Distributed DCR in a TEE

Malthe Kirkbro, Mikkel Gaub, Frederik Madsen

January 17, 2018

The Problem

- Distributed DCR
- Consensus
- SGX

SGX

- Trusted Execution Environment
- Hardware keys

Enclave

- Processor Reserved Memory (PRM)
- Enclave mode
- SGX Enclave Control Structure (SECS)
- Enclave Page Cache (EPC)

Attestation

- Local
  - Report MACed with CPU-fused key (EREPORT)
- Remote
  - Locally attested report signed by EPID private key

Trusted Monotonic Counter

- Monotonic non-volatile counter
- Demo!

Security

- Attacks on confidentiality (including SPECTRE!)
    - Note that this can be problematic with TLS keys after attestation
- No (to us known) attacks on integrity

Related Works

- Some solutions to similar problems exist, using SGX

FastBFT

- BFT with *O(n)*
- SGX solves secret distribution and order of requests

Hyperledger Sawtooth

- Ethereum implementation with blockchain using PoET algorithm instead of mining
- Very similar to our imagined solution