

6th Conference on Advances in Financial Technologies

AFT 2024, September 23–25, 2024, Vienna, Austria

Edited by

Rainer Böhme
Lucianna Kiffer



Editors

Rainer Böhme 

Universität Innsbruck, Austria
rainer.boehme@uibk.ac.at

Lucianna Kiffer 

IMDEA Networks, Madrid, Spain
lucianna.kiffer@imdea.org

ACM Classification 2012

Security and privacy → Mathematical foundations of cryptography; Theory of computation → Cryptographic primitives; Theory of computation → Cryptographic protocols; 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; Applied computing → Economics; Applied computing → Digital cash

ISBN 978-3-95977-345-4

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/978-3-95977-345-4>.

Publication date

September, 2024

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/LIPIcs.AFT.2024.0

ISBN 978-3-95977-345-4

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

- Luca Aceto (Reykjavik University, IS and Gran Sasso Science Institute, IT)
- 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)
- Daniel Král' (Masaryk University, Brno, CZ)
- Meena Mahajan (*Chair*, Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (Nanyang Technological University, SG)
- Phillip Rogaway (University of California, Davis, US)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Raimund Seidel (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)
- Pierre Senellart (ENS, Université PSL, Paris, FR)

ISSN 1868-8969

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

In memory of Ross J. Anderson.

■ Contents

| | |
|---|--------|
| Preface | |
| <i>Rainer Böhme and Lucianna Kiffer</i> | 0:xi |
| Program Committee | |
| | 0:xiii |
| Steering Committee | |
| | 0:xv |
| External Reviewers | |
| | 0:xvii |
| List of Authors | |
| | 0:xix |

Session 1: Consensus

| | |
|---|----------|
| Accountable Secret Leader Election | |
| <i>Miranda Christ, Kevin Choi, Walter McKelvie, Joseph Bonneau, and Tal Malkin</i> | 1:1–1:21 |
| BoLD: Fast and Cheap Dispute Resolution | |
| <i>Mario M. Alvarez, Henry Arneson, Ben Berger, Lee Bousfield, Chris Buckland, Yafah Edelman, Edward W. Felten, Daniel Goldman, Raul Jordan, Mahimna Kelkar, Akaki Mamageishvili, Harry Ng, Aman Sanghi, Victor Shoup, and Terence Tsao</i> | 2:1–2:19 |
| CFT-Forensics: High-Performance Byzantine Accountability for Crash Fault Tolerant Protocols | |
| <i>Weizhao Tang, Peiyao Sheng, Ronghao Ni, Pronoy Roy, Xuechao Wang, Giulia Fanti, and Pramod Viswanath</i> | 3:1–3:25 |

Session 2: Auditing

| | |
|---|----------|
| Cross Ledger Transaction Consistency for Financial Auditing | |
| <i>Vlasis Koutsos, Xiangan Tian, Dimitrios Papadopoulos, and Dimitris Chatzopoulos</i> | 4:1–4:25 |
| Proof of Diligence: Cryptoeconomic Security for Rollups | |
| <i>Peiyao Sheng, Ranvir Rana, Senthil Bala, Himanshu Tyagi, and Pramod Viswanath</i> | 5:1–5:24 |
| Analyzing and Benchmarking ZK-Rollups | |
| <i>Stefanos Chaliasos, Itamar Reif, Adrià Torralba-Agell, Jens Ernstberger, Assimakis Kattis, and Benjamin Livshits</i> | 6:1–6:24 |
| DeFiAligner: Leveraging Symbolic Analysis and Large Language Models for Inconsistency Detection in Decentralized Finance | |
| <i>Rundong Gan, Liyi Zhou, Le Wang, Kaihua Qin, and Xiaodong Lin</i> | 7:1–7:24 |

6th Conference on Advances in Financial Technologies (AFT 2024).

