Distributed Ledgers

Breakout Session

Participants

- Christian Facci
- Severin Kacianka
- Holger Kinkelin

Questions

- How can we use distributed ledgers for accounting and logging?
- Which technology is best suited for relatively small distributed ledger networks?
- Which other interesting (academic) problems exist that can be mitigated by this tech?
- What are interesting academic research questions in this field?

Distributed Ledgers / Blockchains

- Blockchain Structure
  + Consensus on latest Block
  + Replication

- = Unerasable/immutable storage

- = Unmodifiable/tamperproof storage

- ==> Good basis for accounting and logging

Accountability for Trustworthy Network Administration

- **Problem:**
  - Administrator can reconfigure systems as he pleases
  - Administrator can modify log information on device + even external syslog server to some extent
- **We want:**
  - Multi-party approval for (proposed) config changes
  - Accountability/traceability of configuration/approval

Approach

- Prohibit „direct“ administration via SSH, Ansible, Puppet, etc. Distribute configuration from trusted repository (= BC)

- Admin *proposes* new signed configuration of device by writing the config into the Config.-BC

- Auditors *review* configuration and write their signed consent/dissent into Config.-BC

- Devices *pull* (and verify) new configuration from Config.-BC and apply them automatically

How is that different to a GIT/SVN/… repo with signed configs?

- Repos are typically hosted on a (central) server, multiple clients have checked out versions only (no fully history, etc.)
- In a BC nodes have full copies of the BC
- ==> Replication is better
- ==> Admin of repo might roll back an older version to cover her tracks

Accountability for Autonomous System Logs (e.g.: Drone Flight Data)

- **Problem:**
  - Autonomous Drones and drone pilots are a threat when they enter „no-fly zones“, etc.
  - ==> We need log data in case an accident occurs
  - Blackbox in the Drone is not feasible as you cannot build the Blackbox sturdy enough so that it survives catastrophic crashes (Drone vs. Airbus fan blades)
  - Blackbox is maybe not accessible to authorities

Approach

- Drone(s) sends stream of inflight data to ground control station(s)
- Ground control station writes drone data into BC

Problems

- Throughput: BC must be reasonably quick
  - We need to look into this matter more
- Trust into input data: Drone might send faked information
  - Trusted component collecting/sending data
- Privacy: A lot of person-related information could be stored in the BC
  - („Lawful interception“) encryption

Problems II

- Consensus protocol based on Proof of Work used by public BC cannot be applied in smaller networks
    - Network can be biased easily, e.g. DoS some honest nodes
- Possible alternatives that need more investigation
    - Proof of Stake
    - PBFT (practical byzantine fault tolerance)

„Conclusion“

- We think the tech is worth looking into for all sorts of accounting/logging
- We see some advantages compared to other logging solutions
- We must do further research on suitable BC implementations