**Bloxy: Providing Transparent and Generic BFT-Based Ordering Services for Blockchains**

Symposium on Reliable Distributed Systems 2019
Signe Rüssch, Kai Bleeke, Rüdiger Kapitza. TU Braunschweig, Germany.
{ruesch|bleeke|kapitza}@ibr.cs.tu-bs.de

**Motivation**

- Byzantine fault tolerant protocols (BFT):
  - Consensus despite arbitrary behaviour
  - Block creation for blockchains
  - Optimized for different aspects
- Permissioned blockchains: several use cases
- Different use cases have different requirements
  - No one-size-fits-all BFT solution!
  - Generic consensus protocols for blockchains!

**Hyperledger Fabric** [Andreouakis et al., EuroSys’18]

- Permissioned blockchain platform
- Modular design with pluggable consensus
- BFT-SMaRt integration [Rossi et al., DSN’18]
  - "Frontend": Fabric orderer now part of peers
  - BFT client functions compromise modularity
  - Re-implementation for all protocols needed
  - Shift BFT client functionality onto replicas to maintain Fabric’s modularity!

**Bloxy: A Blockchain-Aware Trusted Proxy**

- Consensus proxy for Fabric encapsulates BFT client functionality
- Transparent access to a generic ordering service
- Leverage trusted execution for trusted operations on replicas
  - Hybrid fault model: subsystem can only fail by crashing
- Proof-of-concept integration of BFT protocols:
  - Hybrid protocol Hybster [Beli et al., EuroSys’17]
  - Conventional protocol PBFT [Castro et al., OSDI’99]
- Bloxy functionality:
  - Establishing secure connections
  - Forwarding transactions as BFT requests
  - Majority voting
  - Block dissemination

**Evaluation**

Microbenchmarks of ordering service:
- Lower communication overhead of Bloxy-integrated BFT protocols
- Improved latency and throughput
  - Generic consensus at no performance cost!

Macrobenchmarks of Fabric network:
- Evaluated using Hyperledger Caliper
  - Ordering Service has no noticeable effect on Fabric’s performance

**Block Storage**

- Ensure all peers have all blocks in correct order
- Short-Term Block Storage on replicas
  - Store a block until $f + 1$ orderers received it
  - Orderers can query for missing blocks
  - Tolerate Byzantine orderer nodes

**Conclusion**

- Consensus proxy for Hyperledger Fabric
- Encapsulation of BFT client functionality
- Easy integration of new consensus protocols
- Bloxy maintains Fabric’s modularity
- Good performance compared to directly integrated BFT protocols