Universität Bayreuth
Prof. Dr. Nils Urbach
Professur für Wirtschaftsinformatik
und Strategisches IT-Management

UNIVERSITÄT BAYREUTH

Ansprechpartner
Lehrkoordination WI

Telefon
+49 921 55 - 4705

E-Mail
wi-lehrkoordination@uni-bayreuth.de

Bachelorarbeit / Masterarbeit

Smart Contract Security

Blockchain systems carry significant value by now. Smart contracts, computer programs that are executable in blockchain networks, provide logic for a variety of use cases. Examples include gambling, auctions, escrow services, or lending without a central intermediary. Often, the programs are valuable targets for attackers and first occurrences of security incidents were reported already. However, there is currently no systematization of attacks on smart contracts, making a directed plan of action difficult to develop. The aim of this thesis is therefore to develop a systematization of available attacks on smart contract systems using the attack tree notation. The tree should be based on existing literature and practice on blockchain software engineering. The scope and research method varies depending on the type of thesis (i.e. Master's or Bachelor's thesis).

Empfohlene Einstiegsliteratur:

- Torres, C. F., & Steichen, M. (2019). The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts.
- Atzei, N., Bartoletti, M., & Cimoli, T. (2017, April). A survey of attacks on ethereum smart contracts. In International Conference on Principles of Security and Trust (pp. 164-186). Springer, Berlin, Heidelberg.
- Mauw, S., & Oostdijk, M. (2005, December). Foundations of attack trees. In International Conference on Information Security and Cryptology (pp. 186-198). Springer, Berlin, Heidelberg.

Betreuer: Vincent Schlatt, M.Sc.