Editors: Rainer Böhme and Lucianna Kiffer



Leibniz International Proceedings in Informatics

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

Session 3: Blockchain Foundations

| | |
|---|------------|
| A Circuit Approach to Constructing Blockchains on Blockchains <i>Ertem Nusret Tas, David Tse, and Yifei Wang</i> | 8:1–8:25 |
| Blockchain Space Tokenization <i>Aggelos Kiayias, Elias Koutsoupias, Philip Lazos, and Giorgos Panagiotakos</i> | 9:1–9:20 |
| Optimal RANDAO Manipulation in Ethereum <i>Kaya Alpturer and S. Matthew Weinberg</i> | 10:1–10:21 |

Session 4: Payment Channels

| | |
|---|------------|
| <i>Bribe & Fork: Cheap PCN Bribing Attacks via Forking Threat</i> <i>Zeta Avarikioti, Paweł Kędzior, Tomasz Lizurej, and Tomasz Michalak</i> | 11:1–11:22 |
| Payment Censorship in the Lightning Network Despite Encrypted Communication <i>Charmaine Ndolo and Florian Tschorsch</i> | 12:1–12:24 |
| Musketeer: Incentive-Compatible Rebalancing for Payment Channel Networks <i>Zeta Avarikioti, Stefan Schmid, and Samarth Tiwari</i> | 13:1–13:22 |

Session 5: Cryptographic Building Blocks

| | |
|--|------------|
| SoK: Zero-Knowledge Range Proofs <i>Miranda Christ, Foteini Baldimtsi, Konstantinos Kryptos Chalkias, Deepak Maram, Arnab Roy, and Joy Wang</i> | 14:1–14:25 |
| Privacy Comparison for Bitcoin Light Client Implementations <i>Arad Kotzer and Ori Rottenstreich</i> | 15:1–15:23 |
| CrudiTEE: A Stick-And-Carrot Approach to Building Trustworthy Cryptocurrency Wallets with TEEs <i>Lulu Zhou, Zeyu Liu, Fan Zhang, and Michael K. Reiter</i> | 16:1–16:25 |
| Cornucopia: Distributed Randomness at Scale <i>Miranda Christ, Kevin Choi, and Joseph Bonneau</i> | 17:1–17:23 |

Session 6: Mechanisms

| | |
|--|------------|
| Loss-Versus-Fair: Efficiency of Dutch Auctions on Blockchains <i>Ciamac C. Moallemi and Dan Robinson</i> | 18:1–18:17 |
| Credible, Optimal Auctions via Public Broadcast <i>Tarun Chitra, Matheus V. X. Ferreira, and Kshitij Kulkarni</i> | 19:1–19:16 |
| Optimizing Exit Queues for Proof-Of-Stake Blockchains: A Mechanism Design Approach <i>Michael Neuder, Malleesh Pai, and Max Resnick</i> | 20:1–20:22 |
| Searcher Competition in Block Building <i>Akaki Mamagishvili, Christoph Schlegel, and Benny Sudakov</i> | 21:1–21:12 |

Session 7: Measurements

| | |
|--|------------|
| Who Wins Ethereum Block Building Auctions and Why? <i>Burak Öz, Danning Sui, Thomas Thiery, and Florian Matthes</i> | 22:1–22:25 |
| A Shortfall in Investor Expectations of Leveraged Tokens <i>Reza Rahimian and Jeremy Clark</i> | 23:1–23:24 |
| Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users <i>Marilyne Ordekian, Gilberto Atondo-Siu, Alice Hutchings, and Marie Vasek</i> | 24:1–24:24 |

Session 8: Finance

| | |
|---|------------|
| Adaptive Curves for Optimally Efficient Market Making <i>Viraj Nadkarni, Sanjeev Kulkarni, and Pramod Viswanath</i> | 25:1–25:22 |
| Competitive Policies for Online Collateral Maintenance <i>Ghada Almashaqbeh, Sixia Chen, and Alexander Russell</i> | 26:1–26:16 |
| Thinking Fast and Slow: Data-Driven Adaptive DeFi Borrow-Lending Protocol <i>Mahsa Bastankhah, Viraj Nadkarni, Chi Jin, Sanjeev Kulkarni, and Pramod Viswanath</i> | 27:1–27:23 |

Session 9: Securing Decentralized Systems

| | |
|---|------------|
| SoK: Attacks on DAOs <i>Rainer Feichtinger, Robin Fritsch, Lioba Heimbach, Yann Vonlanthen, and Roger Wattenhofer</i> | 28:1–28:27 |
| Transaction Fee Mechanism Design in a Post-MEV World <i>Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden</i> | 29:1–29:24 |
| Profitable Manipulations of Cryptographic Self-Selection Are Statistically Detectable <i>Linda Cai, Jingyi Liu, S. Matthew Weinberg, and Chenghan Zhou</i> | 30:1–30:23 |

■ Preface

This volume contains 30 papers selected from 106 submissions to the Conference on Advances in Financial Technologies (AFT '24) held at the Oesterreichische Nationalbank (OeNB) in Vienna, Austria, on 23–25 September 2024. This is the 6th year of the conference and the second year that it is independently organised and published in LIPIcs. The host institutions in Austria were the Complexity Science Hub in Vienna and the University of Innsbruck.

