# SolSMT

tiny SMT solver inside the Solidity compiler

Christian Reitwiessner, Mate Soos
Ethereum Foundation

**Solidity**: Most widely used language for Ethereum smart contracts

not to be confused with **SolCMC**: interface to other SMT solvers for program verification

**SolSMT**: tiny integrated SMT solver used in optimizer

- remove redundant overflow checks, determine non-overlapping memory access, etc
- any bug in SMT solver can lead to bug in program
- needs to be fully deterministic and platform-independent for reproducibility
- implements QF_LRA using CDCL(T)
- inspired by MiniSat1.14 plus Dutertre-deMoura for LRA
- written in ~3k lines of C++

plan to add proof generation and checking for SAT and theory

https://github.com/ethereum/solidity  branch=smtComp