ESTUDO DE ALGORITMOS DE CONSENSO NA PLATAFORMA HYPERLEDGER SAWTOOTH [1]

Gilson Sohn Junior [2], Maurício Aronne Pillon[3]

[1] Vinculado ao projeto "TÉCNICAS DE ESCALONAMENTO, PRECIFICAÇÃO E IMPACTO ENERGÉTICO EM PLATAFORMAS DISTRIBUÍDAS."
[2] Acadêmico (a) do Curso de Ciência da Computação – CCT – Bolsista PROBIC/UDESC.
[3] Orientador, Departamento de Ciência da Computação – CCT – mauricio.pillon@udesc.br

Desde a caracterização da tecnologia de *blockchain* no artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", publicado pelo pseudônimo Satoshi Nakamoto em 2008, pesquisas na área têm avançado englobando as mais diversas áreas, *i.e.*, financeira, educação, saúde e logística. Apoiada em conceitos clássicos de sistemas distribuídos e os livros razão distribuídos (*Distributed Ledger Technology* (DLT)), a *blockchain* destaca-se pelas características como imutabilidade, transparência, tolerância a falhas. Em parte, essas características são garantidas por algoritmos de consenso. Neste contexto, este trabalho de iniciação científica tem por objetivo o estudo de algoritmos de consenso na plataforma de desenvolvimento *HyperLedger.* A empresa *Hyperledger Foundation*, que possui uma ampla gama de produtos em projetos *open source,* foi a escolhida devido ao acesso facilitado as ferramentas. Dentre os produtos ofertados, os critérios de escolha foram: (i) aplicação de sistemas distribuídos; (ii) facilidade na instalação da plataforma e apoio dos desenvolvedores através de canais de comunicação e documentação; (iii) ênfase na importância de algoritmos de consenso.

O direcionamento do projeto, após a pesquisa inicial, foi pelo uso do *Hyperledger Sawtooth,* escolhido devido a sua maior aderência aos requisitos definidos. As etapas seguintes foram: (i) aprofundamento do estudo da plataforma e ambiente de instalação; (ii) identificação dos algoritmos de consenso disponíveis e suportados pelo ambiente; (iii) estudo e configuração da ferramenta com os algoritmos disponíveis e escolhidos; (iv) definição de benchmark para análise de desempenho da ferramenta; e (v) definição de ambiente de testes. A primeira abordagem foi o estudo do fluxo de mensagens das requisições entre os atores da plataforma *Sawtooth.* A metodologia utilizada foi a experimentação. Executou-se a rede *Sawtooth* em um ambiente conteinerizado, acoplou-se uma instância do *TCPDump* em cada um dos componentes, e monitorou-se a mensagens entre eles.

O resultado foi o diagrama de sequência ilustrado pela Figura 1. Pode-se observar que existem quatro atores, o cliente, a API, o validador e processador de transação. O cliente sempre inicia o ciclo com uma chamada de operação, através de uma conexão direta com a API. Ele pode receber três transações diferentes de respostas: sucesso, erro ou inválida. O erro pode ocorrer em função de um problema de assinatura ou de processamento. O ambiente pode ser escalado em pares, sempre associando um validador a um processador de transação. Este estudo possibilitou ao projeto criar e adequar um exemplo próprio de um contrato inteligente por meio da plataforma de estudo *Sawtooth*.

Como resultado do estudo dos algoritmos de consenso disponíveis e suportados na plataforma, identificou-se *o Practical Byzantine Fault Tolerance* (PBFT) *e Proof of Elapsed Time* (PoET). Embora alguns manuais indicassem o *RAFT Consensus Algorithm* como disponível para uso no *Sawtooth*, as versões mais recentes da plataforma não o suportavam. Com isso, o levantamento teórico de funcionamento ficou restrito a compreensão dos dois únicos algoritmos suportados atualmente. A configuração da ferramenta com os algoritmos suportados não foi trivial, mas foi

cumprida com sucesso. Atualmente, o ambiente experimental implantado no Laboratório LabP2D está operacional e conta com ambos os algoritmos de consenso.

A definição do *benchmark* seguiu as orientações da comunidade acadêmica, que indicava o *Hyperlegder Caliper* como a solução compatível com as ferramentas *Hyperledger.* O benchmark oferece várias métricas e atende o foco do projeto para análise de desempenho dos algoritmos de consenso junto a plataforma *Sawtooth*. O *Caliper* é genérico, porém tem forte vínculo de desenvolvimento com o *Hyperlegder Fabric*. O versionamento do *Caliper* e do *Sawtooth* não seguiram orientações de projetos sincronizadas e acabaram tomando rumos distintos nas escolhas de implementação. Com isso, acabaram, por ora, dessincronizados em suas versões, impossibilitando o uso conjunto. O estado atual do projeto tem uma plataforma operacional com dois algoritmos de consenso disponíveis, possui um ambiente de testes e um projeto de experimentos prontos, incrementando um número de validadores e processadores de transações, porém carece de adequações do *benchmark* para uso com o *Sawtooth*.

Os trabalhos futuros estão pautados na identificação de outro *benchmark* ou na definição de um conjunto sintético de transações que possibilitem a análise de desempenho dos algoritmos de consenso escolhidos. A médio prazo, pretende-se aplicar o projeto de experimentos ao ambiente de testes e coleta de resultados.

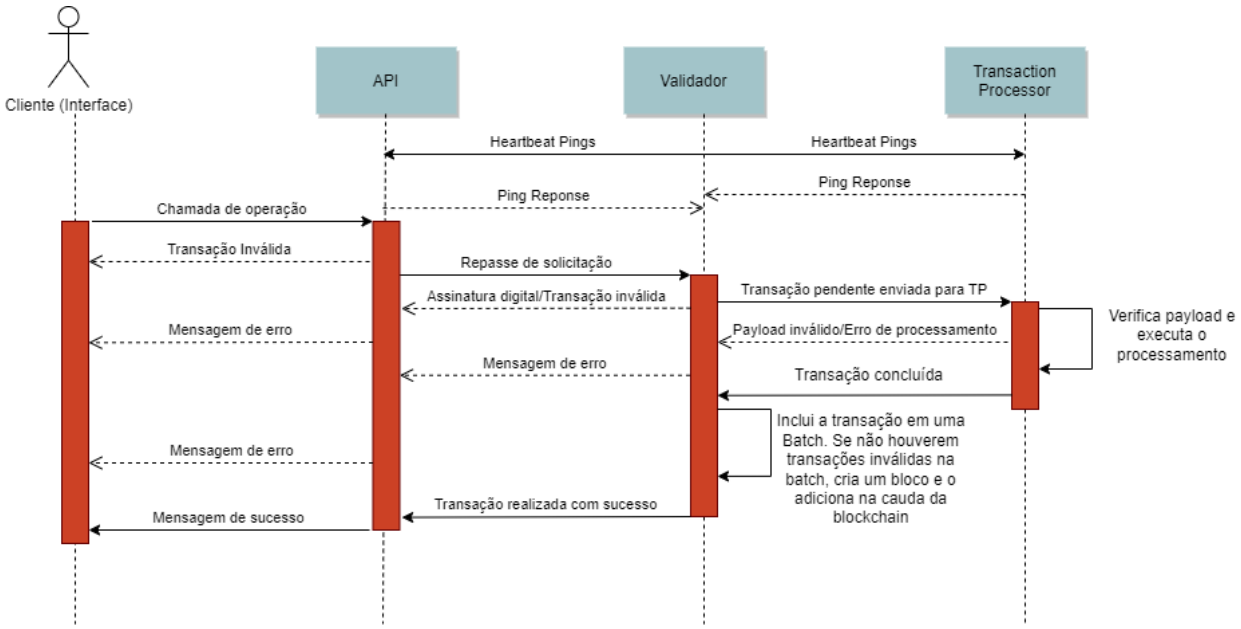

Figura 1. *Fluxo de uma requisição na rede Sawtooth.*

Palavras-chave: Sistemas distribuídos, Blockchain, algoritmos de consenso.