For the first time, this conference was co-located with the Economics of Payments XIII conference, the primary conference for economists, central bankers, and policy researchers to present and discuss their studies on topics related to payment, clearing and settlement systems. The purpose of the co-location was to foster collaboration across disciplinary boundaries and professional communities. Both conferences had an overlap day open to participants from both communities, with keynotes by Neha Narula of the Digital Currency Initiative at MIT and Charles M. Kahn of the University of Illinois and the Bank of Canada, followed by a panel discussion, and culminating in an evening reception and poster session.

AFT '24 also had an associated workshop on Scalability & Interoperability of Blockchains (SIB), co-organized by Zeta Avarikioti and Dionysis Zindros.

The paper selection process followed the conventions in computer science. Each submission received at least three 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 would like to 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 are also grateful to the AFT steering committee for their support and guidance throughout the process.

We would like to acknowledge the industry sponsors whose financial support is essential to running of AFT:

Gold level

- a16z crypto
- EigenLabs
- Kaspas

Silver level

- Ava Labs
- Gnosis Pay
- IC3
- StarkWare

We are deeply grateful to Bernhard Haslhofer, who served as General Chair. Without his initiative and sustained commitment, we would not have brought AFT '24 to Vienna, let alone held it at a central bank and in conjunction with an economics conference. We would further like to thank all the staff at the Complexity Science Hub in Vienna who made this event possible, especially Hannah Scholl, Anja Böck, Sonja Jöchtl, and Svetlana Abramova. Finally, we also would like to thank Helmut Stix, Helmut Elsinger, and Martin Summer at the OeNB for their support in co-hosting this year's AFT edition with Economics of Payments XIII.

Innsbruck, Austria
Madrid, Spain
September 2024

Rainer Böhme
Lucianna Kiffer



■ Program Committee

| | |
|---|---|
| Aggelos Kiayias, University of Edinburgh and IOG | Hong-Sheng Zhou, Virginia Commonwealth University |
| Akaki Mamageishvili, Offchain Labs | Ittay Eyal, Technion |
| Alberto Sonnino, MystenLabs and University College London | Jason Milionis, Columbia University |
| Alexander Spiegelman, Aptos Labs | Jeremy Clark, Concordia University |
| Aljoshia Judmayer, University of Vienna | Jiasun Li, George Mason University |
| Andrew Lewis-Pye, London School of Economics | Jing Chen, Tsinghua University |
| Andrew Miller, University of Illinois Urbana-Champaign | Johnnatan Messias, Matter Labs |
| Arthur Gervais, University College London | Julien Prat, IP Paris |
| Aviad Rubinstein, Stanford University | Kaihua Qin, Imperial College London |
| Aviv Zohar, The Hebrew University | Kanye Ye Wang, University of Macao |
| Aviv Yaish, The Hebrew University | Karl Wüst, Mysten Labs |
| Barnabe Monnot, Ethereum Foundation | Krzysztof Pietrzak, ISTA |
| Bernhard Haslhofer, Complexity Science Hub | Lin William (Will) Cong, Cornell University |
| Christian Cachin, University of Bern | Ling Ren, University of Illinois Urbana-Champaign |
| Ciamac Moallemi, Columbia University | Lioba Heimbach, ETH Zürich |
| Clara Shikhelman, Chaincode Labs | Marco Reuter, International Monetary Fund |
| Ethan Heilman, Massachusetts Institute of Technology DCI | Marie Vasek, University College London |
| Fahad Saleh, University of Florida | Marko Vukolić, ConsensusLab |
| Fan Zhang, Yale University | Maryam Bahrani, a16z crypto |
| Florian Tschorsch, TU Dresden | Matheus Venturyne Xavier Ferreira, University of Virginia |
| Francisco Marmolejo-Cossio, Harvard University | Neha Narula, Massachusetts Institute of Technology |
| Geoffrey Ramseyer, Stanford University | Patrick McCorry, Arbitrum Foundation |
| George Danezis, MystenLabs and University College London | Pedro Moreno-Sanchez, IMDEA Software Institute |
| Georgios Piliouras, Google DeepMind SUTD | Philipp Jovanovic, University College London |
| Ghassan Karame, Ruhr-University Bochum | Pierre-Louis Roman, Independent |
| Guy Goren, Protocol Labs | Pietro Saggese, IMT School for Advanced Studies Lucca |

6th Conference on Advances in Financial Technologies (AFT 2024).

