

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*

## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

More information about this subseries at <http://www.springer.com/series/7410>

Matthew Bernhard · Andrea Bracciali ·  
Lewis Gudgeon · Thomas Haines ·  
Ariah Klages-Mundt · Shin'ichiro Matsuo ·  
Daniel Perez · Massimiliano Sala ·  
Sam Werner (Eds.)

# Financial Cryptography and Data Security

FC 2021 International Workshops

CoDecFin, DeFi, VOTING, and WTSC  
Virtual Event, March 5, 2021  
Revised Selected Papers

### *Editors*


Matthew Bernhard  
University of Michigan–Ann Arbor  
Ann Arbor, MI, USA

Lewis Gudgeon  
Imperial College London  
London, UK

Ariah Klages-Mundt  
Ithaca College  
Ithaca, USA

Daniel Perez  
Imperial College London  
London, UK

Sam Werner  
Imperial College London  
London, UK

Andrea Bracciali   
Computer Science and Mathematics  
Stirling University  
Stirling, UK

Thomas Haines  
Norwegian University of Science  
and Technology  
Trondheim, Norway

Shin'ichiro Matsuo  
Department of Computer Science  
Georgetown University  
Washington, WA, USA

Massimiliano Sala   
Dipartimento di Matematica  
University of Trento  
Trento, Trento, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-662-63957-3

ISBN 978-3-662-63958-0 (eBook)

<https://doi.org/10.1007/978-3-662-63958-0>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Financial Cryptography Association 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature

The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

# CoDecFin 2021 Preface

The Second Workshop on Coordination of Decentralized Finance (CoDecFin 2021) took place in conjunction with Financial Cryptography and Data Security 2021 on March 5, 2021. The CoDecFin workshop is focused on multi-disciplinary issues regarding technologies and operations of decentralized finance based on permissionless blockchain.

From an academic point of view, security and privacy protection are some of the leading research streams. The Financial Cryptography conference discusses these research challenges. On the other hand, other stakeholders than cryptographers and blockchain engineers have different interests in these characteristics of blockchain technology. For example, regulators face difficulty in tracing transactions in terms of anti-money laundering (AML) against privacy-enhancing crypto-assets. Another example is consumer protection in the case of cyberattacks on crypto-asset custodians. Blockchain business entities sometimes start their business before maturing technology, but the technology and operations are not transparent to regulators and consumers. The main problem is a lack of communication among stakeholders of the decentralized finance ecosystem. The G20 discussed the issue of insufficient communication among stakeholders in 2019. It concluded that there is an essential need for multi-stakeholder discussion among engineers, regulators, business entities, and operators based on the neutrality of academia.

The CoDecFin workshop was initiated in 2020 to facilitate such multi-stakeholder discussion in a neutral academic environment. The goals of CoDecFin were to have common understandings of technology and regulatory goals and to discuss essential issues of blockchain technology faced by all stakeholders mentioned above. It was a historic workshop because we could involve regulators and engineers in the discussion at the Financial Cryptography conference.

CoDecFin 2021 consisted of three parts: a keynote talk, presentations by all stakeholders, and roundtable discussions. The keynote talk by Peter Van Balkenburgh discussed “Your Right to DeFi”. The presentations were selected based on the peer-review process. The topics included DeFi risks, AML/KYC, and privacy. As this workshop was held right after the Financial Crimes Enforcement Network (FinCEN) proposed a new draft regulation on AML/KYC and the treatment of un-hosted wallets, the AML/KYC and privacy session focused on the issues related to this proposal. In the third part, we invited panelists from all stakeholders, including blockchain businesses, regulators, engineers, and academia, on the AML/KYC session issues to join the roundtable discussions. Presentations and discussions are included as papers of this proceedings.

