Invited Talk: Harnessing SMT Solvers for Verifying Low Level Programs

Mooly Sagiv

Abstract

Smart contracts are positioned to revolutionize today's business processes by automating financial transactions, digital media distribution, medical record management, property ownership registration, and more. The vast majority of smart contracts are implemented using virtual machines such as EVM and WebAssembly which are very powerful. However, bugs in smart contracts lead to tremendous economic losses.

I will describe our ongoing effort to leverage existing SMT solvers for verifying smart contracts and uncovering subtle bugs. We are developing SaaS technology demo.certora.com for smart contract verification. This technology is intended to be used as part of the CI/CD of smart contract development.

Safety properties of smart contracts are described in a high level manner to enable reuse across different smart contracts. The EVM code is decompiled into an intermediate representation using static analysis and the SMT formula is generated and fed into SMT solvers. The formulas include nonlinear integer arithmetic with large constants, uninterpreted functions, quantifications.

I will also describe some of the high level properties checked and bugs found using the SMT solvers.

This is a joint work with Thomas Bernardi, Nurit Dor, Anastasia Fedotov, Shelly Grossman, Alexander Nutz, Lior Oppenheim, Or Pistiner, John A. Toman, and James R. Wilcox.

François Bobot, Tjark Weber (eds.); SMT 2020, pp. 2–2