Editors: Rainer Böhme and Lucianna Kiffer



Leibniz International Proceedings in Informatics

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

0:xiv Program Committee

Prateesh Goyal, Microsoft Research

Qiang Tang, The University of Sydney

Rafael Pass, Cornell University

Roger Wattenhofer, ETH Zürich

Sara Tucci-Piergiovanni, CEA-List and
Paris-Saclay University

Sarah Azouvi, Independent

Tarun Chitra, Gauntlet

Theo Diamandis, Massachusetts Institute of
Technology

Tim Roughgarden, Columbia University and
a16z crypto

Valeria Nikolaenko, a16z crypto

Victor Luchangco, Catholic Institute of
Technology

Yonatan Sompolinsky, Harvard University

Zeta Avarikioti, TU Vienna and Common
Prefix

■ 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

Satoshi Nakamoto (pending confirmation)

Maureen O'Hara, Cornell University

Tim Roughgarden, Columbia University

Eli Ben Sasson, Technion

Emin Gun Sirer (co-chair), Cornell University

Neha Narula ('22 PC chair), Massachusetts Institute of Technology

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

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

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

Lucianna Kiffer ('24 PC chair), IMDEA Networks


■ External Reviewers

Aditya Saraf
Alejandro Ranchal-Pedrosa
Alireza Kavousi
Álvaro García-Pérez
Amirreza Sarencheh
Benjamin Chan
Charmaine Ndolo
Chengru Zhang
Christina Ovezik
Christos Stefos
Damien Berriaud
Daniël Reijsbergen
Diana Ghinea
Erik Daniel
Faxing Wang
George Bissias
Georgios Chionas
Gilad Stern
Giorgos Panagiotakos
Giulia Scaffino
Harjasleen Malvai
Ilan Tennenhouse
Iosif Sakos
István András Seres
Jacob Leshno
Jayamine Alupotha
Jichen Li
Jorge Soares
Judith Senn
Julian Ma
Kat Molinet

Lei Yang
Lukas Aumayr
Maofan "Ted" Yin
Marc Roeschlin
Marilyne Ordekian
Maxim Jourenko
Michele Fabi
Michelle Yeo
Nicholas Stifter
Orfeas Stefanos Thyfronitis Litos
Pyrros Chaidos
Quentin Knip
Rainer Stütz
Ray Neiheiser
Rex Fernando
Ryann Sim
Sen Yang
Svetlana Abramova
Xiaohai Dai
Xinyu Li
Yann Vonlanthen
Yuheng Wang
Yunqi Li
Zhenliang Lu
Zhixuan Fang
Zhuolun Xiang
Ziling Yang


6th Conference on Advances in Financial Technologies (AFT 2024).

Editors: Rainer Böhme and Lucianna Kiffer

 LIPIC Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany


■ List of Authors

Ghada Almashaqbeh (26)
University of Connecticut, Storrs, CT, USA

Kaya Alpturer  (10)
Princeton University, NJ, USA

Mario M. Alvarez (2)
Offchain Labs, Inc., Clifton, NJ, USA

Henry Arneson (2)
Offchain Labs, Inc., Clifton, NJ, USA


Gilberto Atondo-Siu  (24)
Department of Computer Science,
University of Cambridge, UK


Zeta Avarikioti (11, 13)
Department of Informatics, TU Wien, Austria;
Common Prefix, Vienna, Austria

Maryam Bahrani (29)
Ritual, New York, NY, USA

Senthil Bala (5)
Witness Chain, Bengaluru, India

Foteini Baldimtsi  (14)
Mysten Labs, Palo Alto, CA, USA;
George Mason University, Fairfax, VA, USA

Mahsa Bastankhah  (27)
Princeton University, NJ, USA

Ben Berger  (2)
Offchain Labs, Inc., Clifton, NJ, USA

Joseph Bonneau (1, 17)
New York University, NY, USA;
a16z crypto research, New York, NY, USA

