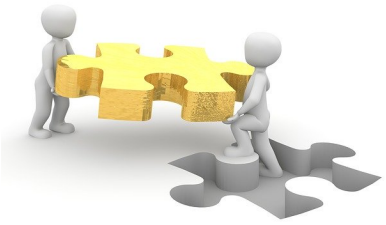
Technical University of Munich

Thesis B.Sc. | Thesis M.Sc. | IDP, Guided Research

Performance of BFT Consensus

Motivation

State-machine-replication (SMR) is used to build fault-tolerant systems such as airplanes, cars, and industrial control systems. SMR consists of multiple machines (replicas), which agree on a common value even in case of faulty behaviour of single machines.
In SMR, there are two main fault models, namely crash-fault-tolerance (CFT) and byzantine-fault-tolerance (BFT). For CFT, a replica runs as specified or it crashes. In BFT, a replica may behave arbitrarily (send wrong values/messages).



In this thesis, we will analyse the performance of two BFT protocols: HotStuff [1] and its variant LibraBFT [2] as used in Facebook's cryptocurrency Libra. First, we want to explore their conceptual commonalities and differences. With a solid understanding, you will compare the implementations especially with respect to their communication behaviour. Then, you will analyse the performance of the two protocols.

Your Tasks

- Familiarize yourself with HotStuff and LibraBFT
- Analyze their conceptual commonalities and differences
- Compare the implementations
- Do performance comparisons between the implementations
- Evaluate the results

References

[1] Yin, Maofan, et al. "Hotstuff: Bft consensus with linearity and responsiveness." Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. 2019.
[2] Baudet, Mathieu, et al. "State machine replication in the Libra Blockchain." (2019).

Contact

Johannes Schleger schleger@net.in.tum.de
Richard von Seck seck@net.in.tum.de
Dr. Holger Kinkelin kinkelin@net.in.tum.de