

7th Conference on Advances in Financial Technologies

AFT 2025, October 8–10, 2025, Pittsburgh, PA, USA

Edited by

Zeta Avarikioti
Nicolas Christin



Editors

Zeta Avarikioti 

TU Wien, Austria
georgia.avarikioti@tuwien.ac.at

Nicolas Christin 

Carnegie Mellon University, Pittsburgh, PA, USA
nicolasc@andrew.cmu.edu

ACM Classification 2012

Security and privacy → Mathematical foundations of cryptography; Security and privacy → Distributed systems security; Security and privacy → Privacy-preserving protocols; Security and privacy → Pseudonymity, anonymity and untraceability; Security and privacy → Economics of security and privacy; Theory of computation → Algorithmic game theory and mechanism design; Theory of computation → Cryptographic primitives; Theory of computation → Cryptographic protocols; Applied computing → Digital cash; Applied computing → Economics

ISBN 978-3-95977-400-0

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/978-3-95977-400-0>.

Publication date

October, 2025

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists all publications of this volume 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/LIPIcs.AFT.2025.0

ISBN 978-3-95977-400-0

ISSN 1868-8969

<https://www.dagstuhl.de/lipics>

LIPICs – Leibniz International Proceedings in Informatics

LIPICs is a series of high-quality conference proceedings across all fields in informatics. LIPICs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board

- Christel Baier (TU Dresden, DE)
- Roberto Di Cosmo (Inria and Université Paris Cité, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Holger Hermanns (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)
- Daniel Král' (Leipzig University, DE and Max Planck Institute for Mathematics in the Sciences, Leipzig, DE)
- Sławomir Lasota (University of Warsaw, PL)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN – Chair)
- Chih-Hao Luke Ong (Nanyang Technological University, SG)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Pierre Senellart (ENS, Université PSL, Paris, France)
- Alexandra Silva (Cornell University, Ithaca, US)

ISSN 1868-8969

<https://www.dagstuhl.de/lipics>

■ Contents

Preface	
<i>Zeta Avarikioti and Nicolas Christin</i>	0:ix
Program Committee	
.....	0:xi
Steering Committee	
.....	0:xiii
External Reviewers	
.....	0:xv
List of Authors	
.....	0:xvii

Session 1: Cryptography and Privacy in Blockchains

Cache Timing Leakages in Zero-Knowledge Protocols	
<i>Shibam Mukherjee, Christian Rechberger, and Markus Schafnegg</i>	1:1–1:26
Zero-Knowledge Authenticator for Blockchain: Policy-Private and Obliviously Updateable	
<i>Kostas Kryptos Chalkias, Deepak Maram, Arnab Roy, Joy Wang, and Aayush Yadav</i>	2:1–2:23
Fast, Private and Regulated Payments in Asynchronous Networks	
<i>Maxence Brugeret, Victor Languille, Petr Kuznetsov, and Hamza Zarfaoui</i>	3:1–3:24
Proxying Is Enough: Security of Proxying in TLS Oracles and AEAD Context Unforgeability	
<i>Zhongtang Luo, Yanxue Jia, Yaobin Shen, and Aniket Kate</i>	4:1–4:24
Blockchain Governance via Sharp Anonymous Multisignatures	
<i>Wonseok Choi, Xiangyu Liu, and Vassilis Zikas</i>	5:1–5:24

Session 2: AMM

Modeling Loss-Versus-Rebalancing in Automated Market Makers via Continuous-Installment Options	
<i>Srisht Fateh Singh, Reina Ke Xin Li, Samuel Gaskin, Yuntao Wu, Jeffrey Klinck, Panagiotis Michalopoulos, Zisis Poulos, and Andreas Veneris</i>	6:1–6:23
Mechanism Design for Automated Market Makers	
<i>T.-H. Hubert Chan, Ke Wu, and Elaine Shi</i>	7:1–7:22
Strategic Analysis of Just-In-Time Liquidity Provision in Concentrated Liquidity Market Makers	
<i>Bruno Llacer Trotti, Weizhao Tang, Rachid El-Azouzi, Giulia Fanti, and Daniel Sadoc Menasché</i>	8:1–8:22

7th Conference on Advances in Financial Technologies (AFT 2025).

