HAL
open science

International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019)

Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, Sara Tucci-Piergiovanni

To cite this version:

Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, Sara Tucci-Piergiovanni. International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019). Leibniz International Proceedings in Informatics , 71, 2020, OpenAccess Series in Informatics (OASIcs), 10.4230/OASIcs.Tokenomics.2019.0 . hal-03096247

HAL Id: hal-03096247

https://hal.science/hal-03096247

Submitted on 4 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

International Conference on Blockchain Economics, Security and Protocols

Tokenomics 2019, May 6–7, 2019, Paris, France

Edited by

Vincent Danos
Maurice Herlihy
Maria Potop-Butucaru
Julien Prat
Sara Tucci-Piergiovanni

OASICS

Editors

Vincent Danos
ENS, CNRS, PSL University, Paris, France
INRIA, Paris, France
Vincent.Danos@ens.fr

Maurice Herlihy
Brown University, Providence, RI, USA
mph@cs.brown.edu

Maria Potop-Butucaru
Sorbonne Université, Paris, France
maria.potop-butucaru@lip6.fr

Julien Prat
CREST, Ecole Polytechnique, Palaiseau, France
Julien.Prat@ensae.fr

Sara Tucci-Piergiovanni
CEA LIST, Palaiseau, France
sara.tucci@cea.fr

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

ISBN 978-3-95977-108-5

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/978-3-95977-108-5.

Publication date
March, 2020

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.2019.0
ISBN 978-3-95977-108-5 **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
Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci-Piergiovanni 0:vii

Keynote Lectures

Demystifying Blockchains: Decentralized and Fault-Tolerant Storage for the Future of Big Data?
Amr El Abbadi 1:1–1:1

Flexible BFT: Separating BFT Protocol Design from the Fault Model
Dahlia Malkhi 2:1–2:1

Regular Papers

A Puff of Steem: Security Analysis of Decentralized Content Curation
Aggelos Kiayias, Benjamin Livshits, Andrés Monteoliva Mosteiro, and Orfeas Stefanos Thyfronitis Litos 3:1–3:21

An Empirical Study of Speculative Concurrency in Ethereum Smart Contracts
Vikram Saraph and Maurice Herlihy 4:1–4:15

Atomic Appends: Selling Cars and Coordinating Armies with Multiple Distributed Ledgers
Antonio Fernández Anta, Chryssis Georgiou, and Nicolas Nicolaou 5:1–5:16

A Smart Contract Oracle for Approximating Real-World, Real Number Values
William George and Clément Lesaege 6:1–6:15

Cryptocurrency Egalitarianism: A Quantitative Approach
Dimitris Karakostas, Aggelos Kiayias, Christos Nasikas, and Dionysis Zindros 7:1–7:21

The Stability and the Security of the Tangle
Quentin Bramas 8:1–8:15

The Impact of Ethereum Throughput and Fees on Transaction Latency During ICOs
Michael Spain, Sean Foley, and Vincent Gramoli 9:1–9:15

F1 Fee Distribution
Dev Ojha and Christopher Goes 10:1–10:6

Selfish Mining and Dyck Words in Bitcoin and Ethereum Networks
Cyril Grunspan and Ricardo Pérez-Marco 11:1–11:10

B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics
Silvia Bonomi, Marco Casini, and Claudio Ciccotelli 12:1–12:15

MixEth: Efficient, Trustless Coin Mixing Service for Ethereum
István András Seres, Dániel A. Nagy, Chris Buckland, and Péter Burcsi 13:1–13:20

International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019).
Editors: Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci-Piergiovanni
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

Blockchains enable new trust architectures. These architectures are not just distributed but they are also *decentralised*. This means that no single person or entity is specifically in charge of running the system – no one runs the show. Instead, the system is arranged in a way that many *unrelated* agents are collectively in charge. From their collective effort emerges ideally a perfect and transparent trusted third party. It is not easy to organise the production of such a decentralised resource. It is the work of the blockchain engine – or consensus algorithm – to keep the many operators with consistent views of the system and to make the system reliable and dependable. Systems built in this way offer no specific point of failure – so the story goes. For the same reason, they are hard and costly to attack, as the adversary needs to recruit massive resources to coordinate sufficiently many agents to take over the system.

