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

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 978-3-95977-209-9

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/978-3-95977-209-9.

Publication date
November, 2021

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.

License
This work is licensed under a Creative Commons Attribution 4.0 International license (CC-BY 4.0): https://creativecommons.org/licenses/by/4.0/legalcode.
In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:
- Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/OASIcs.FMBC.2021.0

ISBN 978-3-95977-209-9 **ISSN 1868-8969** **https://www.dagstuhl.de/oasics**

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

Regular Papers

Short Papers

3rd International Workshop on Formal Methods for Blockchains (FMBC 2021).
Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
OASICS 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 Marmsoler

nomadic labs

3rd International Workshop on Formal Methods for Blockchains (FMBC 2021).
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

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 Kammueller
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

3rd International Workshop on Formal Methods for Blockchains (FMBC 2021).
Editors: Bruno Bernardo and Diego Marmsoler
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

3rd International Workshop on Formal Methods for Blockchains (FMBC 2021).
Editors: Bruno Bernardo and Diego Marmsoler

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

Supporting Reviewers

Yuteng Lu

Luis Arrojado da Horta