2nd International Conference on Blockchain Economics, Security and Protocols

Tokenomics 2020, October 26–27, 2020, Toulouse, France

Edited by

Emmanuelle Anceaume
Christophe Bisière
Matthieu Bouvard
Quentin Bramas
Catherine Casamatta

Editors

Emmanuelle Anceaume
CNRS, IRISA, Rennes, France
Emmanuelle.Anceaume@irisa.fr

Christophe Bisière
Toulouse School of Economics, University Toulouse Capitole, TSM-R, France
christophe.bisiere@tse-fr.eu

Matthieu Bouvard
Toulouse School of Economics, University Toulouse Capitole, TSM-R, France
matthieu.bouvard@tse-fr.eu

Quentin Bramas
ICUBE, University of Strasbourg, France
bramas@unistra.fr

Catherine Casamatta
Toulouse School of Economics, University Toulouse Capitole, TSM-R, France
catherine.casamatta@tse-fr.eu

ACM Classification 2012
Computing methodologies → Distributed algorithms; Security and privacy → Distributed systems security; Applied computing → Economics

ISBN 978-3-95977-157-3

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/978-3-95977-157-3.

Publication date
February, 2021

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 3.0 Unported license (CC-BY 3.0):
https://creativecommons.org/licenses/by/3.0/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.2020.0
ISBN 978-3-95977-157-3 **ISSN 1868-8969** **https://www.dagstuhl.de/oasics**

OASIcs – OpenAccess Series in Informatics

OASIcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. 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
Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta 0:vii–0:viii

Tokenomics 2020 Organization
..... 0:ix–0:x

Invited Talks

Some Economics of Fintech
Jean Tirole 1:1–1:1

When Nakamoto Meets Nash: Blockchain Breakthrough Through the Lens of Game Theory
Ittai Abraham 2:1–2:1

Digital Currencies as Types
Timothy A. K. Zakian 3:1–3:1

Regular Papers

On Fairness in Committee-Based Blockchains
Yackolley Amoussou-Guenou, Antonella Del Pozzo, Maria Potop-Butucaru, and Sara Tucci-Piergiovanni 4:1–4:15

Decentralization in Open Quorum Systems: Limitative Results for Ripple and Stellar
Andrea Bracciali, Davide Grossi, and Ronald de Haan 5:1–5:20

VeriOSS: Using the Blockchain to Foster Bug Bounty Programs
Andrea Canidio, Gabriele Costa, and Letterio Galletta 6:1–6:14

A Foundation for Ledger Structures
Chad Nester 7:1–7:13

Parasite Chain Detection in the IOTA Protocol
Andreas Penzkofer, Bartosz Kusmierz, Angelo Capossele, William Sanders, and Olivia Saa 8:1–8:18

Implementation Study of Two Verifiable Delay Functions
Vidal Attias, Luigi Vigneri, and Vassil Dimitrov 9:1–9:14

Short Papers

Revisiting the Liquidity/Risk Trade-Off with Smart Contracts
Vincent Danos, Jean Krivine, and Julien Prat 10:1–10:5

2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020).
Editors: Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Proof of Behavior
Paul-Marie Grollemund, Pascal Lafourcade, Kevin Thiry-Atighehchi, and Ariane Tichit 11:1–11:6

Blockguard: Adaptive Blockchain Security
Shishir Rai, Kendric Hood, Mikhail Nesterenko, and Gokarna Sharma 12:1–12:5

Welcome to the Jungle: A Reference Model for Blockchain, DLT and Smart-Contracts
Julien Hatin, Emmanuel Bertin, Baptiste Hemery, and Nour El Madhoun 13:1–13:5

Preface

This volume includes the published papers of Tokenomics 2020, the second edition of the International Conference on Blockchain Economics, Security and Protocols.

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.

The conference was initially planned on May 11^{th} and 12^{th}, 2020. Due to the COVID-19 pandemic, it eventually took place on October 26^{th} and 27^{th} of the same year at Toulouse School of Economics (TSE) in an hybrid format with some of the speakers and moderators presenting in front of an audience in TSE new buidling and the other conference participants joining through videoconferencing.

