

Rumo à Avaliação do *Ethereum* e do *Hyperledger Fabric* com Dados Heterogêneos

Ana Caroline Fernandes Spengler¹, Paulo Sérgio Lopes de Souza¹

¹Instituto de Ciências Matemática e de Computação – Universidade de São Paulo (USP)
Avenida Trabalhador São-carlene, 400 – 13566-590 – São Carlos - SP – Brazil

{ana.spengler}@usp.br, {pssouza}@icmc.usp.br

Abstract. *Blockchain was originated with Bitcoin's creation, presenting itself as an infrastructure for distributed storage of financial transactions with guaranteed immutability. Due to its characteristics, blockchain began being used by other applications that can benefit from this infrastructure. These applications present different demands from those focused in financial transactions, such as manipulation of different types of data and information privacy. The aim of this ongoing project is to verify the performance of the blockchain when used on applications that demand heterogeneous data.*

Resumo. *Blockchain nasceu com o surgimento do Bitcoin, apresentando-se como uma infraestrutura para o armazenamento distribuído de transações financeiras com garantia de imutabilidade. Pelas suas características, o blockchain passou a ser utilizado por outras aplicações que podem se beneficiar dessa infraestrutura. Essas aplicações apresentam demandas distintas daquelas focadas em transações financeiras, como manipulação de diferentes tipos de dados e privacidade das informações. O objetivo deste projeto em andamento é verificar o desempenho do blockchain quando utilizado aplicações que demandam dados heterogêneos.*

1. Introdução

O *Bitcoin* foi lançado em 2009 com o objetivo eliminar a centralidade que instituições bancárias e governamentais representam sobre as transações financeiras. A grande inovação desta tecnologia é oferecer uma solução que dispensa esse terceiro elemento centralizador, propondo uma nova maneira distribuída de se operar tais transações [Nakamoto 2009]. A estrutura, utilizada pelo *Bitcoin*, na qual as transações são armazenadas é chamada de *blockchain*. É através desta estrutura que há a garantia de imutabilidade de registros. Essa maneira de armazenar os dados é um dos principais subprodutos do lançamento do *Bitcoin*.

Além do setor financeiro, como o *Bitcoin*, o *blockchain* tem um grande potencial para ser aplicado também na área médica. A necessidade de mecanismos para gerenciar um grande volume de dados, que demandam privacidade e fácil acesso, torna o *blockchain* uma solução atrativa. Com o *blockchain* é possível criar aplicações que além de garantir o compartilhamento de dados entre as diferentes instituições médicas, também seja possível certificar privacidade e segurança dos dados, essenciais para essa finalidade [Shae and Tsai 2017].

Há também iniciativas na área da educação que utilizam *blockchain*. Os autores do artigo [Palma et al. 2019] propõem o uso do *blockchain* para a digitalização de certificados e notas do ensino superior no Brasil. O objetivo deste trabalho é diminuir o número de certificações falsas no intuito de garantir que o documento foi emitido por instituições de ensino. Somado a isso, o *blockchain* oferece a imutabilidade dos dados, de forma que, instituições e alunos possam ter acesso as informações de maneira paralela e segura.

O objetivo geral deste projeto em andamento é avaliar o uso de *blockchain* sob demanda de dados heterogêneos de aplicações distintas àquelas do mercado financeiro, como *Bitcoin*, por exemplo. Dessa forma, deseja-se avaliar essa infraestrutura quando utilizada em contextos diferentes do financeiro, como por exemplo a área da saúde, na qual os dados apresentam demandas específicas, como privacidade e também heterogeneidade de dados, variando, por exemplo, de ficha de pacientes a imagens de alta resolução.

2. Blockchain

O *blockchain* recebe esse nome pelo modo como os registros são mantidos: uma sequência de blocos ligados em forma de cadeia. O bloco consiste da estrutura básica do *blockchain*, onde as transações são armazenadas. O *blockchain* mantém os registros de todas as transações desde o primeiro bloco a criado, o *genesis block*, até o mais recente adicionado na cadeia. Essa sequência de blocos está espalhada em uma rede distribuída *Peer-to-Peer (P2P)*, de forma que maioria, potencialmente todos, os participantes têm uma cópia local da cadeia [Swan 2015].

O processo de criação de um bloco é denominado mineração, sendo o mecanismo pelo qual os registros são validados. Esse nome é dado pelo processo se assemelhar ao modo como outros produtos de valor, como ouro, são extraídos, devido ao esforço dedicado nesse trabalho. No caso do *Bitcoin*, esse processo também é responsável pela criação de novas moedas [Narayanan et al. 2016].

3. Plataformas de Desenvolvimento

Este projeto prevê a utilização de plataformas como por exemplo o *Ethereum* e o *Hyperledger* [Buterin 2014, Dhillon et al. 2017]. Ambos são considerados plataformas consolidadas com robustez e alta aceitação na comunidade acadêmica e comercial.

O *Ethereum* é uma plataforma *Open-Source* para aplicações distribuídas em um ambiente seguro e descentralizado. Seu objetivo é abstrair a complexidade da infraestrutura do *blockchain* para tornar mais simples o desenvolvimento de aplicações *blockchain*. O *Ethereum* provê um ambiente de programação que permite o desenvolvimento de aplicações sob o conceito de contrato, que é uma estrutura utilizada para representar regras para transferência de posses, transações e possíveis estados de um objeto [Buterin 2014]. Os *smart-contracts* são a estrutura básica do *Ethereum*. Eles representam uma entidade do mundo real, descrevendo funcionalidades e possíveis estados que o objeto assume. Desta forma, em poucas linhas de código, pode-se criar uma aplicação na plataforma [Buterin 2014].

