2nd Workshop on Formal Methods for Blockchains

FMBC 2020, July 20–21, 2020, Los Angeles, California, USA (Virtual Conference)

Edited by

Bruno Bernardo

Diego Marmsoler

Editors

Bruno Bernardo
Nomadic Labs, Paris, France
bruno@nomadic-labs.com

Diego Marmsoler
University of Exeter, UK
d.marmsoler@exeter.ac.uk

ACM Classification 2012
Security and privacy → Logic and verification; Software and its engineering → Formal software verification; Security and privacy → Distributed systems security; Computer systems organization → Peer-to-peer architectures

ISBN 978-3-95977-169-6

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at https://www.dagstuhl.de/dagpub/978-3-95977-169-6.

Publication date
December, 2020

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at https://portal.dnb.de.

Digital Object Identifier: 10.4230/OASIcs.FMBC.2020.0

OASIcs – OpenAccess Series in Informatics

OASIcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. OASIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

ISSN 1868-8969

https://www.dagstuhl.de/oasics

Contents

2nd Workshop on Formal Methods for Blockchains (FMBC 2020).
Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The 2nd Workshop on Formal Methods for Blockchains (FMBC) took place virtually on July 20/21 2020 as part of CAV 2020, the 32nd International Conference on Computer-Aided Verification. Its purpose was to be a forum to identify theoretical and practical approaches applying formal methods to blockchain technology.

This second edition of FMBC attracted 18 submissions (10 long papers, 4 short papers, and 4 extended abstracts) 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 10 papers (7 long and 3 short) that will be presented at the workshop as regular talks, as well as 1 long paper and 4 extended abstracts that will be presented as lightning talks. Additionally, we were very pleased to have an invited keynote by Grigore Rosu (University of Illinois at Urbana-Champaign).

This volume contains the papers selected for regular talks, the extended abstracts and paper selected for lightning talks as well as the abstract of the invited talk. Before inclusion, the papers were reviewed a second time after the workshop by the program committee.

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 Shuvendu Lahiri and Chao Wang, Program Chairs of CAV 2020, and to Zvonimir Rakamaric, Workshop Chair of CAV 2020, for their support and guidance. Finally, we would like to express our gratitude to our sponsor Nomadic Labs for its generous support.

October 2020

Bruno Bernardo
Diego Marmsoler

2nd Workshop on Formal Methods for Blockchains (FMBC 2020).
Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
OASICS 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

Bernhard Beckert
Karlsruhe Institute of Technology, Germany

Bruno Bernardo
Nomadic Labs, France

Achim Brucker
University of Exeter, UK

Silvia Crafa
Universita di Padova, Italy

Zaynah Dargaye
Nomadic Labs, France

Jérémie Decouchant
University of Luxembourg, Luxembourg

Ansgar Fehnker
University of Twente, Netherlands

Georges Gonthier
Inria, France

Maurice Herlihy
Brown University, USA

Florian Kammueller
Middlesex University London, UK

Igor Konnov
Informal, Austria

Andreas Lochbihler
Digital Asset, Switzerland

Diego Marmsoler
University of Exeter, UK

Anastasia Mavridou
NASA Ames, USA

Simão Melo de Sousa
Universidade da Beira Interior, Portugal

Andrew Miller
University of Illinois at Urbana-Champaign, USA

Karl Palmskog
KTH, Sweden

Vincent Rahli
University of Birmingham, UK

Andreas Rossberg
Dfinity Foundation, Germany

Claudio Russo
Dfinity Foundation, USA

César Sanchez
Imdea, Spain

Clara Schneidewind
TU Wien, Austria

Ilya Sergey
Yale-NUS College/NUS, Singapore

Bas Spitters
Aarhus University/Concordium, Denmark

Mark Staples
CSIRO Data61, Australia

Meng Sun
Peking University, China

Simon Thompson
University of Kent, UK

Philip Wadler
University of Edinburgh / IOHK, UK

2nd Workshop on Formal Methods for Blockchains (FMBC 2020).
Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2nd Workshop on Formal Methods for Blockchains (FMBC 2020).
Editors: Bruno Bernardo and Diego Marmsoler

OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Supporting Reviewers

Luis Arrojado da Horta

Yi Li

João Santos Reis

Ralf Sasse

Søren Eller Thomsen