Superoptimization of (Optimized) Smart Contracts

(Invited Talk)

Elvira Albert*⋆

*Instituto de Tecnología del Conocimiento, Madrid, Spain
⋆Complutense University of Madrid, Spain
elvira@sip.ucm.es

Superoptimization is a compilation technique that searches for the optimal sequence of instructions semantically equivalent to a given (loop-free) initial sequence. This talks overviews our approach for super-optimization of smart contracts based on Max-SMT which is split into two main phases:

(i) the extraction of a functional specification from the basic blocks of the smart contract, which is simplified using rules that capture the semantics of the arithmetic, bit-wise, relational operations, etc. and

(ii) the synthesis of optimized blocks which, by means of an efficient Max-SMT encoding, finds the bytecode blocks with minimal cost (according to the selected optimization criteria) and whose functional specification is equal (modulo commutativity) to the extracted one.

Our experiments on randomly selected real contracts achieve important gains in gas and in bytes-size over code already optimized by solc.

Submitted to:
VPT 2022