

5th International Workshop on Formal Methods for Blockchains

FMBC 2024, April 7, 2024, Luxembourg City, Luxembourg

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 → Formal methods and theory of security; Security and privacy → Logic and verification; Theory of computation → Program verification; Software and its engineering → Formal software verification; Security and privacy → Distributed systems security; Computer systems organization → Peer-to-peer architectures

ISBN 978-3-95977-317-1

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/978-3-95977-317-1>.

Publication date

May, 2024

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/OASlcs.FMBC.2024.0

ISBN 978-3-95977-317-1

ISSN 1868-8969

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

OASlcs – OpenAccess Series in Informatics

OASlcs is a series of high-quality conference proceedings across all fields in informatics. 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
Program Committee	
.....	0:ix
Supporting Reviewers	
.....	0:xi

Invited Talk

Deductive Verification of Smart Contracts	
<i>Franck Cassez</i>	1:1–1:1

Consensus

Formal Specification of the Cardano Blockchain Ledger, Mechanized in Agda	
<i>Andre Knispel, Orestis Melkonian, James Chapman, Alasdair Hill, Joosep Jääger, William DeMeo, and Ulf Norell</i>	2:1–2:18
Formally Verifying the Safety of Pipelined Moonshot Consensus Protocol	
<i>M. Praveen, Raghavendra Ramesh, and Isaac Doidge</i>	3:1–3:16
Towards Mechanised Consensus in Isabelle	
<i>Elliot Jones and Diego Marmsoler</i>	4:1–4:22

Smart Contracts

Formalizing Automated Market Makers in the Lean 4 Theorem Prover	
<i>Daniele Pusccheddu and Massimo Bartoletti</i>	5:1–5:13
Towards Benchmarking of Solidity Verification Tools	
<i>Massimo Bartoletti, Fabio Fioravanti, Giulia Matricardi, Roberto Pettinau, and Franco Sainas</i>	6:1–6:15
Towards Formally Specifying and Verifying Smart Contract Upgrades in Coq	
<i>Derek Sorensen</i>	7:1–7:14
A Practical Notion of Liveness in Smart Contract Applications	
<i>Jonas Schiffel and Bernhard Beckert</i>	8:1–8:13
Securing Aptos Framework with Formal Verification	
<i>Junkil Park, Teng Zhang, Wolfgang Grieskamp, Meng Xu, Gerardo Di Giacomo, Kundu Chen, Yi Lu, and Robert Chen</i>	9:1–9:16
Structured Contracts in the EUTxO Ledger Model	
<i>Polina Vinogradova, Orestis Melkonian, Philip Wadler, Manuel Chakravarty, Jacco Krijnen, Michael Peyton Jones, James Chapman, and Tudor Ferariu</i>	10:1–10:19



■ Preface

The 5th International Workshop on Formal Methods for Blockchains (FMBC) took place on April 7, 2024, as part of the European Joint Conferences on Theory and Practice of Software (ETAPS 2024). FMBC's purpose is to be a forum to identify theoretical and practical approaches that apply formal methods to blockchain technology.

This fifth edition of FMBC attracted 17 submissions: 13 full papers, 1 short paper, and 3 extended abstracts. Each of these papers was reviewed by at least three program committee members or appointed external reviewers. This led to a selection of 9 (full) papers that were presented at the workshop as regular talks, as well as 2 extended abstracts that were presented as lightning talks. Additionally, we were very pleased to have an invited keynote by Franck Cassez (Head of Research at Mantle).

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 Maxime Cordy and Renzo Gaston Degiovanni, Workshop Chairs of ETAPS 2024, for their help and guidance. FMBC 2024 was financially supported by the Ethereum Foundation's Ecosystem Support Program and Mantle.

April 2024

Bruno Bernardo
Diego Marmsoler



5th International Workshop on Formal Methods for Blockchains (FMBC 2024).

Editors: Bruno Bernardo and Diego Marmsoler



OpenAccess Series in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

■ Program Committee

Massimo Bartoletti
University of Cagliari, Italy

Bernhard Beckert
Karlsruhe Institute of Technology, Germany

Bruno Bernardo
Nomadic Labs, France

Martin Ceresa
IMDEA Software Institute, Spain

Manuel Chakravarty
Tweag, France

Sylvain Conchon
Paris-Saclay University, France

Denisa Diaconescu
University of Bucharest, Romania

Fritz Henglein
University of Copenhagen, Denmark

Maurice Herlihy
Brown University, US

Florian Kammüller
Middlesex University London, UK

Diego Marmsoler
University of Exeter, UK

Baolu Meng
GE Research, US

Ron Van Der Meyden
University of New South Wales, Australia

Burcu Kulahcioglu Ozkan
Delft University of Technology, Netherlands

Gordon J. Pace
University of Malta, Malta

Maria Potop-Butucaru
Sorbonne University, France

Vincent Rahli
University of Birmingham, UK

Sophie Rain
Vienna University of Technology, Austria


Albert Rubio
Complutense University of Madrid, Spain

Bas Spitters
Aarhus University, Denmark

Meng Sun
Peking University, China

5th International Workshop on Formal Methods for Blockchains (FMBC 2024).

Editors: Bruno Bernardo and Diego Marmosler

 OpenAccess Series in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

■ Supporting Reviewers

Pablo Gordillo

Alejandro Hernández-Cerezo

Xiangyu Li

Xiaokun Luan

Saswata Paul

Sarat Chandra Varanasi