Lee Bousfield (2)
Offchain Labs, Inc., Clifton, NJ, USA

Chris Buckland (2)
Offchain Labs, Inc., Clifton, NJ, USA


Linda Cai  (30)
Princeton University, NJ, USA

Stefanos Chaliasos (6)
Imperial College London, UK

Konstantinos Kryptos Chalkias  (14)
Mysten Labs, Palo Alto, CA, USA


Dimitris Chatzopoulos  (4)
University College Dublin, Ireland

Sixia Chen (26)
Adelphi University, Garden City, NY, USA

Tarun Chitra  (19)
Gauntlet, New York, NY, USA

Kevin Choi (1, 17)
New York University, NY, USA


Miranda Christ (1, 14, 17)
Columbia University, New York, NY, USA

Jeremy Clark  (23)
Concordia, University, Montreal, Canada


Yafah Edelman (2)
Offchain Labs, Inc., Clifton, NJ, USA


Jens Ernstberger (6)
Technische Universität München, Germany

Giulia Fanti  (3)
Carnegie Mellon University,
Pittsburgh, PA, USA

Rainer Feichtinger  (28)
ETH Zürich, Switzerland

Edward W. Felten (2)
Offchain Labs, Inc., Clifton, NJ, USA


Matheus V. X. Ferreira  (19)
University of Virginia, Charlottesville, CA, USA


Robin Fritsch  (28)
ETH Zürich, Switzerland


Rundong Gan (7)
School of Computer Science,
University of Guelph, Canada

Pranav Garimidi (29)
a16z Crypto, New York, NY, USA

Daniel Goldman (2)
Offchain Labs, Inc., Clifton, NJ, USA

Lioba Heimbach  (28)
ETH Zürich, Switzerland

Alice Hutchings  (24)
Department of Computer Science,
University of Cambridge, UK

Chi Jin  (27)
Princeton University, NJ, USA

Raul Jordan (2)
Offchain Labs, Inc., Clifton, NJ, USA

Assimakis Kattis (6)
Athens, Greece

6th Conference on Advances in Financial Technologies (AFT 2024).

Editors: Rainer Böhme and Lucianna Kiffer




Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

- Mahimna Kelkar  (2)
Offchain Labs, Inc., Clifton, NJ, USA
- Aggelos Kiayias  (9)
University of Edinburgh, UK;
IOG, London, UK
- Arad Kotzer  (15)
The Department of Computer Science,
Technion, Haifa, Israel
- Vlasis Koutsos  (4)
Hong Kong University of Science and
Technology, Hong Kong
- Elias Koutsoupas  (9)
University of Oxford, UK
- Kshitij Kulkarni  (19)
UC Berkeley, CA, USA
- Sanjeev Kulkarni  (25, 27)
Princeton University, NJ, USA
- Paweł Kędzior (11)
University of Warsaw, Poland
- Philip Lazos  (9)
Jump Trading, London, UK
- Xiaodong Lin  (7)
School of Computer Science,
University of Guelph, Canada
- Jingyi Liu  (30)
Princeton University, NJ, USA
- Zeyu Liu  (16)
Yale University, New Haven, CT, USA
- Benjamin Livshits (6)
Imperial College London, UK;
Matter Labs, London, UK
- Tomasz Lazurek (11)
NASK, Warsaw, Poland;
University of Warsaw, Poland
- Tal Malkin (1)
Columbia University, New York, NY, USA
- Akaki Mamageishvili  (2, 21)
Offchain Labs, Inc., Clifton, NJ, USA;
Offchain Labs, Zurich, Switzerland
- Deepak Maram  (14)
Mysten Labs, Palo Alto, CA, USA
- Florian Matthes  (22)
Technical University of Munich,
Garching, Germany
- Walter McKelvie (1)
Columbia University, New York, NY, USA
- Tomasz Michalak (11)
IDEAS NCBR, Warsaw, Poland;
University of Warsaw, Poland
- Ciamac C. Moallemi  (18)
Graduate School of Business, Columbia
University, New York, NY, USA
- Viraj Nadkarni  (25, 27)
Princeton University, NJ, USA
- Charmaine Ndolo  (12)
Dresden University of Technology, Germany
- Michael Neuder (20)
Ethereum Foundation, New York, NY, USA
- Harry Ng (2)
Offchain Labs, Inc., Clifton, NJ, USA
- Ronghao Ni  (3)
Carnegie Mellon University,
Pittsburgh, PA, USA
- Marilyne Ordekian  (24)
Department of Computer Science,
University College London, UK
- Malleesh Pai  (20)
Special Mechanisms Group, Consensys Inc,
Dallas, TX, USA;
Rice University, Houston, TX, USA
- Giorgos Panagiotakos  (9)
IOG, Athens, Greece
- Dimitrios Papadopoulos  (4)
Hong Kong University of Science and
Technology, Hong Kong
- Kaihua Qin (7)
Yale University, New Haven, CT, USA;
UC Berkeley RDI, CA, USA;
Decentralized Intelligence AG, Zug, Switzerland
- Reza Rahimian  (23)
Concordia University, Montreal, Canada
- Ranvir Rana  (5)
Witness Chain, NJ, USA
- Itamar Reif (6)
Austria, New York, NY, USA
- Michael K. Reiter  (16)
Duke University, New Haven, CT, USA
- Max Resnick (20)
Special Mechanisms Group, Consensys Inc,
Dallas, TX, USA

