Session 4.
Experience with Deployed Blockchains

Experiences with BFT-SMaRT as a consensus substrate of Permissioned Legers

Alysson Bessani, U. Lisbon

- Blockchain is Good for EVERYTHING! (Or for nothing?)
- BFT SmaRT: Byzantine Fault Tolerance based on State Machine Replication
- It's a platform that has now been used by others as a basis for blockchan applications, including:
  - Symbiont: closed source effort, apparently ported code base to Go language. Targeting insurance market, I think.
  - C-rda: open source blockchain project targeting financial model; with no global shared ledger but many distributed ledgers shared by (overlapping?) groups of market participants
  - Hyperledger fabric: IBM open source modular permissioned block chain. Not all "peers" are equal
- Also developing a BFT SMaRT ording service
- Takeaways: performance on LAN /WAN assessed, looks practical
- Research area: interesting bit to investigate diversity/security interactions

Investigating and securing smart contracts
Radu State, U. Luxembourg

A smart contract is a computerised transaction protocol (i.e. a program)

ergo it will have bugs

Attackers can and have exploited these

It makes sense to analyze programs, including smart contracts, to detect these in advance and eliminate them before they cause trouble

OSIRIS program developed to do this specifically for smart contract code

Unresolved issue: how to responsibly disclose bugs found in a smart contract whose participants are anonymous?

Discussion

- Noting disconnects between legal and technical views of smart contracts
- Underlying doubts about investing in "a bag of bits"
  - Can be a legitimate way to provide liquidity for smaller startups
  - Can be a medium of exchange avoiding banks
  - Can be a way to make money, based on "greater fool" theory (Ponzi?)