Report from Dagstuhl Seminar 11013

# Formal Verification Tool Based on Symbolic Execution for Smart Contract

**Edited by**

**Thi Thu Ha Doan[1] and Peter Thiemann[2]**

1 **University of Freiburg, Germany** doanha@informatik.uni-freiburg.de
2 **University of Freiburg, Germany** thiemann@informatik.uni-freiburg.de

## Abstract

In the context of blockchain technology, the immutability of smart contracts once implemented underscores the critical need to ensure their accuracy. Even in cases where smart contract implementations are not overly extensive and have undergone testing before deployment, the blockchain community has identified significant vulnerabilities in their design. In addition, the relatively new nature of smart contract languages has led to unforeseen errors due to a lack of familiarity with their intricacies. To overcome these challenges, formal verification emerges as a key solution to guarantee the correctness of smart contracts. In response to this need, we have developed a formal verification tool for smart contracts, particularly those written in Michelson. This tool uses symbolic execution to simulate the implementation of the smart contract language, helping to detect subtle errors that are difficult for smart contract developers to detect. In addition, our tool includes a domain-specific language that allows users to precisely specify contract properties. By interacting with an SMT solver, it can handle a wide range of properties. In particular, it streamlines the process of reviewing requirements, uncovering hidden errors, and validating user-defined properties. In summary, our research highlights the need for robust verification of smart contracts. We present a purpose-built tool that utilizes symbolic execution and a domain-specific language to improve the correctness of smart contracts and provide a comprehensive solution to mitigate potential pitfalls in blockchain-based applications.

**Seminar** 03.–07. January, 2011 – https://www.dagstuhl.de/11013
**2012 ACM Subject Classification** General and reference → General literature; Hardware → 3D integrated circuits; Software and its engineering → Software design engineering; Networks → Network performance analysis
**Keywords and phrases** Smart Contract, Blockchain, Formal Verification, Symbolic Execution
**Digital Object Identifier** 10.4230/DagRep.1.1.1
**Edited in cooperation with** Tom Collector

## 1 Executive Summary

*T.T.Ha Doan (University of Freiburg, Germany, doanha@informatik.uni-freiburg.de)*
*P. Thiemann (University of Freiburg, Germany, thiemann@informatik.uni-freiburg.de)*



This summary summarizes the outcomes of our seminar. The seminar focused on

- important issues,
- relevant problems, and


Seminar Sample, *Dagstuhl Reports*, Vol. 1, Issue 1, pp. 1–4
Editors: John Q. Open and Joan R. Access
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- adequate solutions.

As a major result from the seminar, the following problems have been identified:

1. The problem of writing a brief, but concise executive summary.
2. The problem of collecting all abstracts from talks.
3. The problem of preparing summaries from working groups, open problem sessions, and panel discussions.

## 2 Table of Contents

## 3 Introduction