O *Hyperledger* pode ser definido como um esforço colaborativo *Open-Source* para promover o *blockchain* em vários setores da tecnologia. A partir desta defini-

ção, a proposta é que o *Hyperledger*, em vez de ser uma única plataforma, como o *Ethereum*, tenha vários projetos sobre sua tutela. Nestes termos, o *hyperledger* visa prover uma interface de programação (API) para aplicações *blockchain* que permita fácil desenvolvimento de aplicações que atendam requisitos de interoperabilidade, escalabilidade e disponibilidade [Dhillon et al. 2017].

Em relação ao *Hyperledger*, o foco deste trabalho está no *Hyperledger Fabric*. Essa implementação fornece uma estrutura para o desenvolvimento de soluções *blockchain* com uma arquitetura modular. Assim, diferentes componentes do *blockchain* podem ser modificados sem alterar a funcionalidade de outras partes da infraestrutura. O *Hyperledger Fabric* tem duas entidades que lidam com a lógica de processamento das transações: o *smart-contract* e o *chaincode*. Esses termos podem ser usados de forma intercambiável, pois juntos controlam a organização das transações. Dentro do *Hyperledger Fabric*, os *smart-contracts* definem a lógica de execução que é responsável por inserir os dados na cadeia. O *chaincode* é usado por administradores da rede para agrupar *smart-contracts* com a mesma finalidade e implementar a lógica de execução definida por eles [Cachin 2016].

4. Trabalhos Relacionados e Estágio Atual do Desenvolvimento

No atual estágio do desenvolvimento deste projeto foi realizado um levantamento da literatura, onde foram encontrados 26 estudos, dos quais destacam-se dois artigos que descrevem o uso de *benchmarks* para a avaliação do blockchain [Dinh et al. 2017, Baliga et al. 2018]. Na primeira publicação o objetivo é desenvolver uma ferramenta, denominada *BlockBench*, para comparar as diferentes plataformas blockchain, focado nas plataformas *Hyperledger Fabric*, *Ethereum* e *Parity* (uma implementação do *Ethereum*) [Dinh et al. 2017]. Nesse estudo, o desempenho das diferentes plataformas é medido em termos de vazão, latência, escalabilidade e tolerância a falhas. No segundo artigo, [Baliga et al. 2018] a avaliação é centrada no desempenho do *Hyperledger Fabric*, em função da vazão e latência do sistema. Adicionalmente, os autores avaliam o impacto de modificações em funcionalidades da plataforma no desempenho da mesma. O *benchmark Hyperledger Caliper* é utilizado para gerar a carga de trabalho nesse artigo.

Após o estudo dos trabalhos relacionados, o projeto foi direcionado para a reprodução dos *benchmarks* propostos nos artigos citados anteriormente. Inicialmente foram analisadas as características, parâmetros e cenários considerados na execução dos experimentos.

Em um segundo momento, a rede na qual o artigo [Baliga et al. 2018] realizou os seus testes foi replicada, utilizando a infraestrutura do *Hyperledger Fabric* em sua versão mais atual (v2.0). Para reproduzir tais experimentos, também está sendo necessário recriar a carga de trabalho com o *Hyperledger Caliper*, atividade que atualmente está em desenvolvimento. Os experimentos previstos neste projeto utilizarão uma carga de trabalho com dados heterogêneos sobre as plataformas citadas, verificando o comportamento das métricas vazão, latência, escalabilidade e tolerância a falhas.

5. Conclusão

Embora este projeto ainda esteja no início de seu desenvolvimento, já é possível elencar alguns desafios encontrados no contexto de sua implementação. A principal dificuldade identificada é derivada da escassez de documentação sobre as plataformas. Ainda que existam tutoriais e materiais oficiais descrevendo as ferramentas estudadas, a ausência de maior detalhamento técnico e exemplos práticos acaba sendo prejudicial para a instalação e execução do *Fabric*. Sendo assim, quando algum erro de execução é encontrado, tem-se um dificuldade em superá-lo. Outro problema encontrado é que as referências não oficiais sobre o *Hyperledger Fabric*, como fóruns, abordam versões anteriores da ferramenta. Além disso, os *benchmarks* propostos pelo trabalho [Baliga et al. 2018] utilizam de uma versão anterior do *Hyperledger Fabric*, desse modo é necessário atualizar os algoritmos em função das novas estruturas introduzidas pela versão 2.0 da plataforma.

Os próximos passos no projeto focam na finalização da replicação dos experimentos para compreender as características dos mesmos. Esse conhecimento será base para a implementação proposta, a qual terá como base em base de dados médicas, considerando sua natureza heterogênea.

Referências

- Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., and Chatterjee, S. (2018). Performance characterization of hyperledger fabric. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 65–74.
- Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform. Acessado em 02/07/2019, às 19:17.
- Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, volume 310.
- Dhillon, V., Metcalf, D., and Hooper, M. (2017). The hyperledger project. In *Blockchain enabled applications*, pages 139–149. Springer.
- Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., and Tan, K.-L. (2017). Blockbench: A framework for analyzing private blockchains. In *2017 ACM Int. Conf. Management of Data, SIGMOD '17*, pages 1085–1100. ACM.
- Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Acessado em 02/07/2019, às 19:17.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, Princeton, NJ, USA.
- Palma, L., Vigil, M., Pereira, F., and Martina, J. (2019). Blockchain and smart contracts for higher education registry in brazil. *IJNM*, page e2061.
- Shae, Z. and Tsai, J. J. P. (2017). On the design of a blockchain platform for clinical trial and precision medicine. In *IEEE 37th ICDCS*, pages 1972–1980.
- Swan, M. (2015). *Blockchain : blueprint for a new economy*. O'Reilly Media, Sebastopol, Calif.