Editors: Zeta Avarikioti and Nicolas Christin



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Session 3: Measurements

Money in Motion: Micro-Velocity and Usage of Ethereum’s Liquid Staking Tokens <i>Benjamin Kraner, Luca Pennella, Nicolò Vallarano, and Claudio J. Tessone</i>	9:1–9:18
Do Inflation Expectations Drive Cryptocurrency Investments? <i>Will Cong, Pulak Ghosh, Jiasun Li, Qihong Ruan, and Artem Streltsov</i>	10:1–10:3
Cryptocurrency Exchange Listings <i>Jiasun Li, Mei Luo, Muzhi Wang, and Zhe Wei</i>	11:1–11:2

Session 4: Consensus I

How Much Public Randomness Do Modern Consensus Protocols Need? <i>Joseph Bonneau, Benedikt Bünz, Miranda Christ, and Yuval Efron</i>	12:1–12:19
Composable Byzantine Agreements with Reorder Attacks <i>Jing Chen, Jin Dong, Jichen Li, Xuanzhi Xia, and Wentao Zhou</i>	13:1–13:23
Optimistic Message Dissemination <i>Chen-Da Liu-Zhang, Christian Matt, and Søren Eller Thomsen</i>	14:1–14:24
Beyond Optimal Fault-Tolerance <i>Andrew Lewis-Pye and Tim Roughgarden</i>	15:1–15:23

Session 5: Consensus II

Nakamoto Consensus from Multiple Resources <i>Mirza Ahad Baig, Christoph U. Günther, and Krzysztof Pietrzak</i>	16:1–16:23
Fully-Fluctuating Participation in Sleepy Consensus <i>Yuval Efron, Joachim Neu, and Toniann Pitassi</i>	17:1–17:22
From Permissioned to Proof-of-Stake Consensus <i>Jovan Komatovic, Andrew Lewis-Pye, Joachim Neu, Tim Roughgarden, and Ertem Nusret Tas</i>	18:1–18:26
Two-Tier Black-Box Blockchains and Application to Instant Layer-1 Payments <i>Michele Ciampi, Yun Lu, Rafail Ostrovsky, and Vassilis Zikas</i>	19:1–19:24

Session 6: Incentives and Tokenomics

Selfish Mining Under General Stochastic Rewards <i>Maryam Bahrani, Michael Neuder, and S. Matthew Weinberg</i>	20:1–20:23
Pool Formation in Oceanic Games: Shapley Value and Proportional Sharing <i>Aggelos Kiayias, Elias Koutsoupias, Evangelos Markakis, and Panagiotis Tsamopoulos</i>	21:1–21:24
Single-Token vs Two-Token Blockchain Tokenomics <i>Aggelos Kiayias, Philip Lazos, and Paolo Penna</i>	22:1–22:22

Session 7: Mechanism Design for Fees and Markets

Transaction Fee Market Design for Parallel Execution <i>Bahar Acilan, Andrei Constantinescu, Lioba Heimbach, and Roger Wattenhofer</i> ..	23:1–23:25
Multidimensional Blockchain Fees Are (Essentially) Optimal <i>Guillermo Angeris, Theo Diamandis, and Ciamac Moallemi</i>	24:1–24:23
The Exchange Problem <i>Mohit Garg and Suneel Sarswat</i>	25:1–25:19

Session 8: Empirical Analysis and MEV

Measuring CEX-DEX Extracted Value and Searcher Profitability: The Darkest of the MEV Dark Forest <i>Fei Wu, Danning Sui, Thomas Thiery, and Mallesh Pai</i>	26:1–26:23
Unravelling the Probabilistic Forest: Arbitrage in Prediction Markets <i>Oriol Saguillo, Vahid Ghafouri, Lucianna Kiffer, and Guillermo Suarez-Tangil</i> ...	27:1–27:24
Optimistic MEV in Ethereum Layer 2s: Why Blockspace Is Always in Demand <i>Ozan Solmaz, Lioba Heimbach, Yann Vonlanthen, and Roger Wattenhofer</i>	28:1–28:24

