

2nd Workshop on Formal Methods for Blockchains

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

Edited by

Bruno Bernardo

Diego Marmosler



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>.

License

This work is licensed under a Creative Commons Attribution 3.0 Unported license (CC-BY 3.0):
<https://creativecommons.org/licenses/by/3.0/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/OASlcs.FMBC.2020.0

ISBN 978-3-95977-169-6

ISSN 1868-8969

<https://www.dagstuhl.de/oasics>

OASlcs – OpenAccess Series in Informatics

OASlcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. OASlcs 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	
<i>Bruno Bernardo and Diego Marmsoler</i>	0:vii
Invited Talk	
Formal Design, Implementation and Verification of Blockchain Languages Using K	
<i>Grigore Rosu</i>	1:1–1:1
Smart contracts and payments	
Formal Specification and Verification of Solidity Contracts with Events	
<i>Ákos Hajdu, Dejan Jovanović, and Gabriela Ciocarlie</i>	2:1–2:9
Populating the Peephole Optimizer of a Smart Contract Compiler	
<i>Maria A. Schett and Julian Nagele</i>	3:1–3:15
Tezla, an Intermediate Representation for Static Analysis of Michelson Smart Contracts	
<i>João Santos Reis, Paul Crocker, and Simão Melo de Sousa</i>	4:1–4:12
A Blockchain Model in Tamarin and Formal Analysis of Hash Time Lock Contract	
<i>Colin Boyd, Kristian Gjøsteen, and Shuang Wu</i>	5:1–5:13
Merkle trees and Bitcoin	
Authenticated Data Structures as Functors in Isabelle/HOL	
<i>Andreas Lochbihler and Ognjen Marić</i>	6:1–6:15
Mechanized Formal Model of Bitcoin’s Blockchain Validation Procedures	
<i>Kristijan Rupić, Lovro Rožić, and Ante Derek</i>	7:1–7:14
Towards Verifying the Bitcoin-S Library	
<i>Ramon Boss, Kai Brännler, and Anna Doukma</i>	8:1–8:9
Consensus	
On the Formal Verification of the Stellar Consensus Protocol	
<i>Giuliano Losa and Mike Dodds</i>	9:1–9:9
Formal Specification and Model Checking of the Tendermint Blockchain Synchronization Protocol	
<i>Sean Braithwaite, Ethan Buchman, Igor Konnov, Zarko Milosevic, Iliana Stoilkovska, Josef Widder, and Anca Zamfir</i>	10:1–10:8
Inter-Blockchain Protocols with the Isabelle Infrastructure Framework	
<i>Florian Kammüller and Uwe Nestmann</i>	11:1–11:12

■ 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

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 Kammueler
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 Marmosler



OpenAccess Series in Informatics
0ASICS 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

