ICT22-007 - ForSmart: Effective Formal Methods for Smart-Contract Certification

Abstract

Correctness and security of smart contracts is critical as digital assets may be at stake. To detect or even avoid such vulnerabilities in smart contracts, there have emerged bug-finding techniques, which lack soundness, and verification techniques, which lack precision. In ForSmart, we aim to develop a hybrid, automated certification framework for smart contracts that symbiotically combines bug-finding in the form of test generation and verification in the form of sound static analysis, thereby achieving soundness and precision. Advanced automated-reasoning mechanisms, which we plan to develop and tailor to this domain, will support both testing and static analysis. We will maximize the impact of ForSmart by applying our framework to concrete applications of academic, industrial, and public relevance, such as DeFi apps, with a focus on certifying functional and security properties, as well as by making our infrastructure available to contract developers, auditors, and users. We additionally plan to leverage our ongoing collaborations with Certora, the Ethereum Foundation, ConsenSys, and Microsoft Research. We request funding for 3 PhD students. The duration of each PhD will be 4 years – the funding will cover 3.5 years, and the remaining time will be spent on internships at the aforementioned companies to encourage industrial adoption of our framework. The core team of ForSmart (PIs) has a 2/3 female participation. We aim to maintain such a balance when expanding.

Scientific disciplines:
IT security (34%) | Software development (33%) | Theoretical computer science (33%)

Keywords:
test generation, static analysis, automated reasoning, hybrid certification, smart contracts

---

Principal Investigator:	Maria Christakis
Institution:	TU Wien
Co-Principal Investigator(s):	Laura Kovács (TU Wien) Matteo Maffei (TU Wien)

v.l.n.r. Maria Christakis ©Oliver Dietze; Laura Kovacs ©Luiza Puiu; Matteo Maffei

---

Status: Ongoing (01.09.2023 - 31.08.2027)

Further links to the persons involved and to the project can be found under
https://www.gmbh.wwtf.at/funding/programmes/ict/ICT22-007/