High-Performance Consensus Mechanisms for Blockchains

Problem Statement
- Transaction ordering based on Proof-of-Work wastes computational power and energy
- Expensive and ecologically harmful: Bitcoin has higher energy demand than Israel!
- BFT protocols considered the solution, but only limited scalability for number of participants

Basics: Blockchains & BFT
- Permissioned blockchains: authenticated participants, e.g. Hyperledger Fabric
- Permissionless blockchains: no regulation on participants, e.g. Bitcoin
- Byzantine Fault Tolerance (BFT): reach consensus with $3f + 1$ nodes even if $f$ nodes behave arbitrarily faulty

Scalable BFT Ordering for Permissioned Blockchains
- Hyperledger Fabric: permissioned blockchain with modular consensus
  - BFT ordering service based on Hybster [Behl et al., EuroSys’17]
  - Hybrid BFT protocol: only $2f + 1$ nodes to tolerate $f$ faults
  - Trusted subsystem based on Intel SGX
  - Designed for high scalability
- Blockchain-aware Trusted Proxy (Bloxy)
  - Based on Troxy [Li et al., DSN’18]
  - Transparent access to BFT cluster
  - Shift BFT reply voting to SGX enclaves on replicas
  - Disseminate created blocks to all connected peers

Advantages:
- Drastically reduced message complexity
- Smooth integration: no modification to Fabric
- SGX-based voting: offloading to replicas, no trust in orderer needed

Remote Direct Memory Access (RDMA)
- BFT protocols incur higher latencies than crash-tolerant protocols
  - Limits adoption of BFT
- RDMA: hardware-based protocol offloading technology in data centers
  - Direct data movement between memory of remote hosts
  - No OS and CPU involvement or intermediate copies as with TCP
  - Low latency

Future Work
- Scalable BFT for permissionless blockchains
- Often thousands of participants → BFT protocol scalability not well-explored for such numbers
- Investigate mechanisms such as threshold cryptography, ring communication, choosing random committees, ...