



BA/SA:

## Improving Asynchronous Byzantine Agreement

Consensus is one of the most fundamental problems in distributed computing; an informal description is as follows: A set of  $n$  nodes start with an individual value, and from that starting point they need to agree on a single value. If there are no failures, Consensus can be solved easily, and even for crash failures there are many known results.

The byzantine agreement (BA) problem has the same requirements as Consensus, however, the system must tolerate up to  $t$  byzantine nodes. Byzantine nodes are malicious and can behave arbitrarily. For fault-tolerant systems, an efficient solution to BA would be essential.

Most algorithms for BA are for the synchronous model. However, in practice, the asynchronous model is capturing reality often a lot better. Your task is therefore to develop a new algorithm for asynchronous BA. We already started to work on this subject, and realized that the difficulty of this problem requires some deeper insight into distributed systems in general. We started with a different approach of modeling distributed systems, similar to finite state machines, which can serve as a starting point for your work.



**Interested?** If you are interested in developing better algorithms and/or improving the representation technique of algorithms in distributed computing, we are happy to hear from you and to have a small chat.

### Requirements:

- Interest in theory of computer science.

### Contacts

- Darya Melnyk: [darya.melnyk@tik.ee.ethz.ch](mailto:darya.melnyk@tik.ee.ethz.ch), ETZ G93