Session 9: Scalability and Interoperability

Efficient Parallel Execution of Blockchain Transactions Leveraging Conflict Specifications <i>Parwat Singh Anjana, Matin Amini, Rohit Kapoor, Rahul Parmar, Raghavendra Ramesh, Srivatsan Ravi, and Joshua Tobkin</i>	29:1–29:26
Ticket to Ride: Locally Steered Source Routing for the Lightning Network <i>Sajjad Alizadeh and Majid Khabbazi</i>	30:1–30:21
Trustless Bridges via Random Sampling Light Clients <i>Bhargav Nagaraja Bhatt, Fatemeh Shirazi, and Alistair Stewart</i>	31:1–31:24
4-Swap: Achieving Grief-Free and Bribery-Safe Atomic Swaps Using Four Transactions <i>Kirti Singh, Vinay J. Ribeiro, and Susmita Mandal</i>	32:1–32:22

Session 10: Cryptocurrency Markets and Adoption

Cuttlefish: A Fair, Predictable Execution Environment for Cloud-Hosted Financial Exchanges <i>Liangcheng Yu, Prateesh Goyal, Ilias Marinos, and Vincent Liu</i>	33:1–33:25
PvpAMM: A Perpetual Market for Unbalanced Long-Short Positions <i>Zhenhang Shang, Zhenyu Zhao, and Kani Chen</i>	34:1–34:19
On-Chain Decentralized Learning and Cost-Effective Inference for DeFi Attack Mitigation <i>Abdulrahman Alhaidari, Balaji Palanisamy, and Prashant Krishnamurthy</i>	35:1–35:27

■ Preface

This volume contains 35 papers selected from a record-high 135 submissions – a 26% acceptance rate – to the Conference on Advances in Financial Technologies (AFT '25) held at Carnegie Mellon University, in Pittsburgh, Pennsylvania, USA, on October 8–10, 2025. This is the seventh year of the conference and the third year that it is independently organized and published in LIPIcs.

This year's edition was hosted in collaboration with the Carnegie Mellon CyLab Security and Privacy Institute, and, more specifically, CyLab's Secure Blockchain Initiative (SBI). CyLab is one of the largest security and privacy academic centers in the United States, and coordinates security and privacy research and education across all university departments at Carnegie Mellon, and SBI is one of its key initiatives. We elected to have this year's conference immediately follow the Secure Blockchain Initiative Summit, to foster collaboration across disciplinary boundaries and professional communities.

The paper selection process followed the typical process used by many computer science conferences. Each submission received at least three, and often four, detailed double-blind reviews by several program committee members and external reviewers. Each accepted paper was presented via a 15-minute live presentation, followed by a 5-minute question/answer period with the audience. We grouped papers in ten topical sessions, covering a broad range of theoretical and practical advances ranging from "Cryptography and Privacy in Blockchains" to "Measurements." Our scientific program was complemented by a keynote speech and an ever-entertaining rump session.

We thank all Program Committee members and external reviewers for their service in selecting the AFT program, and all authors for submitting their work for consideration. We also grateful to the AFT steering committee for their support and guidance throughout the process. We acknowledge the industry sponsors whose financial support was once again essential to running AFT:

Gold level

- a16z crypto

Silver level

- Ava Labs
- IC3
- Input Output
- TRM Labs

We are also deeply thankful for the support by the U.S. National Science Foundation Security, Privacy, and Trust in Cyberspace (SaTC 2.0) program under Grant No. 2420955.

We appreciate the immense efforts of Michael Lisanti, who served as General Co-Chair. Michael and the staff that worked with him – in particular, Ashley Bon, Isabelle Glassmith, and Beth Bucher – tirelessly handled all the logistical questions and were critical in making the event a success.

