Summary of Session 3: Sharding in Blockchain

Jay Lala

Session Chair

Summary of 1st Presentation: "A simple recipe for scaling Byznatine fault tolerant systems" by Fernando Pedone, USI, Switzerland

- Fernando began by making the disclaimer that the talk isn't about scaling blockchain.
  - However, scaling of BFT systems may be applicable to permissioned blockchains, but not likely for permissionless blockchains.
  - There was no clear conclusion after discussion as to why the latter is so.
- What's common between BFT and Blockchains?
  - Users have expectations of scalability, availability, and security in the presence of malicious participants.
- Specific problem addressed is strong consistency and order commands in a sharded and replicated system.
- The presentation went into details of BFT atomic multicast protocols, starting with naïve protocols and their deficiencies, and then proposing ByzCast which is a compromise between reusability and scalability.
  - Perf comparison of ByzCast with naïve protocol in LAN and WAN environments was discussed.
- Fernando concluded with a discussion of the overlay trees.

Summary of 2nd Presentation: "Fast Transaction Commit in Sharded Data Stores and Blockchains" by Gregory Chokler, U of London

- Gregory began by summarizing the state of blockchain technologies:
  - Transactional semantics and fault tolerance are non-negotiable, proof-of-work is slow, and committee consensus is fast but bandwidth-bound.
  - One way to scale blockchains is to scale the committee – but, how?
- He addressed the specific problem of fast transactions for sharded, replicated data store, with following requirements:
  - How to commit a transaction touching objects in multiple shards, ACID guarantees, and reliable shards, at least to begin with.
  - He then introduced a unified framework that combines both 2-phase commit and concurrency control
- Next problem addressed was implementation of a resilient Transaction Service (TCS) under a.) crash fault, and b.) Byzantine fault conditions
  - This is the formal framework for multi-shot transaction commit.
  - Both protocols were described in great detail and latency compared to Black-Box protocols.
- How these TCS BFT protocols can be applied for blockchain scaling is left for future work.