Session 1: Dependability and Security Aspects for Blockchain Consensus

Andrea Bondavalli

Introduction to Blockchain Security and Dependability Challenges: a viewpoint.

(Jiangshan Yu, University of Luxembourg, LU)

Blockchain Consensus Protocols: an Outlook

(Marko Vukolić, IBM Research Zurich, Switzerland)

Introduction to Blockchain Security and Dependability Challenges: a viewpoint.

- Jiangshan gave an overview of the basic concepts of blockchains: Goals, Architecture and threats: DOUBLE SPENDING
- Challenges: **Security**, **Privacy**, **Consensus**, **and Scalability**
- CHALLENGE 1
- Gap between BFT and blockchains → PoW
- 51% attack
- BitCoin.... BitCoin-NG...... ByzCoin
- RepuCoin and its resiliency....

Other Challenges

► CHALLENGE 2 explosion of proposals - a lot of confusion and doubtful implementations

- Proof of Stake,
- PeerCensus,
- Proof of Capacity,
- Proof of Activity,
- ......

Thunderella
Solida
ByzCoin
HoneyBadger
....

► Challenge 3 Privacy: Reconcile Privacy and Transparency (not elaborated much)

Blockchain Consensus Protocols: an Outlook

- Marko started with some definitions and immediately attaked CONSENSUS to let the chain grow
- **Proof-of-Work (PoW)**
  - Forks (double spending)
  - PERFORMANCE (scalability, thoughput, ENERGY CONSUMPTION!) 987 kWh per transaction!
- **Proof-of-Stake (PoS)** **cheaper**
  - PoS usually sits on top of PoW tree data structure
  - Forks

- BFT in Blockchains
  - All PoS protocols resort in one way or another to BFT
- PoW vs. BFT for Blockchains..
- Outstanding challenges in BFT for blockchains
  - **Maximizing throughput on WANs (bottlenecks)**
  - **Scaling to 100+ nodes, without sacrificing performance**
  - **Robust but understandable protocols**
  - **Scalable incentives**
  - **Simplicity, provability and testing**

General discussion

- The two speakers subject to frequent attacks from malicious attendees stealing their time - which they have only partially managed!!

- However out of the discussion:
- Assumptions and fault models not clear! (E.G. Time)
- Cost per transactions very very high - leaves many concerns
- Business model? And applications?