Vienna, Austria
Pittsburgh, PA, USA
October 2025

Zeta Avarikioti
Nicolas Christin



■ Program Committee

Aggelos Kiayias, University of Edinburgh and IOG

Akaki Mamageishvili, Offchain Labs

Alberto Sonnino, MystenLabs and University College London

Aljosha Judmayer, University of Vienna

Andrew Lewis-Pye, London School of Economics

Andrew Miller, University of Illinois Urbana-Champaign

Ari Juels, Cornell Tech

Ariel Zetlin-Jones, Carnegie Mellon University

Arthur Gervais, University College London

Aviad Rubinstein, Stanford University

Aviv Yaish, Yale University, IC3

Bernardo David, IT University of Copenhagen

Bernhard Haslhofer, Complexity Science Hub

Bryan Routledge, Carnegie Mellon University

Christian Cachin, University of Bern

Ciamac Moallemi, Columbia University

Clara Shikhelman, Chaincode Labs

Dimitris Karakostas, University of Edinburgh and Common Prefix

Dionysis Zindors, Common Prefix

Fahad Saleh, University of Florida

Fan Zhang, Yale University

Florian Tschorsch, TU Dresden

Geoffrey Ramseyer, Stellar Development Foundation

George Danezis, MystenLabs and University College London

Georgios Piliouras, Google DeepMind and SUTD

Ghassan Karame, Ruhr-University Bochum

Giulia Fanti, Carnegie Mellon University

Guy Goren, Aptos Labs

Hong-Sheng Zhou, Virginia Commonwealth University

Ittay Eyal, Technion

James Chiang, Aarhus University and Common Prefix

Jason Milionis, Columbia University

Jiasun Li, George Mason University

Jing Chen, Tsinghua University

Johnnatan Messias, Max Planck Institute for Software Systems (MPI-SWS)

Julien Prat, IP Paris

Kaihua Qin, Yale University

Kanye Ye Wang, University of Macau

Karl Wüst, Mysten Labs

Krzysztof Pietrzak, ISTA

Kyle Soska, Independent

Lioba Heimbach, ETH Zurich

Lucianna Kiffer, IMDEA Networks

Lukas Aumayr, University of Edinburgh and Common Prefix

Marco Reuter, International Monetary Fund

Marie Vasek, University College London

Matheus Xavier Ferreira, University of Virginia

Philipp Jovanovic, University College London

Pierre-Louis Roman, Independent

Pietro Saggese, IMT School for Advanced Studies Lucca

7th Conference on Advances in Financial Technologies (AFT 2025).

Editors: Zeta Avarikioti and Nicolas Christin



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Qiang Tang, The University of Sydney

Rainer Boehme, University of Innsbruck

Robin Fritsch, ETH Zurich

Ruizhe Jia, Stanford University

Sara Tucci-Piergiovanni, CEA LIST

Paris-Saclay University

Sarah Azouvi, Independent

Tarun Chitra, Gauntlet

Tim Roughgarden, Columbia University and
a16z crypto

Will Cong, Cornell SC Johnson

Yonatan Sompolinsky, Harvard University

■ Steering Committee

Ittai Abraham (co-chair), VMware research

Dan Boneh, Stanford University

Christian Cachin, University of Bern

Ittay Eyal (co-chair), Technion

Maurice Herlihy, Brown University

Maureen O'Hara, Cornell University

Tim Roughgarden, Columbia University

Eli Ben Sasson, Technion

Emin Gun Sirer (co-chair), Cornell
University

S. Matthew Weinberg ('23 PC chair),
Princeton University

Joseph Bonneau ('23 PC chair), New York
University

Rainer Boehme ('24 PC chair), University of
Innsbruck

Lucianna Kiffer ('24 PC chair), IMDEA
Networks

Nicolas Christin ('25 PC chair), Carnegie
Mellon University

Zeta Avarikioti ('25 PC chair), TU Wien and
Common Prefix



7th Conference on Advances in Financial Technologies (AFT 2025).

