Fast Probabilistic Consensus (FPC)

Return to Consensus Mechanism

Fast Probabilistic Consensus (FPC) is a leaderless protocol within Byzantine Infrastructures with low communicational complexity and which allows a set of nodes to come to a consensus on a value of a single bit. It makes the assumption that part of the nodes are Byzantine, and are thus controlled by an adversary who intends to either delay the consensus or break it (this defines that at least a couple of honest nodes come to different conclusions). The protocol works with high probability when its parameters are suitably chosen. This protocol could be applied to reaching consensus in decentralized cryptocurrency systems. A special feature of it is that it makes use of a sequence of random numbers which are either provided by a trusted source or generated by the nodes themselves using some decentralized random number generating protocol. This increases the overall trustworthiness of the infrastructure.[1)]

1)

Serguei Popov, William J. Buchanan; Cornell University, Computer Science, Distributed, Parallel and Cluster Computing; FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures; 26 May 20219; Accessed: 15 July 2021; https://arxiv.org/abs/1905.10895