# CoDecFin 2021 Organization

## Workshop Chair

Shin'ichiro Matsuo

Georgetown University, NTT Research, and  
BSafe.network, USA

## Program Committee

Julien Bringer

Joaquin Garcia-Alfaro

Arthur Gervais

Byron Gibson

Feng Chen

Shin'ichiro Matsuo (Chair)

Steven Nam

Michele Benedetto Neitz

Roman Danziger Pavlov

Robert Schwentker

Yonatan Sompolsky

Shigeya Suzuki

Ryosuke Ushida

Robert Wardrop

Pindar Wong

Aaron Wright

Anton Yemelyanov

Aviv Zohar

Kallistech, France

Telecom SudParis, France

Imperial College London, UK

Stanford Center for Blockchain Research, USA

University of British Columbia, Canada

Georgetown University, NTT Research, and  
BSafe.network, USA

Stanford Journal of Blockchain Law & Policy, USA

Golden Gate University, USA

SafeStead Inc., USA

DLT Education and BSafe.network, USA

The Hebrew University of Jerusalem and DAGlabs,  
Israel

Keio University

JFSA and Georgetown University, USA

University of Cambridge, UK

BSafe.network, Hong Kong

Cardozo School of Law, USA

Base58 Association, Canada

The Hebrew University of Jerusalem, Israel

## DeFi 2021 Preface

These proceedings collect the papers accepted at the First Workshop on Decentralized Finance (DeFi 2021 - <http://fc21.ifca.ai/defi/>), held in association with the Financial Cryptography and Data Security 2021 conference (FC 2021) on March 5, 2021.

The focus of the DeFi workshop series is decentralized finance, a blockchain powered peer-to-peer financial system. This first workshop coincided with the early fruition of DeFi, and sought to solicit contributions from both academia and industry which focussed on addressing fundamental, timely, and important questions at the centre of DeFi.

This first workshop received 40 submissions, of which 22 were accepted either as a short paper (9) or as a talk (13). All of the short papers and a subset of the talks, as précis, appear in these proceedings. Overall, the organizers were extremely impressed by the quality of submissions received and were delighted by the strong attendance and lively discussion during the workshop. The workshop was conducted online as a result of the COVID-19 pandemic, but we look forward to future years where it can be conducted in person.

In addition to talks pertaining to submissions we had a guest speaker, Raphael Auer, from the Bank for International Settlements, and we would like to thank him for his talk. The workshop closed with a panel, featuring Tarun Chitra (Gauntlet), Robert Leshner (Compound), Andrew Miller (University of Illinois at Urbana-Champaign), and Jeremy Musighi (Balancer), which covered a wide range of topics from privacy in DeFi to the role of auditors. We would like to sincerely thank the panelists for taking part and for the lively discussion.

The Organizing Committee would like to extend sincere thanks to all those who submitted their work, the Program Committee for their careful work, and all those who participated in the workshop. In addition, we would like to extend our thanks to Kevin McCurley and Kay McKelly, for their seamless organization of the online support needed to conduct this event virtually, and Rafael Hirschfeld for his flawless support, organization, and encouragement of this first workshop.

June 2021

Lewis Gudgeon  
Ariah Klages-Mundt  
Daniel Perez  
Sam Werner

# DeFi 2021 Organization

## Workshop Chairs

Lewis Gudgeon  
Ariah Klages-Mundt  
Daniel Perez  
Sam Werner

Imperial College London, UK  
Cornell University, USA  
Imperial College London, UK  
Imperial College London, UK

## Program Committee

Cuneyt Akcora  
Raphael Auer  
Tarun Chitra  
Martin Florian  
Dominik Harz  
William Knottenbelt  
Jiasun Li  
Benjamin Livshits  
Jun-You Liu  
Patrick McCorry  
Andrew Miller  
Andreea Minca  
Daniel Moroz  
David Parkes  
Julien Prat  
Tim Roughgarden  
Alexei Zamyatin  
Fan Zhang

University of Manitoba, Canada  
Bank for International Settlements, Switzerland  
Gauntlet Networks, USA  
Humboldt-Universität zu Berlin  
Imperial College London, UK  
Imperial College London, UK  
George Mason University, USA  
Imperial College London and Brave Software, UK  
Cornell University, USA  
anydot, UK  
University of Illinois at Urbana-Champaign, USA  
Cornell University, USA  
Harvard University, USA  
Harvard University, USA  
CNRS, France  
Columbia University, USA  
Imperial College London, UK  
Chainlink, USA



# **VOTING 2021 Preface**

VOTING 2021 marks the 6th Workshop on Advances in Secure Electronic Voting associated with the Financial Cryptography and Data Security 2021 conference (FC 2021) held virtually due to the COVID-19 pandemic on March 5, 2021.