Blockchains have been around for some time now and continue to grow in use and in diversity of services and underpinning mechanisms. There are many trust engines – each with different trade-offs between various criteria of performance and various levels of maturity. The creativity in the field is truly staggering and a consequence of its openness. Note that openness is a natural correlate of decentralisation: if the system is closed, it is the beginning of an inventory of the various agents and one eventually will come to know who they are. People love openness as they have direct access to the levers of governance/consensus and monetary policies, things most people never get to see in a lifetime except when playing video games maybe. This combination of openness and of having a computational substrate opens up new algorithmic economic spaces. Voting, allocation, rewards, monetary policies, pricing cascades, tax systems everything is up for reinvention in a framework where everything can be seen and everyone sees that rules are correctly applied. In this enthusiastic universe we have already seen crises, collapses, and subsequent evolution. We have now some data points and an incipient understanding of what works and what not.

However, there are many things the field still needs to improve. One which is most frequently mentioned is the need to *scale up* decentralised systems to a level comparable to that of the traditional trust systems they purport to replace (at least in part). Another one is the ability to offer *confidentiality-preserving* modes of operation as the need of secrecy is often a necessity in business transactions. Also it would help if the price of the collective computational resource was lower (compared to centralised cloud computing) and more predictable.

But there are other pressing and perhaps more difficult questions. No matter what technique is used for consensus, it all relies on a key assumption: namely that the multiple agents in charge are *independent* or approximately so - and will therefore act neutrally with respect to the users and be only driven by their own interests. Agents do not collude - it is assumed. The trust therefore derives not from traditional *reputation-and-regulation* mechanisms but from this neutrality postulate on which everything blockchain hinges. For this assumption to be realistic, one needs many agents - so many that no actor can summon enough resources to corrupt or otherwise control a sufficiently large subset of the agents of the system.

It follows that such systems are harder to update and to set back on a good course should there be a problem. It is a logical necessity that the system has no single point of accountability. It is also hard to repair or amend a system with many independent operators. One needs means of coordination and yet no means of collusion. It sounds difficult and it is!

International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019).
Editors: Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci-Piergiovanni
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

One fundamental need of the economic world may be a need for some level of reversibility that is hard to combine with decentralised mechanisms. Another aspect of the coordination-without-collusion problem is that there is not even the common legally operative notion of a "one" agent - meaning the various software agents (commonly called nodes, miners, block makers, and users) that maintain and provide the computational resources of the system are not legal entities (persons or other type of legal entity such as firms). This is another fundamental and fundamentally unanswered question at the time of writing. Namely, how one can even define and measure – let alone incentivise – decentralisation. Counting how many nodes there are can only be a proxy. This is one aspect of the famous Sybil problem: namely the near-zero cost of creating new on-line pseudo-identities. Yet another unavoidable correlate of decentralisation is that agents in the system need to find an incentive to maintain that system - and that incentive has to be baked in the decentralised operation (else the nodes are someone's employee or friends and the system is no longer de-centralised).

The ambition of the conference we have organised – which we hope will be the first of a series – was specifically to cater to this broad type of questions around the incentive structures that are needed to keep up and stabilize decentralised systems. How does one measure, induce, and monitor "decentralised" in a decentralised environment. If trust is a resource, how much trust does one need for what usage and at what price. How does one design incentives that will hold the trust-providing system together, keep its different actors happy, and foster stability and resilience. Specifically, how does one set up the rules for the allocation of platform profits, and how does one handle the profit/price dilemma. That is to say how can one reconcile profit distribution rules with the price of the system's own token/cryptocurrency which is the means by which incentives are implemented. Token holders want a high price but platform contributors want a high profit.

There is need for methodological guidance to find both pen and paper and data-driven solution paths to the key questions above; to produce tools that will help designers of decentralised socio-technical systems to 'science out' fundamental difficulties; to reinforce and build better trust structures with sound economics; and understand the complex multi-objective optimisation which is implied. We hope this conference and its subsequent editions will provide a favourable space for the further exploration of these new territories in computer science and economics.

For this first edition, there were 38 papers submitted: 23 papers in computer science (17 as regular papers for publication in the proceedings and 6 for presentation only) and 16 papers in economics. The computer science program committee selected 11 papers for publication and presentation and 3 papers for presentation only. The economics program committee selected 8 papers for presentation at the conference. Every submitted paper was evaluated by at least three members of the program committee.

