Workshop on Byzantine Consensus and Resilient Blockchains (BCRB '18)

Alysson Bessani
Universidade de Lisboa
Portugal
anbessani@fc.ul.pt

Hans P. Reiser
University of Passau
Germany
hans.reiser@uni-passau.de

Marko Vukolić
IBM Zurich
Switzerland
mvu@zurich.ibm.com

Tobias Distler
FAU Erlangen-Nürnberg
Germany
distler@cs.fau.de

Overview

The ability to cope with random faults, unexpected disruptions, and targeted attacks is an increasingly important aspect of dependable systems, which is why Byzantine fault tolerance has become an active field of research in the past two decades. With new application scenarios and technologies such as trusted-computing hardware features, the Internet of Things, and Industry 4.0 emerging, existing approaches towards Byzantine consensus (i.e., Byzantine fault-tolerant replication) need to be revisited. Most notably, this is true with regard to a novel use case of Byzantine consensus that promises a revolution in several aspects of our society: resilient blockchains.

The *Workshop on Byzantine Consensus and Resilient Blockchains (BCRB '18)* gives researchers a forum to promote and discuss ideas on open challenges in the domain of Byzantine consensus in general and resilient blockchains as well as distributed ledgers in particular. In an effort to foster discussion and information exchange between the two (overlapping) communities, the workshop furthermore aims at determining new application areas for Byzantine fault tolerance and blockchain. Apart from elaborating on further use cases, BCRB '18 gives researchers an opportunity to present system support and techniques for improving the resilience and scalability of Byzantine fault-tolerant systems, for example, by exploiting recently developed hardware mechanisms. Finally, the workshop provides a platform to identify new threat and attack scenarios for Byzantine consensus and blockchain technologies, and to discuss open problems and possible future research directions.

Program Committee

The Program Committee of the BCRB '18 workshop consisted of the following members from academia and industry:

- Eduardo Alchieri (Universidade de Brasília)
- Lorenzo Alvisi (Cornell University)
- Pierre-Louis Aublin (Imperial College London)
- Rune Aune (Symbiont)
- Massimo Bartoletti (Università degli Studi di Cagliari)
- Miguel Correia (Universidade de Lisboa)
- Ittay Eyal (Technion)
- Franz J. Hauck (Ulm University)
- Rüdiger Kapitza (TU Braunschweig)
- Marcelo Pasin (Université de Neuchâtel)
- Francois Taiani (Université de Rennes 1 - ESIR / IRISA)
- Jiangshan Yu (University of Luxembourg)

Presentations

BCRB '18 has welcomed contributions in two categories: (1) *full research papers* presenting previously unpublished work, which are included in the workshop proceedings, and (2) *short research statements* summarizing existing work or outlining new ideas. Based on the recommendations provided by the reviewers, seven research papers and five research statements were selected for presentation at the workshop. The accepted contributions cover a wide spectrum of topics that can be divided into the following four main areas of research:

Improving Performance and Scalability. Four presentations target the problem of enhancing the performance of systems based on Byzantine fault-tolerant state-machine replication. Topics include the use of remote direct memory access for inter-replica communication, the visualization of distributed systems to identify bottlenecks, a technique to implement dynamic partitioning of application state, as well as the optimized selection of a leader replica in wide-area environments.

Resilience of Blockchains Against Attacks. Three presentations analyze different weaknesses of blockchain protocols, studying network-level attacks on Bitcoin and proposing solutions for enhancing network privacy as well as for improving the resilience of early-stage proof-of-work-based blockchains.

Formal Methods for Blockchains. Two presentations argue for the need of formal methods to verify the correctness of blockchains, thereby identifying specific challenges that typically arise when protocols are not formally specified and discussing new ideas towards probabilistic model checking.

Smart Contracts. Three presentations focus on different aspects of smart contracts as, for example, provided by the Ethereum blockchain. Apart from a study analyzing multiple techniques to improve scalability by partitioning Ethereum's blockchain graph, there are also presentations on a tool that automates the search for vulnerabilities in Ethereum, and on how to engineer smart contracts for cyber-physical systems.

In addition to these talks, the BRCB '18 program includes a keynote by Paulo Veríssimo (University of Luxembourg).

Acknowledgments

We would like to thank all authors who submitted to BCRB '18 for their contributions, and the Program Committee members and external reviewers, Tiziana Cimoli and Anaïs Durand, for their valuable feedback. Furthermore, we are grateful to Johannes Köstler for his support as Web and Publication Chair.