Byzantine Agreement: From Theory to Practice

A distributed system consists of \( n \) nodes. The system is byzantine fault tolerant (BFT) if it can tolerate at most \( f < \frac{n}{3} \) arbitrarily malicious (byzantine) nodes. BFT protocols have been studied in great detail since many decades, both in theory and practice. Nowadays, BFT protocols are the key to building “permissioned blockchains”, an area traditionally known as “state machine replication” [9, 10].

In practice, BFT protocols have many applications ranging from online shopping to credit card transactions, cryptocurrencies and stock market trades; whenever a set of clients makes concurrent requests for (or with) limited resources, the service providers have an interest to both prevent fraudulent and tolerate faulty behaviour in the system.

From a research perspective, the interest in BFT systems has first been reignited by Castro and Liskov when they presented their “Practical” BFT (PBFT) system [2]. After PBFT, a large number of other BFT systems emerged [8, 11, 5, 12, 13, 1, 7, 3, 4, 6].

At our group we have developed a new BFT protocol that inverts the process of previous BFT protocols, achieving a better bound for transaction commit delay theoretically. However, it is not always straightforward how to get from theory to practice. In this project, we aim to overcome the challenges that arise in real-world systems as you will implement a BFT library based on our initial proposal (and a simple simulation environment for testing).

Requirements: An interest in algorithmic problems is required. Programming experience in python is a great advantage. For this project, the student(s) should be able to solve basic implementation problems independently, while we discuss solutions / new ideas for upcoming problems in weekly meetings!

Interested? Please contact us for more details!

Contacts

- Roland Schmid: roschmi@ethz.ch, ETZ G94
References


