# Lecture Notes in Computer Science 11222

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7408

Kyungmin Bae · Peter Csaba Ölveczky (Eds.)

# Formal Aspects of Component Software

## 15th International Conference, FACS 2018
## Pohang, South Korea, October 10–12, 2018
## Proceedings

Springer

*Editors*
Kyungmin Bae
Pohang University of Science
and Technology
Pohang
South Korea

Peter Csaba Ölveczky
University of Oslo
Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-02145-0 ISBN 978-3-030-02146-7 (eBook)
https://doi.org/10.1007/978-3-030-02146-7

Library of Congress Control Number: 2018957278

LNCS Sublibrary: SL2 – Programming and Software Engineering

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This volume contains the proceedings of the 15th International Conference on Formal Aspects of Component Software (FACS 2018), held at Pohang University of Science and Technology (POSTECH), Korea, during October 10–12, 2018.

Component-based software development proposes sound engineering principles and techniques to cope with the complexity of present-day software systems. However, many challenging conceptual and technological issues remain in component-based software development theory and practice. Furthermore, the advent of service-oriented and cloud computing, cyber-physical systems, and the Internet of Things has brought to the fore new dimensions, such as quality of service and robustness to withstand faults, which require revisiting established concepts and developing new ones.

The FACS series of events addresses the application of formal methods in all aspects of software components and services. Formal methods have provided foundations for component-based software through research on mathematical models for components, composition and adaptation, and rigorous approaches to verification, deployment, testing, and certification.

FACS 2018 received 32 regular and tool paper submissions. All but four submissions were reviewed by at least three reviewers. Based on the reviews and extensive discussions, the program committee decided to accept 12 regular papers and two tool papers. This volume contains those 14 papers, an invited paper by Edward A. Lee, and an abstract of an invited talk by Grigore Rosu.

Many colleagues and friends contributed to FACS 2018. We thank Edward A. Lee and Grigore Rosu for accepting our invitations to give invited talks, and the authors who submitted their work to FACS 2018. We are grateful to the members of the program committee for providing timely and insightful reviews as well as for their involvement in the post-reviewing discussions. We also thank the members of the FACS steering committee for their useful suggestions. Finally, we thank Saron Kim and Moonhyeon Jung for their assistance in organizing FACS 2018, and acknowledge financial support from the Brain Korea 21 Plus program and the POSTECH Basic Science Research Institute.

August 2018

Kyungmin Bae
Peter Csaba Ölveczky

# Organization

## Program Chairs

| | |
|---|---|
| Kyungmin Bae | Pohang University of Science and Technology, Korea |
| Peter Csaba Ölveczky | University of Oslo, Norway |

## Steering Committee

| | |
|---|---|
| Farhad Arbab | CWI and Leiden University, The Netherlands |
| Luís Barbosa | INESC TEC and University of Minho, Portugal |
| José Luiz Fiadeiro | Royal Holloway, University of London, UK |
| Ramtin Khosravi | University of Tehran, Iran |
| Olga Kouchnarenko | FEMTO-ST and University of Franche-Comté, France |
| Zhiming Liu | Southwest University, China |
| Markus Lumpe | Swinburne University of Technology, Australia |
| Eric Madelaine (Chair) | Inria and University of Côte d'Azur, Sophia Antipolis, France |
| Peter Csaba Ölveczky | University of Oslo, Norway |
| José Proença | University of Minho, Portugal |

## Program Committee

| | |
|---|---|
| Farhad Arbab | CWI and Leiden University, The Netherlands |
| Cyrille Artho | KTH Royal Institute of Technology, Sweden |
| Kyungmin Bae | Pohang University of Science and Technology, Korea |
| Luís Barbosa | INESC TEC and University of Minho, Portugal |
| Simon Bliudze | Inria Lille, France |
| Roberto Bruni | University of Pisa, Italy |
| Zhenbang Chen | National University of Defense Technology, China |
| Yunja Choi | Kyungpook National University, Korea |
| José Luiz Fiadeiro | Royal Holloway, University of London, UK |
| Xudong He | Florida International University, USA |
| Sung-Shik Jongmans | The Open University, The Netherlands |
| Yunho Kim | KAIST, Korea |
| Olga Kouchnarenko | FEMTO-ST and University of Franche-Comté, France |
| Ivan Lanese | University of Bologna/Inria, Italy |
| Axel Legay | Inria Rennes, France |
| Shaoying Liu | Hosei University, Japan |
| Zhiming Liu | Southwest University, China |
| Markus Lumpe | Swinburne University of Technology, Australia |
| Eric Madelaine | Inria and University of Côte d'Azur, Sophia Antipolis, France |

| | |
|---|---|
| Hernán Melgratti | University of Buenos Aires, Argentina |
| José Meseguer | University of Illinois at Urbana-Champaign, USA |
| Kazuhiro Ogata | JAIST, Japan |
| Peter Csaba Ölveczky | University of Oslo, Norway |
| Catuscia Palamidessi | Inria, France |
| José Proença | University of Minho, Portugal |
| Gwen Salaün | University of Grenoble Alpes, France |
| Francesco Santini | University of Perugia, Italy |
| Meng Sun | Peking University, China |
| Antonio Vallecillo | University of Málaga, Spain |
| Dániel Varró | McGill University, Canada, and Budapest University of Technology and Economics, Hungary |
| Shoji Yuen | Nagoya University, Japan |
| Min Zhang | East China Normal University, China |

## Additional Reviewers

Chen, Xin
Chirita, Claudia
Chouali, Samir
Cristescu, Ioana
Dadeau, Frederic
Koutsoukos, Giorgios
Krishna, Ajay
Li, Yi
Liu, Bo
Masson, Pierre-Alain
Quilbeuf, Jean
Zhang, Xiyue

# Formal Design, Implementation and Verification of Blockchain Languages (Abstract of Invited Paper)

Grigore Rosu[1,2]

[1] University of Illinois at Urbana-Champaign, USA
grosu@illinois.edu
http://fsl.cs.illinois.edu/grosu
[2] Runtime Verification, Inc., USA
grigore.rosu@runtimeverification.com

**Abstract.** Many of the recent cryptocurrency bugs and exploits are due to flaws or weaknesses of the underlying blockchain programming languages or virtual machines. The usual post-mortem approach to formal language semantics and verification, where the language is firstly implemented and used in production for many years before a need for formal semantics and verification tools naturally arises, simply does not work anymore. New blockchain languages or virtual machines are proposed at an alarming rate, followed by new versions of them every few weeks, together with programs (or smart contracts) in these languages that are responsible for financial transactions of potentially significant value. Formal analysis and verification tools are therefore needed immediately for such languages and virtual machines. We present recent academic and commercial results in developing blockchain languages and virtual machines that come directly equipped with formal analysis and verification tools. The main idea is to generate all these automatically, correct-by-construction from a formal specification. We demonstrate the feasibility of the proposed approach by applying it to two blockchains, Ethereum and Cardano.

**Keywords:** Formal verification · Formal semantics · Blockchain

## Links

Runtime Verification, Inc:

- http://runtimeverification.com

Smart contract verification approach and verified contracts:

- https://runtimeverification.com/smartcontract/
- https://github.com/runtimeverification/verified-smart-contracts

Supported in part by NSF grant CCF-1421575, NSF grant CNS-1619275, and an IOHK (http://iohk.io) gift.

Formally specified, automatically generated virtual machines for the blockchain:

- EVM: https://github.com/runtimeverification/evm-semantics
- IELE: https://github.com/runtimeverification/iele-semantics

# Contents

## Invited Paper

## Regular Papers

**Tool Papers**