

A modern office interior with glass walls and orange chairs. The image is partially obscured by a white overlay on the right side, which contains the title and authors. The office has a clean, minimalist design with white walls and a glass railing on the upper level.

# **Distributed DCR in a TEE**

Malthe Kirkbro, Mikkel Gaub, Frederik Madsen

January 17, 2018

# The Problem

- ▶ Distributed DCR
- ▶ Consensus
- ▶ SGX

- ▶ Trusted Execution Environment
- ▶ Hardware keys

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

- ▶ 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!

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

- ▶ Some solutions to similar problems exist, using SGX



- ▶ 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