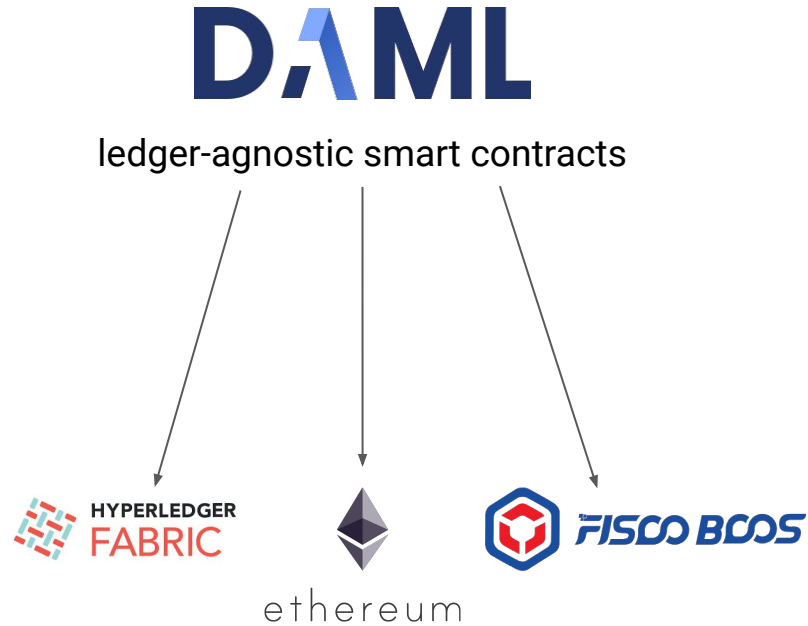


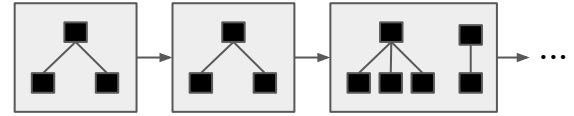
# A semantic domain for privacy-aware smart contracts and interoperable sharded ledgers

Sören Bleikertz, **Andreas Lochbihler**, Ognjen Marić, Simon Meier,  
Phoebe Nichols, Matthias Schmalz, Ratko G. Veprek

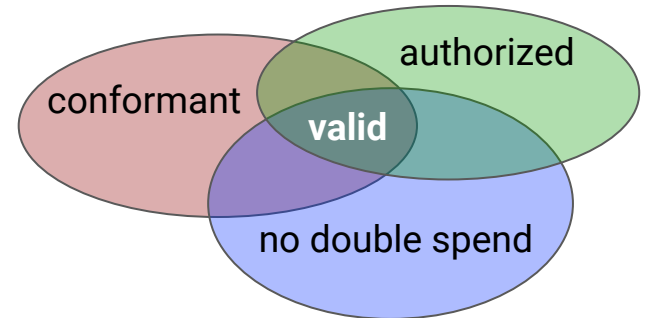
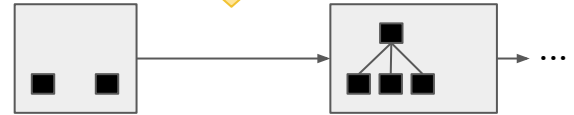
# DAML ledger model



ledger = list of hierarchical transactions

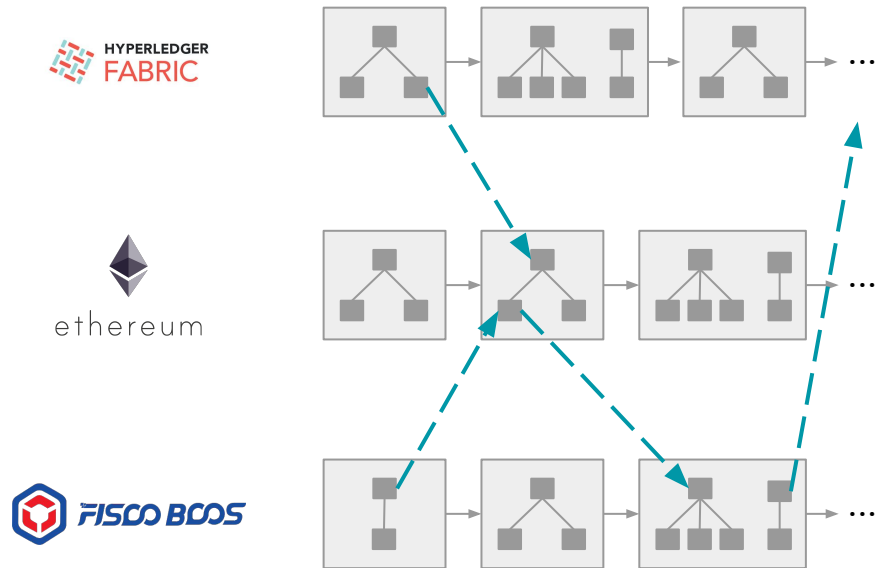


privacy-aware projection



# Sharding and Interoperability

Partially order the transactions



**Canton protocol:**  
synchronize across ledgers with vector clocks

Verification challenges:

- **Correctness** Vector clocks ensure causality
- **Liveness** No deadlocks

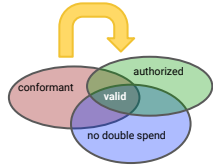
with Byzantine behaviour and privacy-awareness

# Formalization status



## Completed

- Totally ordered ledgers



## Next steps

- relaxation to partial orders
- vector clocks

## Open

- How to define deadlock?

# More information



Tuesday Jan 19, 20:00-20:30 CET  
Breakout room: Digital Asset (CPP)