Deductive Verification of Smart Contracts

Franck Cassez
Mantle R&D, Sydney, Australia

Abstract

At the core of the Ethereum network is the Ethereum Virtual Machine (EVM) which can execute programs written in EVM bytecode. This remarkable feature empowers users to define complex business logic that can be executed programmatically by programs called smart contracts. Smart contracts are programs and may contain bugs. There are several examples of smart contract vulnerabilities that have been exploited in the past: in 2016, a re-entrance vulnerability in the Decentralised Autonomous Organisation (DAO) smart contract was exploited to steal more than USD50 Million. The total value netted from DeFi hacks in 2023 is estimated to be more than $1.5 billion. In this talk I will discuss formal verification of smart contracts. The main technique is deductive verification supported by the verification-friendly language Dafny. I will show how we can use deductive verification to reason about smart contracts, from high-level specifications (Dafny), to intermediate representation (Yul) and finally low-level EVM bytecode.

2012 ACM Subject Classification Software and its engineering → Formal software verification

Keywords and phrases Smart Contracts, Deductive Verification

Digital Object Identifier 10.4230/OASIcs.FMBC.2024.1

Category Invited Talk

Bio

Dr. Franck Cassez is currently Head of Research at Mantle. From 2019 to April 2023, he was Lead Researcher at Consensys in the R&D department. Before joining ConsenSys, he worked as a research scientist/academic for 25 years, at the French National Centre for Scientific Research (CNRS, France), National ICT Australia (NICTA now DATA61, Sydney AU) and Macquarie University (Sydney AU). He received his dual Engineering Degree in Computer Science/M.S. (1990) and a Ph.D. in Computer Science from from Ecole Centrale, Nantes, France in 1993.

Franck has published papers at major conferences including CONCUR, CAV, TACAS, ATVA, LPAR and several other venues. He was the recipient of several best paper awards including LPAR 2015, FMICS 2022, a Test-of-Time Award at CONCUR'22, and a Marie Curie Fellowship (2008-2011), an individual EU research excellence competitive grant. Franck has collaborated with many research groups in Europe and Australia and is known for some important results on timed automata (e.g. Test-of-Time Award at CONCUR'22 for the 2002 CONCUR paper The Impressive Power Of Stopwatches with Kim G. Larsen) and some efficient algorithms for timed games and time Petri nets.

Franck's contributions also include bringing research in practice, including static analysis tools (Goanna at NICTA, patent on Analysis of Program code, Skink at the International Software Verification Competition) or general purpose software packages (e.g. ScalaSMT a Scala interface combining state-of-the-art SMT-solvers). Franck's interest for blockchain technology started in 2019 when he joined ConsenSys and worked on several Ethereum research projects including the verification of the Deposit Contract, the formal verification of Smart Contracts in Dafny(best paper award at FMICS'22), a semantics of the EVM in Dafny, a semantics of Yul in Dafny. He has co-authored over 90 academic papers.

Franck's research interests include smart contracts security and analysis, formal verification techniques, programming languages, concurrent systems, zk-proof technology and rollups.

5th International Workshop on Formal Methods for Blockchains (FMBC 2024).
Editors: Bruno Bernardo and Diego Marmsoler; Article No. 1; pp. 1:1–1:1
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany