3rd International Workshop on Formal Methods for Blockchains

FMBC 2021, July 18-19, 2021, Los Angeles, California, USA
(Virtual Conference)

Edited by
Bruno Bernardo
Diego Marmsoler
OASIcs – OpenAccess Series in Informatics

OASIcs is a series of high-quality conference proceedings across all fields in informatics. OASIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board

- Daniel Cremers (TU München, Germany)
- Barbara Hammer (Universität Bielefeld, Germany)
- Marc Langheinrich (Università della Svizzera Italiana – Lugano, Switzerland)
- Dorothea Wagner (Editor-in-Chief, Karlsruher Institut für Technologie, Germany)

ISSN 1868-8969

https://www.dagstuhl.de/oasics
Contents

Preface
   Bruno Bernardo and Diego Marmsoler ........................................... 0:vii

Program Committee
   ................................................................................. 0:ix

Supporting Reviewers
   ................................................................................. 0:xi

Regular Papers

Towards Verified Price Oracles for Decentralized Exchange Protocols
   Kinnari Dave, Vilhelm Sjöberg, and Xinyuan Sun ................................. 1:1–1:14

Money Grows on (Proof-)Trees: The Formal FA1.2 Ledger Standard
   Murdoch J. Gabbay, Arvid Jakobsson, and Kristina Sojakova ............... 2:1–2:14

Short Papers

Using Coq to Enforce the Checks-Effects-Interactions Pattern in DeepSEA Smart Contracts
   Daniel Britten, Vilhelm Sjöberg, and Steve Reeves .............................. 3:1–3:8

Formally Documenting Tenderbake
   Sylvain Conchon, Alexandrina Korneva, Çagdas Bozman, Mohamed Iguernlala, and Alain Mebsout ......................................................... 4:1–4:9

Towards Contract Modules for the Tezos Blockchain
   Thi Thu Ha Doan and Peter Thiemann ............................................... 5:1–5:9

Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
Preface

The 3rd International Workshop on Formal Methods for Blockchains (FMBC) took place virtually on July 18/19 2021 as part of CAV 2021, the 33rd International Conference on Computer-Aided Verification. FMBC’s purpose is to be a forum to identify theoretical and practical approaches applying formal methods to blockchain technology.

This third edition of FMBC attracted 15 submissions on topics such as verification of smart contracts or analysis of consensus protocols. Each paper was reviewed by at least three program committee members or appointed external reviewers. This led to a selection of 5 papers (2 long and 3 short) that were presented at the workshop as regular talks, as well as 3 extended abstracts that were presented as lightning talks. Additionally, we were very pleased to have an invited keynote by David L. Dill (Novi/Facebook, USA).

This volume contains the papers selected for regular talks as well as the abstract of the invited talk.

We thank all the authors that submitted a paper, as well as the program committee members and external reviewers for their immense work. We are grateful to Arie Gurfinkel, Workshop Chair of CAV 2021, for his guidance. Finally, we would like to express our gratitude to our sponsor Nomadic Labs for its generous support.

September 2021

Bruno Bernardo
Diego Marmolnol

nomadic labs

Editors: Bruno Bernardo and Diego Marmolnol
OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
Program Committee

Wolfgang Ahrendt
Chalmers University of Technology, Sweden
Lacramioara Astefanoei
Nomadic Labs, France
Massimo Bartoletti
University of Cagliari, Italy
Bruno Bernardo
Nomadic Labs, France
Joachim Breitner
Dfinity Foundation, Germany
Achim Brucker
University of Exeter, UK
Zaynah Dargaye
Nomadic Labs, France
Jérémie Decouchant
TU Delft, Netherlands
Dana Drachsler Cohen
Technion, Israel
Ansgar Fehnker
University of Twente, Netherlands
Maurice Herlihy
Brown University, USA
Lars Hupel
INNOQ, Germany
Florian Kammüller
Middlesex University London, UK
Igor Konnov
Informal Systems, Austria
Andreas Lochbihler
Digital Asset, Switzerland
Diego Marmsoler
University of Exeter, UK
Simão Melo de Sousa
Universidade da Beira Interior, Portugal
Karl Palmskog
KTH, Sweden

Maria Potop-Butucaru
Sorbonne Université, France
Andreas Rossberg
Dfinity Foundation, Germany
Albert Rubio
Complutense University of Madrid, Spain
César Sanchez
Imdea, Spain
Clara Schneidewind
TU Wien, Austria
Ilya Sergey
Yale-NUS College/NUS, Singapore
Mark Staples
CSIRO Data61, Australia
Meng Sun
Peking University, China
Simon Thompson
University of Kent, UK
Josef Widder
Informal Systems, Austria
Supporting Reviewers

Yuteng Lu
Luis Arrojado da Horta