# 4th International Workshop on Formal Methods for Blockchains

**FMBC 2022, August 11, 2022, Haifa, Israel**

Edited by

Zaynah Dargaye

Clara Schneidewind

*Editors*

**Zaynah Dargaye**
Nomadic Labs, Paris, France
Zaynah.Dargaye@nomadic-labs.com

**Clara Schneidewind**
MPI-SP, Bochum, Germany
clara.schneidewind@mpi-sp.org

*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 978-3-95977-250-1

*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/978-3-95977-250-1.

*Publication date*
September, 2022

*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.2022.0

## 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.



**ISSN 1868-8969**

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

# Contents



4th International Workshop on Formal Methods for Blockchains (FMBC 2022).
Editors: Zaynah Dargaye and Clara Schneidewind
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

# Preface

The 4th International Workshop on Formal Methods for Blockchains (FMBC) took place on August 11, 2022, as part of CAV 2022, the 34th International Conference on Computer Aided Verification, and FLoC 2022, the 8th Federated Logic Conference. FMBC's purpose is to be a forum to identify theoretical and practical approaches that apply formal methods to blockchain technology.

This fourth edition of FMBC attracted 12 submissions on topics such as verification and testing of smart contracts or analysis of blockchain protocols. Each paper was reviewed by at least three program committee members or appointed external reviewers. This led to a selection of 4 (long) papers that were presented at the workshop as regular talks, as well as 6 works that were presented as lightning talks. Additionally, we were very pleased to have an invited keynote by Massimo Bartoletti (Università degli Studi di Cagliari, Italy).

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 Bruno Bernado and Diego Marmsoler, the Program Committee Chairs of the last editions of FMBC, for their constant support. Further, we would like to thank Shaull Almagor and Guillermo A. Pérez, Workshop Chairs of FLoC 2022, for their guidance. Finally, we would like to express our gratitude to our sponsors Algorand, Cluster of Excellence CASA – Cyber Security in the Age of Large-Scale Adversaries, IOHK, and Nomadic Labs for their generous support.

September 2022

Zaynah Dargaye
Clara Schneidewind





4th International Workshop on Formal Methods for Blockchains (FMBC 2022).
Editors: Zaynah Dargaye and Clara Schneidewind
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

# Program Committee

Wolfgang Ahrendt
Chalmers University of Technology, Sweden

Leonardo Alt
Ethereum Foundation, Germany

Lacramioara Astefanoaei
Nomadic Labs, France

Roberto Blanco
MPI-SP, Germany

Joachim Breitner
Germany

Achim Brucker
University of Exeter, UK

Ethan Cecchetti
University of Maryland, USA

Manuel Chakravarty
IOHK & Tweag, Netherlands

Jing Chen
Algorand Inc, USA

Zaynah Dargaye
Nomadic Labs, France

Jérémie Decouchant
TU Delft, Netherlands

Antonella Del Pozzo
Université Paris-Saclay & CEA & List, France

Dana Drachsler Cohen
Technion, Israel

Cezara Dragoi
INRIA & ENS & CNRS & PSL, France

Ansgar Fehnker
Twente, Netherlands

Dominik Harz
Interlay & Imperial College London, UK

Lars Hupel
INNOQ, Germany

Igor Konnov
Informal Systems, Austria

Paul Laforgue
Nomadic Labs, France

Julian Nagele
Bank of America, USA

Russel O'Connor
Blockstream

Maria Potop-Butucaru
LIP6, France

Albert Rubio
Complutense University of Madrid, Spain

César Sanchez
IMDEA, Spain

Clara Schneidewind
MPI-SP, Germany

Sun Meng
Peking University, China

Simon Thompson
IO Global, UK

Josef Widder
Informal Systems, Austria

4th International Workshop on Formal Methods for Blockchains (FMBC 2022).
Editors: Zaynah Dargaye and Clara Schneidewind
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

# Supporting Reviewers

Mojtaba Eshghie

4th International Workshop on Formal Methods for Blockchains (FMBC 2022).
Editors: Zaynah Dargaye and Clara Schneidewind

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