This year's workshop received 14 papers with 7 accepted. We are grateful for our Program Committee for their time and effort, and especially their flexibility when we extended the submission deadline. We also thank the authors of all submitted papers, and especially the presenters for joining the workshop online despite the ongoing COVID-19 crisis. We are also grateful to Ray Hirschfeld, Sergi Delgado Segura, and IFCA for organizing all the logistics of the event and the FC workshop chairs for their continued support of VOTING. For VOTING 2022 the tradition of staggered chairs is continued with Thomas Haines and Aleks Essex serving as program chairs.

April 2021

Matthew Bernhard  
Thomas Haines

# VOTING 2021 Organization

## Program Chairs

Matthew Bernhard  
Thomas Haines

VotingWorks, USA  
Norwegian University of Science and Technology,  
Norway

## Program Committee

Roberto Araujo	Universidade Federal do Pará, Brazil
Josh Benaloh	Microsoft Research, USA
Jeremy Clark	Concordia University, Canada
Chris Culnane	Independent Researcher, UK
Constantin Dragan	University of Surrey, UK
Jeremy Epstein	SRI International, USA
Aleksander Essex	Western University, Canada
Kristian Gjøsteen	Norwegian University of Science and Technology
Rajeev Gore	The Australian National University, Australia
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Reto Koenig	Bern University of Applied Sciences, Switzerland
Ralf Kuesters	University of Stuttgart, Germany
Oksana Kulyk	IT University of Copenhagen, Denmark
Olivier Pereira	Université catholique de Louvain, Belgium
Peter Rønne	University of Luxembourg, Luxembourg
Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Steve Schneider	University of Surrey, UK
Carsten Schuermann	IT University of Copenhagen, Denmark
Philip Stark	University of California, Berkeley, USA
Vanessa Teague	Thinking Cybersecurity, Australia
Poorvi Vora	The George Washington University, USA
Dan Wallach	Rice University, USA

## WTSC 2021 Preface

These proceedings collect the papers accepted at the Fifth Workshop on Trusted Smart Contracts (WTSC21 - <http://fc21.ifca.ai/wtsc/>) associated with the Financial Cryptography and Data Security 2021 conference (FC 2021).

The WTSC series focuses on smart contracts, i.e., self-enforcing agreements in the form of executable programs, and other decentralized applications that are deployed to, and run on top of, (specialized) blockchains. These technologies introduce a novel programming framework and execution environment, which, together with the supporting blockchain technologies, carry unanswered and challenging research questions. Multidisciplinary and multifactorial aspects affect correctness, safety, privacy, authentication, efficiency, sustainability, resilience, and trust in smart contracts and decentralized applications.

WTSC aims to address the scientific foundations of Trusted Smart Contract engineering, i.e., the development of contracts that enjoy some verifiable “correctness” properties, and to discuss open problems, proposed solutions, and the vision on future developments amongst a research community that is growing around these themes and brings together users, practitioners, industry, institutions, and academia. This was reflected in the multidisciplinary Program Committee (PC) of this fifth edition of WTSC, comprising members from companies, universities, and research institutions from several countries worldwide, who kindly accepted to support the event. The association with FC 2021 provided, once again, an ideal context for our workshop.

