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

Zusammenfassung

Die Korrektheit und Sicherheit von Smart Contracts ist von entscheidender Bedeutung, da digitale Vermögenswerte auf dem Spiel stehen können. Um Schwachstellen in Smart Contracts zu erkennen oder sogar zu vermeiden, werden digitale Methoden zur Fehlersuche und Verifikation eingesetzt, denen es bisher aber an Zuverlässigkeit bzw. Präzision fehlt.

In ForSmart wollen wir eine hybride, digitale Methodologie für die Analyse von Smart Contracts entwickeln, welche die Fehlersuche durch Testen, formaler Verifizierung und mathematischem Beweis kombiniert. Dadurch werden eine hohe Zuverlässigkeit und eine hohe Präzision erreicht.

Die Wirkung von ForSmart wird maximiert, indem wir unsere Methodologie auf konkrete Anwendungsbeispiele von akademischer, industrieller und öffentlicher Relevanz anwenden, und die Ergebnisse Entwicklern von Smart Contracts, Auditoren sowie Benutzern zur Verfügung stellen werden. Wir planen außerdem, bestehende Kooperationen mit Certora, der Ethereum Foundation, ConsenSys und Microsoft Research im Rahmen des Projekts vorteilhaft zu nutzen.

Wir beantragen die Finanzierung von 3 Doktoranden, die im Rahmen ihrer Doktorarbeit Praktika bei den oben genannten Unternehmen durchführen sollen, um die Einführung der ForSmart Methoden in der Industrie anzuregen.

Das Kernteam von ForSmart (PIs) ist zu 2/3 weiblich. Eine derartige Verteilung wollen wir bei Expansion wahren.

Wissenschaftliche Disziplinen:
IT security (34%) | Software development (33%) | Theoretical computer science (33%)

Schlagworte:
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: Laufend (01.09.2023 – 31.08.2027)

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://www.wwtf.at/funding/programmes/ict/ICT22-007/

Wiener Wissenschafts-,
Forschungs- und Technologiefonds
Vienna Science and Technology Fund