6th International Workshop on Formal Methods for Blockchains

FMBC 2025, May 4, 2025, Hamilton, Canada

Edited by

Diego Marmsoler

Meng Xu

Editors

Diego Marmsoler
University of Exeter, UK
D.Marmsoler@exeter.ac.uk

Meng Xu
University of Waterloo, Canada
meng.xu.cs@uwaterloo.ca

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 978-3-95977-371-3

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/978-3-95977-371-3.

Publication date
May, 2025

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.2025.0

ISBN 978-3-95977-371-3 **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.

ISSN 1868-8969

https://www.dagstuhl.de/oasics

Contents

Preface
Diego Marmsoler and Meng Xu 0:vii

Program Committee Chairs
..... 0:ix

Steering Committee
..... 0:xi

Program Committee
..... 0:xiii

Supporting Reviewers
..... 0:xv

Invited Talks

Is Formal Verification Practical?
Wolfgang Grieskamp 1:1–1:2

Bringing the Power of Interactive Theorem Proving to Web3
Julian Sutherland 2:1–2:1

Regular Papers

Formal Verification in Solidity and Move: Insights from a Comparative Analysis
Massimo Bartoletti, Silvia Crafa, and Enrico Lipparini 3:1–3:18

ByteSpector: A Verifying Disassembler for EVM Bytecode
Franck Cassez 4:1–4:15

Towards a Mechanization of Fraud Proof Games in Lean
Martín Ceresa and César Sánchez 5:1–5:17

Validity, Liquidity, and Fidelity: Formal Verification for Smart Contracts in Cardano
Tudor Ferariu, Philip Wadler, and Orestis Melkonian 6:1–6:21

A Readable and Computable Formalization of the Streamlet Consensus Protocol
Mauro Jaskelioff, Orestis Melkonian, and James Chapman 7:1–7:18

Formal Verification of a Fail-Safe Cross-Chain Bridge
Filip Marić, Bernhard Scholz, and Pavle Subotić 8:1–8:18

Verifying Smart Contract Transformations Using Bisimulations
Kegan McIlwaine and James Caldwell 9:1–9:19

Program Logics for Ledgers
Orestis Melkonian, Wouter Swierstra, and James Chapman 10:1–10:22

Formally Specifying Contract Optimizations with Bisimulations in Coq
Derek Sorensen 11:1–11:13

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Tool Papers

Isabelle/Solidity: A Tool for the Verification of Solidity Smart Contracts
Asad Ahmed and Diego Marmsoler 12:1–12:9

A Benchmark Framework for Byzantine Fault Tolerance Testing Algorithms
João Miguel Louro Neto and Burcu Kulahcioglu Ozkan 13:1–13:11

Scar: Verification-Based Development of Smart Contracts
Jonas Schiffl and Bernhard Beckert 14:1–14:13

Preface

This volume contains the proceedings of the 6th International Workshop on Formal Methods for Blockchains (FMBC 2025), to be held in Hamilton, Canada on May 04, 2025.

FMBC aims to bring together researchers and practitioners in the areas of formal methods and blockchain to promote a deeper understanding of how formal methods can be used for blockchain technology. Blockchain is a novel technology to store data in a decentralized way. Although the technology was originally invented to enable cryptocurrencies, it quickly found applications in several other domains. Since blockchains are often used to store financial transactions, bugs may result in huge economic losses and thus it is now of utmost importance to have strong guarantees of the behaviour of blockchain software. These guarantees can be brought by using formal methods. Indeed, blockchain software encompasses many topics of computer science where using formal methods techniques and tools is relevant: consensus algorithms to ensure the liveness and the security of the data on the chain, programming languages specifically designed to write smart contracts, cryptographic protocols, such as zero-knowledge proofs, used to ensure privacy, etc.

FMBC 2025 is the 6th International Workshop on Formal Methods for Blockchains, a series of workshops started in 2019. In past years, FMBC took place in Porto (2019, co-located with FM), online (2020 and 2021, co-located with CAV), Haifa (2022, co-located with CAV), and Luxembourg City (2024, co-located with ETAPS). This year FMBC attracted 18 submissions covering different areas of formal methods for blockchains. Each paper was reviewed by at least three reviewers and the Program Committee accepted 9 regular long papers and 3 tool papers.

FMBC 2025 would not have been possible without the deep investment and involvement of many supporters. We would like to express our gratitude to all the authors who submitted their work to the conference, the Steering Committee members who provided precious guidance and support, all the colleagues who served on the Program Committee, as well as the external reviewers, whose professional and efficient work during the review process helped us to produce a high-quality conference program. Particular thanks are given to the invited speakers, Julian Sutherland from Nethermind and Wolfgang Grieskamp from Aptos, for their willingness to talk about their research and share their perspective about formal methods for blockchains. The abstracts of the invited talks and a short bio of the speakers are included in this volume as well.

FMBC 2025 is co-located with ETAPS 2025, hosted and sponsored by McMaster University, Canada. Many thanks to all the local organizers and in particular to Alan Wassyng and Angelo Gargantini, Workshop Chairs of ETAPS 2025, for their help and guidance. FMBC 2025 was financially supported by Aptos and Movement Labs.

April 2025

Diego Marmsoler
Meng Xu

APTOS

Movement {LABS}

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Program Committee Chairs

Diego Marmsoler
University of Exeter

Meng Xu
University of Waterloo

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu

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

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu

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

Steering Committee

Bruno Bernardo
Nomadic Labs

Diego Marmsoler
University of Exeter

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu

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

Program Committee

Massimo Bartoletti
University of Cagliari

Bernhard Beckert
Karlsruhe Institute of Technology

Franck Cassez
Movement Labs

Denisa Diaconescu
University of Bucharest

Maurice Herlihy
Brown University

Sebastian Holler
Max Planck Institute for Security and Privacy

Enrico Lipparini
University of Genoa

Fan Long
University of Toronto

Orestis Melkonian
Input Output (IOG)

Baoluo Meng
GE Aerospace Research

Burcu Kulahcioglu Ozkan
Delft University of Technology

Gordon Pace
University of Malta

Vincent Rahli
University of Birmingham

Sophie Rain
TU Wien

Augusto Sampaio
Federal university of Pernambuco

Derek Sorensen
Certora

Bas Spitters
Aarhus University

Meng Sun
Peking University

Mark Utting
The University of Queensland

Adele Veschetti
TU Darmstadt

Christoph Weidenbach
Max Planck Institute for Informatics

Teng Zhang
Aptos Labs

6th International Workshop on Formal Methods for Blockchains (FMBC 2025).
Editors: Diego Marmsoler and Meng Xu

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

Supporting Reviewers

Sarat Chandra Varanasi

Terru Stübinger