Karlsruher Institut für Technologie

KASTEL - Information Security and Dependability
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Student Assistants / Theses

Smart Contracts: Modelling and Verification

Overview. Smart contracts are programs which run in conjunction with a blockchain or another type of distributed ledger. They function as a trusted computing platform, in the sense that anyone can be sure what transactions are made and what computations are performed, without having to run the programs themselves. Smart contracts are

- **immutable:** cannot be changed after deployment
- **public:** bytecode (and usually source code) is open for all to see
- **attractive targets** because they handle valuable assets

Therefore: **Smart contracts have to be correct upon deployment!**

Research Goals.

Design and development of

- a method for modeling smart contract applications in an intuitive way,
- tools for specifying the intended behaviour,
- a process for verifying that the application works as intended and is secure against malicious agents.

How You can contribute. Are you interested in designing an abstract representation of smart contracts, and methods for verifying correctness and security properties?

⇒ **Apply for a Bachelor's or Master's Thesis!**

Are you interested in implementing the abstract representation and its interfaces to formal analysis tools?

⇒ **Apply as a Student Assistant / "Hiwi"!**

Contact

Jonas Schiffl jonas.schiffl@kit.edu 50.34 R226