

# Optimal Byzantine Fault Tolerance Consensus Algorithm for permissioned systems

*Friday 5 November 2021 15:00 (20 minutes)*

In this paper, we propose the “Optimal Byzantine Fault Tolerance” consensus algorithm for permissioned replicated distributed systems with Byzantine fault tolerance. It seems to achieve total fairness, in the sense that it is impossible for an attacker to manipulate which of two transactions will be chosen to be first in the consensus order. It has asynchrony, no leaders, no round robin and no Proof-of-Work. A main characteristic for this algorithm is the digital signatures and broadcast usage to record network activity. The consensus participants inform everyone else about the set of accepted or rejected transactions in a time frame. As to the ordering of transactions, three mechanisms have been proposed: computer clocks, lexicographical order for message hashes and the semantic order given by the versioned data, manipulated inside transactions. Considering these traits, we can say the algorithm yields fair Byzantine agreement and a total order for all transactions, with very little communication overhead beyond the transactions themselves.

**Authors:** Prof. ALBOAIE, Lenuța (Faculty of Computer Science, University of Alexandru Ioan Cuza); Dr ALBOAIE, Sinică (Faculty of Computer Science, University of Alexandru Ioan Cuza); Mrs CALANCEA, Cristina Georgiana (University Alexandru Ioan Cuza Iasi, Romania)

**Presenter:** Mrs CALANCEA, Cristina Georgiana (University Alexandru Ioan Cuza Iasi, Romania)

**Session Classification:** Open Distance Learning && Technologies for Future Internet

**Track Classification:** Technologies for Future Internet