Editors: Zeta Avarikioti and Nicolas Christin



LIPIC Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

■ External Reviewers

Amirreza Sarencheh, University of Edinburgh

Bo Li, Hong Kong Polytechnic University

Burak Öz, TU Munich

Hao Chung, Carnegie Mellon University

Jichen Li, Peking University

Matthias Fitzi, IOHK

Paolo Penna, IOHK

Peter Gaži, IOG

Pyrros Chaidos, IOG

Sandro Coretti-Drayton, IOG

Sotiris Georganas, City University London

Wenrui Zuo, University of Edinburgh

■ List of Authors

Bahar Acilan  (23)
ETH Zürich, Switzerland

Abdulrahman Alhaidari  (35)
School of Computing and Information,
University of Pittsburgh, Pittsburgh, PA, USA

Sajjad Alizadeh (30)
Department of Electrical and Computer
Engineering, University of Alberta, Edmonton,
Canada

Matin Amini  (29)
University of Southern California,
Los Angeles, CA, USA

Guillermo Angeris  (24)
Bain Capital Crypto, Boston, MA, USA

Parwat Singh Anjana  (29)
Supra Research, Udaipur, India

Maryam Bahrani  (20)
Ritual, Vancouver, BC, Canada

Mirza Ahad Baig  (16)
Institute of Science and Technology Austria,
Klosterneuburg, Austria

Bhargav Nagaraja Bhatt  (31)
Web3 Foundation, Zug, Switzerland

Joseph Bonneau  (12)
New York University, NY, USA

Maxence Brugeris  (3)
LTCI, Telecom Paris, Institut Polytechnique de
Paris, France; Forvis Mazars, Levallois-Perret,
France

Benedikt Bünz  (12)
New York University, NY, USA

T-H. Hubert Chan  (7)
University of Hong Kong, Hong Kong

Jing Chen (13)
Department of Computer Science and
Technology, Tsinghua University, Beijing, China

Kani Chen  (34)
Hong Kong University of Science and
Technology, Hong Kong SAR, China

Wonseok Choi  (5)
DGIST, Daegu, South Korea

Miranda Christ  (12)
Columbia University, New York, NY, USA

Michele Ciampi  (19)
University of Edinburgh, UK

Will Cong  (10)
Cornell University, Ithaca, NY, USA

Andrei Constantinescu  (23)
ETH Zürich, Switzerland

Theo Diamandis  (24)
Bain Capital Crypto, Boston, MA, USA

Jin Dong (13)
Beijing Academy of Blockchain and Edge
Computing (BABEC), China

Yuval Efron  (12, 17)
Columbia University, New York, NY, USA

Rachid El-Azouzi  (8)
Avignon University, France

Giulia Fanti  (8)
Carnegie Mellon University,
Pittsburgh, PA, USA

Mohit Garg  (25)
Indian Institute of Science, Bengaluru, India

Samuel Gaskin  (6)
Independent Researcher, Toronto, Canada

Vahid Ghafouri  (27)
Oxford Internet Institute, UK

Pulak Ghosh  (10)
Indian Institute of Management,
Bangalore, India

Prateesh Goyal  (33)
Microsoft Reserach, Redmond, WA, USA

Christoph U. Günther  (16)
Institute of Science and Technology Austria,
Klosterneuburg, Austria

Lioba Heimbach  (23, 28)
ETH Zürich, Switzerland

Yanxue Jia  (4)
Purdue University, United States

Rohit Kapoor  (29)
Supra Research, New Delhi, India

Aniket Kate  (4)
Purdue University, United States;
Supra Research, United States

7th Conference on Advances in Financial Technologies (AFT 2025).