This year’s edition of WTSC received 30 submissions by about 90 authors, confirming a growing trend and increased interest. Given the high quality of submission, 16 papers were accepted after double-blind peer review. Thanks to the generous effort by the PC, each paper received an average of 3.3 reviews, providing constructive feedback to authors. Papers revised after the discussion at the workshop are collected in the present volume. These analyze the current state of the art of smart contracts and their development. Important aspects that were discussed at the workshop included security and verification, attacks’ analysis, scalability, relationships of smart contracts and consensus, and privacy-preserving applications. An emerging theme received a lot of attention: decentralized finance (DeFi). Apart from the contributed talks, we had a final roundtable on DeFi jointly with the 2nd Workshop on Coordination of Decentralized Finance (CoDecFin 2021).

Generally speaking, the presentations made a full day of interesting talks and discussion. More detailed video presentations are made available online on a dedicated YouTube channel<sup>1</sup> that can be reached from the workshop’s web page. Following our tradition of excellent invited speakers (Buterin, Breitman, Gutmann, Mishra, Artamonov, Grigg), our workshop started with a beautiful presentation by Darren Tapp, leading scientist in the cryptocurrency community DASH.

---

<sup>1</sup> [https://www.youtube.com/watch?v=MvGnPhpkNIM&list=PL\\_aN0fSJkEsoopkLAivp89w5hHdF19W0A](https://www.youtube.com/watch?v=MvGnPhpkNIM&list=PL_aN0fSJkEsoopkLAivp89w5hHdF19W0A).

This year's edition was planned to take place in Granada, Spain, on March 5, 2021, but was held online due to the COVID-19 pandemic. Although we missed direct interaction a lot, we believe the community enjoyed the online presentations and discussions.

WTSC 2021's chairs would like to thank everyone for their usual, and this year extra, effort and valuable contributions: authors, Program Committee members and reviewers, and participants, as well as the support by IFCA, FC 2021 committees, Kevin McCurley and Kay McKelly for the online framework to run the conference, and Ray Hirschfeld for the usual exceptional organization of the event.

May 2021

Andrea Bracciali  
Massimiliano Sala

# WTSC 2021 Organization

## Workshop Chairs

Andrea Bracciali  
Massimiliano Sala

University of Stirling, UK  
University of Trento, Italy

## Program Committee

Monika di Angelo  
Igor Artamonov  
Daniel Augot  
Surya Bakshi  
Fadi Barbara  
Massimo Bartoletti  
Stefano Bistarelli  
Christina Boura

Vienna University of Technology, Austria  
Ethereum Classic, UK  
Inria, France  
University of Illinois, USA  
University of Turin, Italy  
University of Cagliari, Italy  
University of Perugia, Italy  
Versailles Saint-Quentin-en-Yvelines University,  
France

Andrea Bracciali  
Daniel Broby  
James Chapman  
Martin Chapman  
Alexander Denzler

University of Stirling, UK  
Strathclyde University, UK  
IOHK, UK  
King's College London, UK  
Lucerne University of Applied Sciences and Arts,  
Switzerland

Nicola Dimitri  
Nadia Fabrizio  
Murdoch Gabbay  
Oliver Giudice  
Davide Grossi  
Yoichi Hirai  
Lars R. Knudsen  
Ioannis Kounelis  
Pascal Lafourcade  
Andrew Lewis-Pye  
Carsten Maple  
Michele Marchesi  
Fabio Martinelli  
Luca Mazzola

University of Siena, Italy  
Cefriel, Italy  
Heriot-Watt University, UK  
Banca d'Italia, Italy  
University of Groningen, The Netherlands  
brainbot technologies AG, Denmark  
Technical University of Denmark, Denmark  
Joint Research Centre, European Commission, Italy  
University of Clermont Auvergne, France  
London School of Economics, UK  
University of Warwick, UK  
University of Cagliari, Italy  
IIT-CNR, Italy  
Lucerne University of Applied Sciences and Arts,  
Switzerland

Sihem Mesnager  
Philippe Meyer  
Bud Mishra

University of Paris 8 Vincennes-Saint-Denis, France  
Avalog, Switzerland  
New York University, USA