For this second edition, there were 45 papers submitted: 12 papers in computer science (11 as regular papers and 1 as a short paper) and 32 papers in economics. The economics program committee selected 14 papers for presentation at the conference. The computer science program committee selected 6 regular papers for presentation at the conference and publication in this volume. Additionally, 4 submissions were accepted as short papers, for presentation at the conference and publication in this volume.

In addition to accepted papers, we had the pleasure to welcome four distinguished invited keynote speakers:

- Ittai Abraham, senior researcher at vmware research. Abraham discussed the use of game theoretical tools into computer science to model blockchains and cryptocurrencies
- Long Chen, Secretary-General of the Luohan Academy, an open research institute initiated by Alibaba, and former Chief Strategy Officer at Ant Financial. Chen gave an overview of the ongoing changes in financial services driven by progresses in information technologies.
- Jean Tirole, Researcher at TSE and 2014 laureate of the Sveriges Riksbank prize in economic sciences in memory of Alfred Nobel. Tirole discussed the challenges faced by cryptocurrencies using the framework of economic theory.
- Timothy Zakian, Software Engineer, Novi, Facebook. Zakian presented Move, the programming language developed to implement transactions and smart contracts on the Libra blockchain.

Together with the computer science contributions gathered in these proceedings, the papers presented in the economics track tackled a wide range of issues reflecting the vitality of the research on blockchains and cryptocurrencies in economics. This growing interest reflects the current and potential impact of blockchain-based applications for consumers, businesses and governments. It also captures a fundamental feature of blockchains: implementing a distributed consensus is as much an incentive problem as it is a technological challenge.

A first subset of these papers focuses on the functioning of the blockchain itself. In keeping with an earlier stream of papers in computer sciences and economics, Ebrahimi, Routledge and Zetlin-Jones ("Getting Blockchain Incentives Right") use game theory to analyze miners' equilibrium strategies under proof of work and the possibility they may fail to ensure consensus. Amoussou-Guenou, Biais, Potop-Butucaru and Tucci-Piergiovanni ("Rational vs Byzantine Players in Consensus-based Blockchains") use a similar game-theoretic toolbox to analyze the strategies of committee members in a Byzantine Fault Tolerant blockchain. Garatt and van Oordt ("Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies") show how miners' cost structure, notably the existence of sunk equipment costs, affect their

2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020).
Editors: Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

incentives to deploy hashpower in response to the cryptocurrency price movements. Finally, Hinzen, John and Saleh ("Bitcoin's Fatal Flaw: The Limited Adoption Problem") model how the information time lags inherent to fully distributed consensus create a hard technical constraint on the throughput of permissionless blockchains.

A second set of papers adopts an industrial organization approach to understand the distinctive features of blockchain-powered businesses. Lyandres ("Product Market Competition with Crypto Tokens and Smart Contracts") shows how native tokens and smart contracts alter the nature of the competition between an incumbent firm and a potential entrant. Cong, He and Wang ("Token-Based Platform Finance") combine the industrial organization angle with corporate finance implications: they evaluate the dual role of tokens as influencing users' adoption of a platform, and as providing entrepreneurs with a source of funding. Finally, Bakos and Halaburda ("When Do Smart Contracts and IoT Improve Efficiency? Automated Execution vs. Increased Information") draw on contract theory to clarify the capabilities of smart contracts. In particular, they distinguish between two features of smart contracts, the expansion of the contracting space thanks to IoT sensors and the automatization of the contract execution.

