Toward an Optimal Consensus Protocol for Private Blockchains

In many fields, managing information securily is one of the main concerns because of data sensitivity, privacy and confidentiality. Centralized data storage is often risky and decentralized systems are the most used. In this context, Blockchain is an emerging technology that enables secure data storage in a distributed and decentralized way. When the participants should be authenticated before joining the blockchain, public blockchains like Bitcoin and Ethereum are not suitable. Private Blockchains, on the other hand, allow collaborators to manage information internally.

In Blockchain, data is added to the database once the majority of nodes agree on it. Therefore, consensus protocols are a central concern in this technology. Practical Byzantine Fault Tolerance (PBFT) is the most widely used protocol. However, it suffers from poor scalability because of the large amount of data exchanged.

In this thesis, we try to optimize this protocol in order to achieve better scalability, fewer messages loading the network and faster response delays without comprimising its security.