

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>.

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.2022.0

ISBN 978-3-95977-250-1

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>Zaynah Dargaye and Clara Schneidewind</i> | 0:vii |
| Invited Talk | |
| MEV-Freedom, in DeFi and Beyond | |
| <i>Massimo Bartoletti</i> | 1:1–1:1 |
| Regular Papers | |
| Finding Smart Contract Vulnerabilities with ConCert’s Property-Based Testing Framework | |
| <i>Mikkel Milo, Eske Hoy Nielsen, Danil Annenkov, and Bas Spitters</i> | 2:1–2:13 |
| Automatic Generation of Attacker Contracts in Solidity | |
| <i>Ignacio Ballesteros, Clara Benac-Earle, Luis Eduardo Bueso de Barrio, Lars-Åke Fredlund, Ángel Herranz, and Julio Mariño</i> | 3:1–3:14 |
| Proofgold: Blockchain for Formal Methods | |
| <i>Chad E. Brown, Cezary Kaliszyk, Thibault Gauthier, and Josef Urban</i> | 4:1–4:15 |
| Multi: A Formal Playground for Multi-Smart Contract Interaction | |
| <i>Martín Ceresa and César Sánchez</i> | 5:1–5:16 |

■ 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.

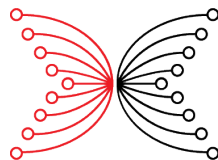
This fourth edition of FMBC attracted 12 submissions on topics such as verification and testing of smart contracts or analysis of blockchain protocols. Each paper was reviewed by at least three program committee members or appointed external reviewers. This led to a selection of 4 (long) papers that 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 Marmosoler, the Program Committee Chairs of the last editions of FMBC, for their constant support. Further, we would like to thank Shaul 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

The Algorand logo features a stylized 'A' icon composed of three overlapping shapes, followed by the word 'Algorand' in a bold, sans-serif font.The CASA logo consists of the word 'CASA' in a large, bold, teal font, with the tagline 'CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES' in a smaller, teal font below it.

INPUT | OUTPUT



nomadic labs

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



OpenAccess Series in Informatics
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 Drachslar 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



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

■ Supporting Reviewers

Mojtaba Eshghie



