novos experimentos utilizando outras entradas e cenários mais complexos, além do uso de diferentes plataformas de blockchain.



Obrigada!

Dúvidas?

pamella.soares@aluno.uece.br



UNIVERSIDADE
ESTADUAL DO CEARÁ



Programa de Pós-Graduação
em Ciência da Computação



UNIVERSIDADE
FEDERAL DO CEARÁ