Editors: Zeta Avarikioti and Nicolas Christin



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- Majid Khabbazzian  (30)
Department of Electrical and Computer
Engineering, University of Alberta, Edmonton,
Canada
- Aggelos Kiayias  (21, 22)
University of Edinburgh, UK;
Input Output Global (IOG), Edinburgh, UK
- Lucianna Kiffer  (27)
IMDEA Networks, Madrid, Spain
- Jeffrey Klinck  (6)
University of Toronto, Canada
- Jovan Komatovic  (18)
École Polytechnique Fédérale de Lausanne
(EPFL), Switzerland
- Elias Koutsoupas  (21)
University of Oxford, UK
- Benjamin Kraner  (9)
Blockchain & Distributed Ledger Technologies
Group, University of Zurich, Switzerland
- Prashant Krishnamurthy  (35)
School of Computing and Information,
University of Pittsburgh, Pittsburgh, PA, USA
- Kostas Kryptos Chalkias  (2)
Mysten Labs, Palo Alto, CA, USA
- Petr Kuznetsov  (3)
LTCL, Telecom Paris, Institut Polytechnique de
Paris, France
- Victor Languille  (3)
LTCL, Telecom Paris, Institut Polytechnique de
Paris, France; EDF R&D, Paris, France
- Philip Lazos  (22)
London, UK
- Andrew Lewis-Pye  (15, 18)
London School of Economics (LSE), UK
- Jiasun Li  (10, 11)
George Mason University, Fairfax, VA, USA
- Jichen Li  (13)
Department of Computer Science and
Technology, Tsinghua University, Beijing, China
- Reina Ke Xin Li  (6)
University of Toronto, Canada
- Vincent Liu  (33)
University of Pennsylvania,
Philadelphia, PA, USA
- Xiangyu Liu  (5)
CISPA Helmholtz Center for Information
Security, Saarbrücken, Germany
- Chen-Da Liu-Zhang  (14)
Lucerne University of Applied Sciences and Arts,
Rotkreuz, Switzerland;
Web3 Foundation, Zug, Switzerland
- Bruno Llacer Trotti  (8)
Federal University of Rio de Janeiro (UFRJ),
Brazil
- Yun Lu  (19)
University of Victoria, Canada
- Mei Luo (11)
Tsinghua University, Beijing, China
- Zhongtang Luo  (4)
Purdue University, United States
- Susmita Mandal  (32)
Institute for Development and Research in
Banking Technology, Hyderabad, India
- Deepak Maram  (2)
Mysten Labs, Palo Alto, CA, USA
- Ilias Marinos  (33)
Nvidia, Redmond, WA, USA
- Evangelos Markakis  (21)
Athens University of Economics and Business,
Greece;
Input Output Global (IOG), Athens, Greece
- Christian Matt  (14)
Primev, Steinhausen, Switzerland
- Daniel Sadoc Menasché  (8)
Federal University of Rio de Janeiro (UFRJ),
Brazil
- Panagiotis Michalopoulos  (6)
University of Toronto, Canada
- Ciamac Moallemi  (24)
Graduate School of Business, Columbia
University, New York, NY, USA
- Shibam Mukherjee  (1)
Graz University of Technology, Austria;
Know Center, Graz, Austria
- Joachim Neu  (17, 18)
a16z Crypto Research, New York, NY, USA
- Michael Neuder  (20)
Ethereum Foundation, New York, NY, USA

Rafail Ostrovsky  (19)
University of California, Los Angeles (UCLA),
CA, USA

Malleesh Pai  (26)
Rice University, Houston, TX, USA;
Tempo Labs, Houston, TX, USA;
Paradigm, Houston, TX, USA

Balaji Palanisamy  (35)
School of Computing and Information,
University of Pittsburgh, Pittsburgh, PA, USA

Rahul Parmar  (29)
Supra Research, Ahmedabad, India

Paolo Penna  (22)
IOG, Zurich, Switzerland

Luca Pennella  (9)
Department of Economics, Business,
Mathematics and Statistics, University of
Trieste, Italy

Krzysztof Pietrzak  (16)
Institute of Science and Technology Austria,
Klosterneuburg, Austria

Toniann Pitassi (17)
Columbia University, New York, NY, USA

Zissis Poulos  (6)
York University, Toronto, Canada

Raghavendra Ramesh  (29)
Supra Research, Brisbane, Australia

Srivatsan Ravi  (29)
Supra Research, Los Angeles, CA, USA;
University of Southern California, Los Angeles,
CA, USA