The program included two keynotes lecture in computer science by Amr El Abbadi (UCSB, USA) and Dahlia Malkhi (VMware, USA) and two keynotes lectures in economics by Lin William Cong (University of Chicago Booth School of Business, USA) and Catherine Casamatta (Toulouse School of Economics, France). The abstracts of the keynote lectures in computer science are included in this volume.

The best paper award was presented by William George and Clement Leseage for the paper:*a Smart Contract Oracle for Approximating Real-World, Real Number Values*. The paper was awarded with the "Asseth - Kaiko Prize for Research in Cryptoeconomics" (1,500 euros).

The success of this first edition was the result of a team effort. We thank the authors for providing valuable content for the conference and the program committee who worked hard in reviewing papers and giving feedback to the authors. We also thank the Ecole

Normale Superieure who hosted the conference, our institutional supporters, CEA LIST, CNRS, CREST, ENS, Sorbonne Université, and our financial supporters, Asseth-Kaiko, Capgemini, Institut Carnot. Finally, we want to thank our wonderful students and colleagues, Antonella, Yackolley, Pablo, Gewu, Nicolas, Zeinab, Zainah, Agnès, Onder, Thibault, Aimen and Francois that helped with all the logistics of the conference.

Maria, Vincent, Sara, Julien and Maurice

Tokenomics 2019 Organization

General Chairs

Vincent Danos, Ecole Normale Supérieure (France)
Maurice Herlihy, Brown University (USA)
Maria Potop-Butucaru, Sorbonne Université (France)
Julien Prat, CREST, Ecole Polytechnique (France)
Sara Tucci-Piergiovanni, CEA LIST (France)

Program Committee

Computer Science

Emmanuelle Anceaume, IRISA (France)
Antonio Fernández Anta, IMDEA Networks (Spain)
Daniel Augot, INRIA, Ecole Polytechnique (France)
Konstantinos Chalkias, R3 (UK, USA)
Vincent Danos, Ecole Normale Supérieure (France)
Fabrice Le Fessant, OCaml PRO (France)
Bryan Ford, Ecole Polytechnique Fédérale de Lausanne - EPFL (Switzerland)
Georg Fuchsbauer, Ecole Normale Supérieure (France)
Juan A. Garay. Texas A&M University (USA)
Chryssis Georgiou, University of Cyprus (Cyprus)
Vincent Gramoli, The University of Sydney (Australia)
Rachid Guerraoui, Ecole Polytechnique Fédérale de Lausanne - EPFL (Switzerland)
Maurice Herlihy, Brown University (USA)
Guillaume Jourjon, Data61-CSIRO (Australia)
Aggelos Kiayias, The University of Edinburgh (UK)
Mario Larangeira, IOHK, Tokyo Institute of Technology (Japan)
Žarko Milošević. Tendermint, Singidunum University (Serbia)
Maria Potop-Butucaru, Sorbonne Université (France)
Michel Raynal, IRISA-IFSIC, Institut Universitaire de France (France)
Ilya Sergey, Yale-NUS College (Singapore)
Alexander Spiegelman, VMware Research Group (Israel)
Francois Taiani, INRIA, IRISA (France)
Sara Tucci-Piergiovanni, CEA LIST (France)
Marko Vukolic, IBM Research - Zurich (Switzerland)
Roger Wattenhofer, ETH Zurich (Switzerland)
Josef Widder, TU Wien (Austria)

Economics

Bruno Biais, HEC (France)
Christophe Bisière, Toulouse School of Economics (France)
Andrea Canidio, IMT and INSEAD (Italy)
Lin William Cong, University of Chicago Booth School of Business (USA)
Guillaume Haeringer, Baruch College (USA)

International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019).
Editors: Vincent Danos, Maurice Herlihy, Maria Potop-Butucaru, Julien Prat, and Sara Tucci-Piergiovanni
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Hanna Halaburda, NYU Stern School of Business (USA)
Gur Huberman, Columbia University (USA)
Winfried Koeniger, St-Gallen University (Switzerland)
Gina Pieters, University of Chicago (USA)
Julien Prat, CREST, Ecole Polytechnique (France)
Linda Schilling, Ecole Polytechnique (France)