On Scalability and Performance of Permissioned Blockchain Systems

Chrysoula Stathakopoulou
IBM Research – ETH Zurich

Problem
State of the art consensus protocols do not correspond to the requirements of permissioned blockchain setups.

Motivation
Smart Contracts have attracted considerable interest into blockchain as a future enterprise platform.

Approach
Fast, secure, scalable, reconfigurable, incentive compatible consensus.

Expected Impact
Enabling new use cases via sustainable blockchain systems.

Permissioned Blockchain Properties
✔ Access control → No Sybil attacks
✔ Known number of participants

Requirements
➢ High throughput
➢ Low latency
➢ Scalability to > 1000 nodes
➢ Final consensus

Salability & Performance

State of the Art

From Byzantine Fault Tolerance to Rational Players

Traditional Machine State Replication
➢ Up to k out of n replicas are expected to behave arbitrarily

Enterprise Blockchain Ecosystem
➢ Nodes in different organizations
➢ Possibly conflicting interests
➢ Each participant has an operating cost
➢ Participants/organizations try to maximize their utility

Rational participants who must be incentivized to participate and follow the protocol

Decoupling Ordering form Execution

A Public Ordering Service for Permissioned Blockchains
➢ Scalability
➢ Reconfiguration
➢ Incentive Compatibility