Christian Rechberger  (1)
Graz University of Technology, Austria;
TACEO, Graz, Austria

Vinay J. Ribeiro  (32)
Indian Institute of Technology Bombay, India

Tim Roughgarden  (15, 18)
Columbia University, New York, NY, USA;
a16z Crypto Research, New York, NY, USA

Arnab Roy  (2)
Mysten Labs, Palo Alto, CA, USA

Qihong Ruan  (10)
Cornell University, Ithaca, NY, USA

Oriol Saguillo  (27)
IMDEA Networks, Madrid, Spain

Suneel Sarswat (25)
National Institute of Securities Markets,
Mumbai, India

Markus Schofnegger  (1)
Fabric Cryptography, San Francisco, CA, USA

Zhenhang Shang  (34)
Hong Kong University of Science and
Technology, Hong Kong SAR, China

Yaobin Shen  (4)
Xiamen University, China

Elaine Shi  (7)
Carnegie Mellon University,
Pittsburgh, PA, USA

Fatemeh Shirazi (31)
Web3 Foundation, Zug, Switzerland

Kirti Singh  (32)
Indian Institute of Technology Bombay, India;
Institute for Development and Research in
Banking Technology, Hyderabad, India

Srisht Fateh Singh  (6)
University of Toronto, Canada

Ozan Solmaz  (28)
ETH Zürich, Switzerland

Alistair Stewart  (31)
Web3 Foundation, Zug, Switzerland

Artem Streltsov (10)
SUNY Buffalo, Buffalo, NY, USA

Guillermo Suarez-Tangil  (27)
IMDEA Networks, Madrid, Spain

Danning Sui  (26)
Flashbots, San Francisco, CA, USA

Weizhao Tang  (8)
Carnegie Mellon University,
Pittsburgh, PA, USA

Ertem Nusret Tas  (18)
Stanford University, CA, USA

Claudio J. Tessone  (9)
UZH Blockchain Center,
University of Zurich, Switzerland

Thomas Thiery  (26)
Ethereum Foundation, Lisbon, Portugal

Søren Eller Thomsen  (14)
Partisia, Aarhus, Denmark

Joshua Tobkin (29)
Supra Research, Taipei, Taiwan

Panagiotis Tsamopoulos  (21)
Athens University of Economics and Business,
Greece

Nicolò Vallarano  (9)
UZH Blockchain Center,
University of Zurich, Switzerland

Andreas Veneris  (6)
University of Toronto, Canada

Yann Vonlanthen  (28)
ETH Zürich, Switzerland

Joy Wang  (2)
Mysten Labs, Palo Alto, CA, USA

Muzhi Wang  (11)
Central University of Finance and Economics,
Beijing, China

Roger Wattenhofer  (23, 28)
ETH Zürich, Switzerland

Zhe Wei (11)
Shantou University, China

S. Matthew Weinberg  (20)
Princeton University, NJ, USA

Fei Wu  (26)
King's College London, UK

Ke Wu  (7)
University of Michigan, Ann Arbor, MI, USA;
Carnegie Mellon University, Pittsburgh, PA,
USA

Yuntao Wu  (6)
University of Toronto, Canada

Xuanzhi Xia  (13)
Department of Computer Science and
Technology, Tsinghua University, Beijing, China

Aayush Yadav  (2)
George Mason University, Fairfax, VA, USA

Liangcheng Yu  (33)
Microsoft Research, Redmond, WA, USA;
University of Pennsylvania, Philadelphia, PA,
USA

Hamza Zarfaoui  (3)
LTCI, Telecom Paris, Institut Polytechnique de
Paris, France

Zhenyu Zhao  (34)
Hong Kong University of Science and
Technology, Hong Kong SAR, China

Wentao Zhou  (13)
Department of Computer Science and
Technology, Tsinghua University, Beijing, China

Vassilis Zikas  (5, 19)
Georgia Institute of Technology,
Atlanta, GA, USA