- Dan Robinson (18)
Paradigm, San Francisco, CA, USA
- Ori Rottenstreich  (15)
The Department of Computer Science and the
Department of Electrical and Computer
Engineering, Technion, Haifa, Israel
- Tim Roughgarden (29)
a16z Crypto, New York, NY, USA;
Columbia University, New York, NY, USA
- Arnab Roy  (14)
Mysten Labs, Palo Alto, CA, USA
- Pronoy Roy (3)
Carnegie Mellon University,
Pittsburgh, PA, USA
- Alexander Russell (26)
University of Connecticut, Storrs, CT, USA;
IOG, Singapore
- Aman Sanghi (2)
Offchain Labs, Inc., Clifton, NJ, USA
- Christoph Schlegel (21)
Flashbots, George Town, Cayman Islands
- Stefan Schmid  (13)
TU Berlin, Germany;
Fraunhofer SIT, Berlin, Germany;
Weizenbaum Institute, Berlin, Germany
- Peiyao Sheng  (3, 5)
University of Illinois Urbana-Champaign, IL,
USA;
Witness Chain, NJ, USA
- Victor Shoup  (2)
Offchain Labs, Inc., Clifton, NJ, USA
- Benny Sudakov  (21)
ETH Zürich, Switzerland
- Danning Sui  (22)
Flashbots, San Francisco, CA, USA
- Weizhao Tang  (3)
Carnegie Mellon University,
Pittsburgh, PA, USA
- Ertem Nusret Tas  (8)
Stanford University, CA, USA
- Thomas Thiery  (22)
Ethereum Foundation, Lisbon, Portugal
- Xiangnan Tian  (4)
Hong Kong University of Science and
Technology, Hong Kong
- Samarth Tiwari  (13)
Centrum Wiskunde & Informatica,
Amsterdam, The Netherlands
- Adrià Torralba-Agell (6)
Universitat Oberta de Catalunya,
San Martí, Spain
- Terence Tsao (2)
Offchain Labs, Inc., Clifton, NJ, USA
- Florian Tschorsch  (12)
Dresden University of Technology, Germany
- David Tse  (8)
Stanford University, CA, USA
- Himanshu Tyagi (5)
Witness Chain, Bengaluru, India
- Marie Vasek  (24)
Department of Computer Science,
University College London, UK
- Pramod Viswanath  (3, 5, 25, 27)
Princeton University, NJ, USA;
Witness Chain, NJ, USA
- Yann Vonlanthen  (28)
ETH Zürich, Switzerland
- Joy Wang  (14)
Mysten Labs, Palo Alto, CA, USA
- Le Wang  (7)
School of Computer Science,
University of Guelph, Canada
- Xuechao Wang  (3)
Hong Kong University of Science and
Technology, Guangzhou, China
- Yifei Wang  (8)
Stanford University, CA, USA
- Roger Wattenhofer  (28)
ETH Zürich, Switzerland
- S. Matthew Weinberg  (10, 30)
Princeton University, NJ, USA
- Fan Zhang  (16)
Yale University, New Haven, CT, USA
- Chenghan Zhou  (30)
Stanford University, Palo Alto, CA, USA
- Liyi Zhou (7)
The University of Sydney, Australia;
UC Berkeley RDI, CA, USA;
Decentralized Intelligence AG, Zug, Switzerland

0:xxii Authors

Lulu Zhou  (16)
Yale University, New Haven, CT, USA

Burak Öz  (22)
Technical University of Munich,
Garching, Germany