Session Summary

Performance and Scalability Aspects of Blockchain

Session Summary

- Problem: improving performance of blockchain
  - Still unsolved
  - But great progress are being made
- A blockchain system
  - **Consensus**
  - **And other stuff**
- Two insightful talks:
  - Roy Friedman:
    - Coloring Smart Contracts and Other Musings About Efficient Blockchain Execution
  - Qiang Tang:
    - Dumbo Protocols: Making Asynchronous Consensus Real

Improving Consensus

- 1st gen: PoW -> PBFT
- HotStuff and variants:
  - Better communication complexity
- Some notable optimization:
  - Network level: decoupling consensus vs. non-consensus messages
  - Rotating leaders
  - Sharding (local vs. geo-replicated setting)

Improving Consensus

- Asynchronous consensus: overcoming the FL Impossibility result
        - Live and safety in fully asynchronous network
        - But, probabilistic
- Dumbo family of asynchronous consensus:
    - HoneyBadger:
        - Use reliable broadcast to send message to everyone
        - Bottleneck: Binary Byzantine agreement protocol
    - Dumbo2:
        - Binary -> Multi-value Byzantine agreement
        - Demonstrate the significant of MVBA
        - Still quite expensive
    - Bolt-Dumbo-Transformer: optimistic
        - Good days: run deterministic BFT
        - Bad days (lots of complaints) -> switch
        - Performance comparable to BFT

Other stuffs

- Consensus getting too good
  - Now bottleneck is elsewhere
    - Storage
    - Verification
    - Network round trips
- Systems level optimizations:
  - FastFabric
  - Redbelly
- Concurrent transactions:
  - Main challenges: all nodes have the same concurrency schedule
  - DAG based
  - Coloring: extract set of concurrent tx from colored dependency graph

Key takeaways

- Lots of progress in consensus, driven by blockchain
- Asynchronous consensus:
  - May not be too complex to understand
- How to close the gap to the consensus limit
- Techniques from systems/databases communities are powerful