4th International Conference on Blockchain Economics, Security and Protocols

Tokenomics 2022, December 12–13, 2022, Paris, France

Edited by

Yackolley Amoussou-Guenou
Aggelos Kiayias
Marianne Verdier

Editors

Yackolley Amoussou-Guenou
Université Paris-Panthéon-Assas, CRED, Paris, France
Yackolley.Amoussou-Guenou@u-paris2.fr

Aggelos Kiayias
University of Edinburgh, UK
IOG, Edinburgh, UK
Aggelos.Kiayias@ed.ac.uk

Marianne Verdier
Université Paris-Panthéon-Assas, CRED, Paris, France
marianne.verdier@u-paris2.fr

ACM Classification 2012
Theory of computation → Distributed algorithms; Security and privacy → Cryptography; Mathematics of computing → Mathematical analysis

ISBN 978-3-95977-274-7

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/978-3-95977-274-7.

Publication date
July, 2023

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/OASIcs.Tokenomics.2022.0

ISBN 978-3-95977-274-7 **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.

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
Yackolley Amoussou-Guenou, Aggelos Kiayias, and Marianne Verdier 0:vii

List of Authors
..... 0:ix

Program Committee
..... 0:xi

Invited Talks

Algorithmic Game Theory and Blockchains
Elias Koutsoupias 1:1–1:2

How Blockchain Tokens Are Changing Platform Economics
Hanna Halaburda 2:1–2:7

Regular Papers

1DLT: Rapid Deployment of Secure and Efficient EVM-Based Blockchains
Simone Bottoni, Anwitaman Datta, Federico Franzoni, Emanuele Ragnoli, Roberto Ripamonti, Christian Rondanini, Gokhan Sagirlar, and Alberto Trombetta 3:1–3:15

Consistency of Automated Market Makers
Vincent Danos and Weijia Wang 4:1–4:12

Interest Rate Rules in Decentralized Finance: Evidence from Compound
Amit Chaudhary, Roman Kozhan, and Ganesh Viswanath-Natraj 5:1–5:6

Maximal Extractable Value (MEV) Protection on a DAG
Dahlia Malkhi and Pawel Szalachowski 6:1–6:17

Extended Abstracts

Commit-Reveal Schemes Against Front-Running Attacks
Andrea Canidio and Vincent Danos 7:1–7:5

The Demand for Programmable Payments: Extended Abstract
Charles M. Kahn and Maarten R.C. van Oordt 8:1–8:1

4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2022).
Editors: Yackolley Amoussou-Guenou, Aggelos Kiayias, and Marianne Verdier
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

This volume includes the published papers of Tokenomics 2022, the fourth edition of the International Conference on Blockchain Economics, Security and Protocols which took place on December 12^{th} – 13^{th} 2022 and was hosted at Sorbonne Université, Paris, France.

Tokenomics is an international forum for theory, design, analysis, implementation and applications of blockchains and smart contracts. The goal of the conference is to bring together economists, computer science researchers and practitioners working on blockchains in a unique program featuring outstanding invited talks and academic presentations.

Following the tradition since its very beginning, the Program Committee of the conference was divided into two complementary sub-committees. The *Distributed Computing* sub-committee consisted of 23 expert computer science researchers, chaired by Aggelos Kiayias, and the *Economics* sub-committee consisted of 28 expert economics researchers, and was chaired by Marianne Verdier, with Yackolley Amoussou-Guenou as co-chair.

In total there were 55 submissions for consideration 11 mainly targeted to the distributed computing sub-committee and 44 mainly targeted toward the economics sub-committee. On average, submissions toward the distributed computing sub-committee got three reviews each, and submissions to the economics sub-committee got two reviews each. After the collection of all the reviews from the program committee members, the program committee chairs met to choose the accepted papers for the conference, and, given the reviews, took into account some constraints such as the topic of the papers. We would like to mention that the selection was done irrespective to which sub-committee they were submitted to. The objective was to have presentations fitting the goals of the conference and create interdisciplinary and coherent sessions. The program committee deliberations concluded with 16 papers being accepted for the final program, ranging from studies of consensus protocols to distributed applications. We give below the list of the contributions presented by session.

- MEV and front-running. This session grouped papers analyzing the problem of front-running attacks in distributed applications. In particular the papers studied different ways to mitigate them. It consisted of the following presentations: "*Credible Decentralized Exchange Design via Verifiable Sequencing Rules*" by Ferreira and Parkes; "*The Evolution of Blockchain: From Public to Private Mempools*" by Jia, Capponi and Wang; and "*Commitment Against Front Running Attacks*" by Canidio and Danos.
- DeFi. In this session the presentations analyzed different aspects of decentralised finance and possible ways to improve them. It consisted of the following presentations: "*The Need for Fees at a DEX: How Increases in Fees Can Increase DEX Trading Volume*" by Hasbrouck, Rivera, and Saleh; "*Interest Rate Parity in Decentralized Finance*" by Chaudhary, Kozhan, and Viswanath-Natraj; and "*Token Incentives and Platform Competition: a Tale of two swaps*" by Liu, Chen, and Zhu.
- Blockchain, CBDC and Payments. This session covered various presentations related to central bank digital currencies (CBDC), payments platforms, and user adoption of innovative payment instruments. It consisted of the following presentations: "*The Demand for Programmable Payments*" by Kahn and van Oort; "*CBDC and Payment Platform Competition*" by Liu, Reshidi, and Rivadeneyra; and "*Central Bank Digital Currency and Banking Choice: The Impact of Service Location*" by Usher, Li, and Zhu.
- Smart contracts, oracles and AMMs. The presentations of this session were about smart contracts. In particular, some works studied the functioning of automated market makers from a theoretical perspective, and the last presentation exposed why truth-telling cannot

4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2022).
Editors: Yackolley Amoussou-Guenou, Aggelos Kiayias, and Marianne Verdier
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

always be guaranteed with oracles. It consisted of the following presentations: "*Axioms for Constant Function AMMs*" by Schlegel and Mamageishvili; "*Consistency of automated market makers*" by Danos and Wang; and "*An Impossibility Theorem on Truth-Telling in Fully Decentralized Systems*" by Garratt and Monnet.

- Efficiency of Blockchain protocols. This session focused on improving the efficiency and the analytical tools for blockchain (or more broadly, consensus) protocols. It consisted of the following presentations: "*Equilibrium Staking Levels in a Proof-of-Stake Blockchain*" by John, Rivera, and Saleh; "*Maximal Extractable Value (MEV) Protection on a DAG*" by Malkhi and Szalachowski; "*An Economic Model of Consensus on Distributed Ledgers*" by Halaburda, He, and Li; and "*QPQ 1DLT: A System For the Rapid Deployment of Secure and Efficient EVM-Based Blockchains*" by Bottoni, Datta, Franzoni, Ragnoli, Ripamonti, Rondanini, Sagirlar, and Trombetta.

At the end of the conference, on the basis of an assessment of the content of the article as well as the presentation, Charles Kahn and Maarten van Oort received the best-paper prize for their paper on "*The Demand for Programmable Payments*", thanks to the sponsoring of Keyrock.[1]

In addition to the accepted papers, the program included three stimulating keynote presentations. The topics were chosen after discussing with the speakers about three important directions for future research: the regulation of cryptoassets, the role of tokens in shaping firms' incentives to adopt a platform business model, and the analysis of the players' strategies via the use of algorithmic game theory. Claudine Hurman (Banque de France, France), director of Infrastructures, Innovation and Payments Regulating crypto-assets and experimenting at the French central bank presented "*CBDC: two sides of the same coin*"; Hanna Halaburda (New York University, Stern School of Business, USA) presented "*How Blockchain Tokens are Changing Platform Economics*"; and Elias Koutsoupias (Oxford University, UK), 2012 Gödel prize, presented "*Algorithmic game theory and blockchains*".

Overall, the topical works presented at the conference, as well as the numerous interactions (also between different disciplines), make us think that the conference was a success. We hope this venue will continue fostering interactions between economists, computer science researchers and practitioners, and will further stimulate interdisciplinary research in the broader area.

We are grateful to the sponsors of this fourth edition of the Tokenomics conference: the Blockchain@Polytechnique chair, the Finance Digitale chair, Keyrock, IOG, and the LIP6, Sorbonne Université.

We would like to thank the authors for submitting their work to the conference and the program committee members who worked very hard in reviewing papers and giving feedback to the authors. We are grateful for their help in building this great program. A special thanks to all the presenters for their well prepared and clear presentations, and to the audience for all the discussions that took place. We also thank all the volunteers who helped the conference run smoothly.

Last but not least, we would like to thank Julien Prat and Maria Potop-Butucaru, the general co-chairs of Tokenomics 2022 for their help and advice for the organization of the conference.

Aggelos, Marianne, and Yackolley

[1] Keyrock (`https://keyrock.eu/`) sponsored the best paper award, as part of having industrial practitioners at the conference, one of the conference's goals.