Carlos Molina-Jimenez	University of Cambridge, UK
Massimo Morini	Banca IMI, Italy
Immaculate Motsi-Omoijiade	University of Warwick, UK
Alex Norta	Tallin University of Technology, Estonia
Akira Otsuka	Institute of Information Security, Japan
Federico Pintore	University of Oxford, UK
Massimiliano Sala	University of Trento, Italy
Jason Teutsch	Truebit, USA
Roberto Tonelli	University of Cagliari, Italy
Luca Viganò	University of Verona, Italy
Philip Wadler	University of Edinburgh, UK
Yilei Wang	Qufu Normal University, China
Tim Weingärtner	Hochschule Lucerne, Switzerland
Ales Zamuda	University of Maribor, Slovenia
Santiago Zanella-Beguelin	Microsoft, UK
Dionysis Zindros	University of Athens, Greece

# Contents

## CoDecFin – DeFi Risks

Risk Framework for Bitcoin Custody Operation with the Revault Protocol .....	3
<i>Jacob Swambo and Antoine Poinot</i>	

Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs .....	21
<i>Ryosuke Ushida and James Angel</i>	

## CoDecFin – AML/KYC and Privacy

Collaborative Deanonymization .....	39
<i>Patrik Keller, Martin Florian, and Rainer Böhme</i>	

Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets .....	47
<i>Ryan Taylor</i>	

Analyzing FinCEN’s Proposed Regulation Relating to AML and KYC Laws .....	54
<i>Aaron Wright and Sachin Meier</i>	

## DeFi – Protocol Design

Optimal Fees for Geometric Mean Market Makers .....	65
<i>Alex Evans, Guillermo Angeris, and Tarun Chitra</i>	

Market Based Mechanisms for Incentivising Exchange Liquidity Provision .....	80
<i>W. Gawlikowicz, B. Mannerings, T. Rudolph, and D. Šiška</i>	

Understand Volatility of Algorithmic Stablecoin: Modeling, Verification and Empirical Analysis .....	97
<i>Wenqi Zhao, Hui Li, and Yuming Yuan</i>	

Measuring Asset Composability as a Proxy for DeFi Integration .....	109
<i>Victor von Wachter, Johannes Rude Jensen, and Omri Ross</i>	

Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum . . . . .	115
<i>Mudabbir Kaleem and Weidong Shi</i>	
On Stablecoin Price Processes and Arbitrage . . . . .	124
<i>Ingolf Gunnar Anton Pernice</i>	
Red-Black Coins: Dai Without Liquidations . . . . .	136
<i>Mehdi Salehi, Jeremy Clark, and Mohammad Mannan</i>	
<b>DeFi – Formal Attack Analysis</b>	
Formal Analysis of Composable DeFi Protocols . . . . .	149
<i>Palina Tolmach, Yi Li, Shang-Wei Lin, and Yang Liu</i>	
How to Exploit a DeFi Project . . . . .	162
<i>Xinyuan Sun, Shaokai Lin, Vilhelm Sjöberg, and Jay Jie</i>	
<b>DeFi – Economics and Regulation</b>	
DeFi as an Information Aggregator . . . . .	171
<i>Jiasun Li</i>	
A Game-Theoretic Analysis of Cross-ledger Swaps with Packetized Payments . . . . .	177
<i>Alevtina Dubovitskaya, Damien Ackerer, and Jiahua Xu</i>	
<b>DeFi – MEV and Illicit Activity</b>	
Wendy Grows Up: More Order Fairness . . . . .	191
<i>Klaus Kursawe</i>	
Measuring Illicit Activity in DeFi: The Case of Ethereum . . . . .	197
<i>Jiasun Li, Foteini Baldimtsi, Joao P. Brandao, Maurice Kugler, Rafelh Hulays, Eric Showers, Zain Ali, and Joseph Chang</i>	
<b>DeFi – Order Routing and Formal Methods</b>	
Global Order Routing on Exchange Networks . . . . .	207
<i>Vincent Danos, Hamza El Khalloufi, and Julien Prat</i>	
Towards a Theory of Decentralized Finance . . . . .	227
<i>Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente</i>	



