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

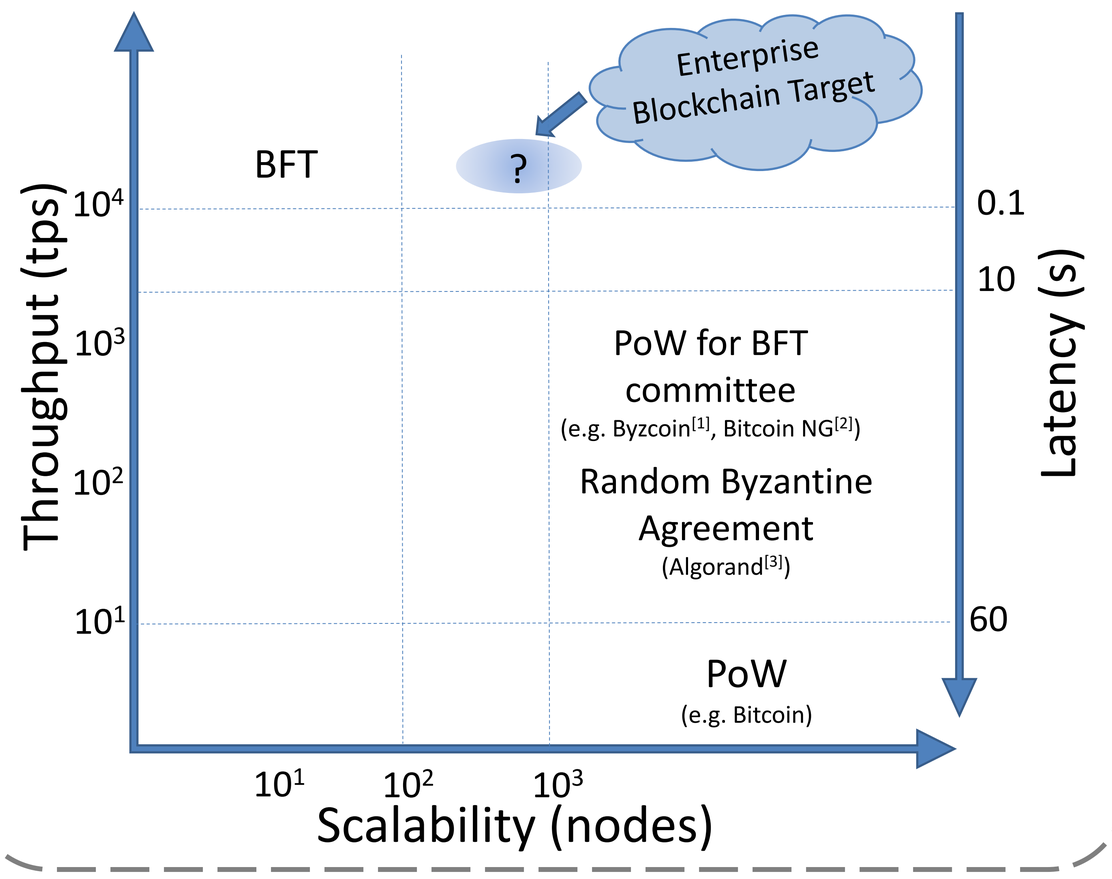
Properties

- ✓ 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

	Proof of Work	Proof of Stake	Byzantine Fault Tolerance
Scalability	☺	☺	☹
Latency	☹	☹	☺
Throughput	☹	☹	☺
Energy Sustainability	☹	☺	☺
Consensus Finality	☹	☹	☺

From Byzantine Fault Tolerance to Rational Players

Traditional Machine State Replication

- ➢ Up to k out of n replicas are expected to behave arbitrarily

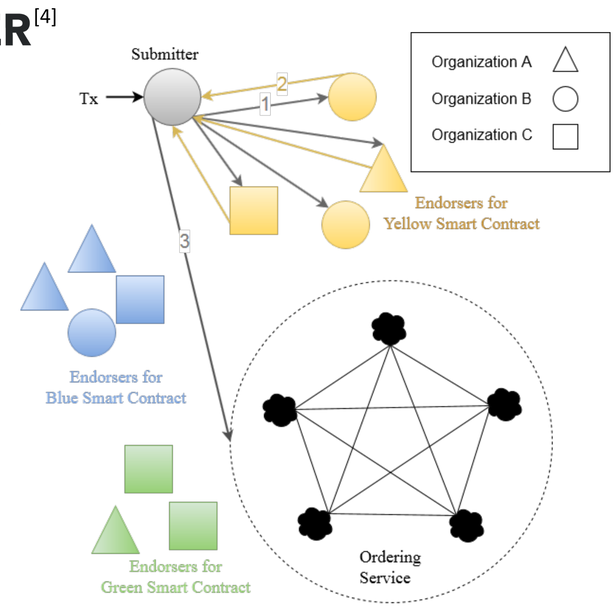
Enterprise Blockchain Ecosystem

- ➢ 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

HYPERLEDGER[4] FABRIC

Decoupling Ordering form Execution



towards

A Public Ordering Service for Permissioned Blockchains

- ➢ Scalability
- ➢ Reconfiguration
- ➢ Incentive Compatibility

[1] Kogias, Eleftherios Kokoris, et al. "Enhancing bitcoin security and performance with strong consistency via collective signing." *25th USENIX Security Symposium (USENIX Security 16)*. 2016.
[2] Eyal, Ittay, et al. "Bitcoin-NG: A Scalable Blockchain Protocol." *NSDI*. 2016.
[3] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.
[4] Androulaki, Elli, et al. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." In *EuroSys 2018: Thirteenth EuroSys Conference.* ACM, 2018.