Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

KASTEL

Praxis der Forschung

Formal Modeling of Distributed Ledger Applications

Background.

Smart Contracts...

- work in a distributed ledger or blockchain system (e.g., Ethereum or Hyperledger Fabric)
- take control over resources
- can be written in domain-specific languages (Solidity for Ethereum) or general-purpose languages (Java, Go, Javascript for Hyperledger Fabric)
- consist of *transactions* that can be called by users or other contracts

Distributed Ledger Applications...

- created by one or more smart contracts and their environment
- conceptually more complicated than a single transaction or smart contract

Goals.

Modeling distributed ledger applications:

- Abstract from concrete platforms or languages
- Capture the behavior of an application
- Allow formal reasoning about interesting properties:
  - Functional Correctness
  - Safety, security, and liveness properties
  - Invariants of the ledger
  - Temporal properties
  - Confidentiality, integrity, authenticity of data

Kontakt

Jonas Schiffl jonas.schiffl@kit.edu Office: 50.34, R226