## Voting

Auditing Hamiltonian Elections .....	235
<i>Michelle Blom, Philip B. Stark, Peter J. Stuckey, Vanessa Teague, and Damjan Vukcevic</i>	
Cast-as-Intended: A Formal Definition and Case Studies .....	251
<i>Peter B. Rønne, Peter Y. A. Ryan, and Ben Smyth</i>	
Mobile Voting – Still Too Risky? .....	263
<i>Sven Heiberg, Kristjan Krips, and Jan Willemson</i>	
New Standards for E-Voting Systems: Reflections on Source Code Examinations .....	279
<i>Thomas Haines and Peter Roenne</i>	
Post-quantum Online Voting Scheme .....	290
<i>Guillaume Kaim, Sébastien Canard, Adeline Roux-Langlois, and Jacques Traoré</i>	
Short Paper: Ballot Secrecy for Liquid Democracy .....	306
<i>Mahdi Nejadgholi, Nan Yang, and Jeremy Clark</i>	
Shorter Lattice-Based Zero-Knowledge Proofs for the Correctness of a Shuffle .....	315
<i>Javier Herranz, Ramiro Martínez, and Manuel Sánchez</i>	
<b>WTSC – Security and Verification</b>	
On-Chain Smart Contract Verification over Tendermint .....	333
<i>Luca Olivieri, Fausto Spoto, and Fabio Tagliaferro</i>	
Publicly Verifiable and Secrecy Preserving Periodic Auctions .....	348
<i>Hisham S. Galal and Amr M. Youssef</i>	
EthVer: Formal Verification of Randomized Ethereum Smart Contracts .....	364
<i>Łukasz Mazurek</i>	
Absentia: Secure Multiparty Computation on Ethereum .....	381
<i>Didem Demirag and Jeremy Clark</i>	
Empirical Analysis of On-chain Voting with Smart Contracts .....	397
<i>Robert Muth and Florian Tschorsch</i>	

**WTSC – Foundations**

Mirroring Public Key Infrastructures to Blockchains for On-Chain Authentication ..... 415  
*Ulrich Gellersdörfer, Friederike Groschupp, and Florian Matthes*

Reactive Key-Loss Protection in Blockchains ..... 431  
*Sam Blackshear, Konstantinos Chalkias, Panagiotis Chatzigiannis, Riyaz Faizullahoy, Irakliy Khaburzaniya, Eleftherios Kokoris Kogias, Joshua Lind, David Wong, and Tim Zakian*

Merkle Trees Optimized for Stateless Clients in Bitcoin ..... 451  
*Bolton Bailey and Suryanarayana Sankagiri*

Soft Power: Upgrading Chain Macroeconomic Policy Through Soft Forks ..... 467  
*Dionysis Zindros*

Privacy-Preserving Resource Sharing Using Permissioned Blockchains: (The Case of Smart Neighbourhood) ..... 482  
*Sepideh Avizheh, Mahmudun Nabi, Saoreen Rahman, Setareh Sharifian, and Reihaneh Safavi-Naini*

**WWTSC – Attacks’ Analysis**

SoK: Algorithmic Incentive Manipulation Attacks on Permissionless PoW Cryptocurrencies ..... 507  
*Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl*

Pay to Win: Cheap, Cross-Chain Bribing Attacks on PoW Cryptocurrencies ... 533  
*Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl*

**WTSC – DeFi and Tokens**

SoK: Lending Pools in Decentralized Finance ..... 553  
*Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente*

Standardized Crypto-Loans on the Cardano Blockchain ..... 579  
*Dmytro Kondratiuk, Pablo Lamela Seijas, Alexander Nemish, and Simon Thompson*

Fairness in ERC Token Markets: A Case Study of CryptoKitties ..... 595  
*Kentaro Sako, Shin’ichiro Matsuo, and Sachin Meier*

Coins, Covid, Keynes and K-Shaped Recovery .....	611
<i>Pepi Martinez, William Huang, and Bud Mishra</i>	
<b>Author Index</b> .....	<b>629</b>