Last, a third set of papers approaches tokens from an asset pricing side. Pratt, Danos and Marcassa ("Reversible and Composable Financial Contracts") show how the value of utility tokens can be derived from users' benefits from immediately accessing the services of a platform. Dai, Jiang, Kou and Qin ("From Hotelling to Nakamoto: The Economic Meaning of Bitcoin Mining") propose a model that relates Bitcoin prices to miners' decisions to warehouse or sell the bitcoins they earn by confirming blocks. This model delivers quantitative predictions and is calibrated to the data. Shams ("The Structure of Cryptocurrency Returns") studies the comovement of multiple cryptocurrency prices and empirically connects high correlations to common demand factors. Finally, Benigno, Schilling and Uhlig ("Cryptocurrencies, Currency Competition, and the Impossible Trinity") study the implications of the adoption of a global cryptocurrency for monetary policies and exchange rates between fiat moneys.

Overall, the breadth of the topics explored by the participants to this conference illustrates the fruitful interaction between computer science and economics for understanding the implications of blockchain-based solutions. It also suggests much more ground to cover and we hope this conference will further stimulate research in this area.

We thank the authors for submitting their work at the conference and the program committee who worked hard in reviewing papers and giving feedback to the authors.

Catherine, Christophe, Emmanuelle, Matthieu and Quentin

Tokenomics 2020 Organization

General Chairs

Emmanuelle Anceaume, CNRS, Irisa (France)
Christophe Bisière, University Toulouse Capitole, TSE and TSM-R (France)
Matthieu Bouvard, University Toulouse Capitole, TSE and TSM-R (France)
Quentin Bramas, ICUBE, University of Strasbourg (France)
Catherine Casamatta, University Toulouse Capitole, TSE and TSM-R (France)

Program Committee

Computer Science

Emmanuelle Anceaume, CNRS, Irisa (France)
Daniel Augot, INRIA, Ecole Polytechnique (France)
Quentin Bramas, ICUBE, University of Strasbourg (France)
Vincent Danos, CNRS, Ecole Normale Supérieure (France)
Giuseppe Antonio Di Luna, Sapienza University of Rome (Italy)
Antonio Fernández Anta, IMDEA Networks (Spain)
Fabrice Le Fessant, OCaml PRO (France)
Juan A. Garay, Texas A&M University (USA)
Chryssis Georgiou, University of Cyprus (Cyprus)
Vincent Gramoli, The University of Sydney (Australia)
Braham Hamid, IRIT (France)
Maurice Herlihy, Brown University (USA)
Pascal Lafourcade, Université Clermont Auvergne (France)
Mario Larangeira, IOHK, Tokyo Institute of Technology (Japan)
Romaric Ludinard, IMT Atlantique (France)
Maria Potop-Butucaru, Sorbonne Université (France)
Leonardo Querzoni, Sapienza University of Rome (Italy)
François Taiani, Université Rennes 1, Irisa (France)
Sara Tucci-Piergiovanni, CEA LIST (France)
Marko Vukolic, IBM Research - Zurich (Switzerland)
Josef Widder, Interchain Foundation & TU Wien (Austria)

Economics

Bruno Biais, HEC Paris (France)
Christophe Bisière, University Toulouse Capitole, TSE and TSM-R (France)
Matthieu Bouvard, University Toulouse Capitole, TSE and TSM-R (France)
Catherine Casamatta, University Toulouse Capitole, TSE and TSM-R (France)
Jonathan Chiu, Bank of Canada (Canada)
Will Cong, Cornell University, Johnson Graduate School of Management (USA)
Guillaume Haeringer, Baruch College, Zicklin School of Business (USA)
Hanna Halaburda, New York University and Bank of Canada (USA & Canada)
Zhiguo He, University of Chicago, Booth School of Business (USA)

2nd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2020).
Editors: Emmanuelle Anceaume, Christophe Bisière, Matthieu Bouvard, Quentin Bramas, and Catherine Casamatta
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

0:x Tokenomics 2020 Organization

Emiliano Pagnotta, Imperial College Business School (U.K.)
Julien Pratt, CNRS and CREST (France)
Linda Shilling, Ecole Polytechnique and CREST (France)
Katrin Tinn, McGill University, Desautels Faculty of Management (Canada)
David Yermack, New York University, Stern School of Business (USA)