List of Authors

Simone Bottoni (3)
RTM, Lugano, Switzerland

Andrea Canidio (7)
IMT School for Advanced Studies, Lucca, Italy;
CoW Protocol, Paris, France

Amit Chaudhary (5)
Warwick Business School, University of Warwick, Coventry, UK

Vincent Danos (4, 7)
CNRS, Paris, France;
DI ENS, INRIA, PSL, Paris, France

Anwitaman Datta (3)
Nanyang Technological University, Singapore, Singapore

Federico Franzoni (3)
Unaffiliated Researcher, Barcelona, Spain

Hanna Halaburda (2)
Stern School of Business, New York University, NY, USA

Charles M. Kahn (8)
Department of Finance, University of Illinois, Urbana-Champaign, IL, USA

Elias Koutsoupias (1)
University of Oxford, UK

Roman Kozhan (5)
Warwick Business School, University of Warwick, Coventry, UK

Dahlia Malkhi (6)
Chainlink Labs, UK

Maarten R.C. van Oordt (8)
Tinbergen Institute, Amsterdam,
The Netherlands;
Vrije Universiteit Amsterdam, The Netherlands

Emanuele Ragnoli (3)
RTM, Lugano, Switzerland

Roberto Ripamonti (3)
RTM, Lugano, Switzerland

Christian Rondanini (3)
RTM, Lugano, Switzerland

Gokhan Sagirlar (3)
RTM, Lugano, Switzerland

Pawel Szalachowski (6)
Chainlink Labs, UK

Alberto Trombetta (3)
Insubria University, Varese, Italy

Ganesh Viswanath-Natraj (5)
Warwick Business School, University of Warwick, Coventry, UK

Weijia Wang (4)
ENS, Paris, France

4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2022).
Editors: Yackolley Amoussou-Guenou, Aggelos Kiayias, and Marianne Verdier
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Program Committee

General Chairs

- Julien Prat, ENSAE, CREST, Ecole Polytechnique
- Maria Potop-Butucaru, LIP6, Sorbonne Université

Distributed Computing

- Aggelos Kiayias, University of Edinburgh and IOG (Chair)
- Elli Androulaki, IBM Research – Europe
- Vincent Danos, CNRS
- Ittay Eyal, Technion
- Matheus Xavier Ferreira, Harvard
- Juan Garay, Texas A&M University
- Arthur Gervais, Imperial College
- Maurice Herlihy, Brown University and Algorand
- Dimitris Karakostas, University of Edinburgh
- William J. Knottenbelt, Imperial College
- Philip Lazos, IOG
- Andrew Lewis-Pye, London School of Economics
- Francisco Marmolejo, Harvard
- Tal Rabin, University of Pennsylvania and Algorand Foundation
- Tim Roughgarden, Columbia University and a16z Crypto
- Jan Christoph Schlegel, City University of London
- David Siska, University of Edinburgh
- Qiang Tang, University of Sydney
- Vanessa Teague, Thinking Cybersecurity
- Sara Tucci-Piergiovanni, CEA-LIST, Université Paris-Saclay
- Catherine Tucker, MIT Chryssis Georgiou, University of Cyprus
- Dimitrios Vasilopoulos, IMDEA Software Institute
- Dionysis Zindros, Stanford

Economics

- Marianne Verdier, Université Paris-Panthéon-Assas (chair)
- Yackolley Amoussou-Guenou, Université Paris-Panthéon-Assas (co-chair)
- Arash Aloosh, NEOMA Business School
- Vlad Babich, Georgetown University
- Christophe Bisière, Toulouse School of Economics
- Matthieu Bouvard, Toulouse School of Economics
- Agostino Capponi, Columbia University
- Catherine Casamatta, Toulouse School of Economics
- Jonathan Chiu, Bank of Canada
- Will Cong, Cornell University
- Bertrand Crettez, Université Paris-Panthéon-Assas
- Michele Fabi, ENSAE, CREST, Ecole Polytechnique
- Rod Garratt, BIS
- Guillaume Haeringer, Baruch College

4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2022).
Editors: Yackolley Amoussou-Guenou, Aggelos Kiayias, and Marianne Verdier
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- Zhiguo He, University of Chicago
- Samuel Haefner, Web 3.0 Technologies Foundation
- Gur Huberman, Columbia University
- Thorsten Koeppl, Queens University
- Jiasun Li, George Mason University
- Simon Mayer, HEC
- Julien Prat, ENSAE, CREST, Ecole Polytechnique
- Mariana Rojas Breu, Université Paris-Panthéon-Assas
- Fahad Saleh, Wake Forest University
- Linda Schilling, Washington University in St Louis
- Alexander Teytelboym, Dept of economics, University of Oxford
- Katrin Tinn, McGill University
- Marteen Van Oord, Vrije University Amsterdam
- Russell Wang, Federal Reserve Bank of Richmond
- Luana Zaccaria, EIEF
- Marius Zoican, University of Toronto