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.

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.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

7th Conference on Advances in Financial Technologies (AFT 2025).
Editors: Zeta Avarikioti and Nicolas Christin
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Session 3: Measurements

Session 4: Consensus I

Session 5: Consensus II

Session 6: Incentives and Tokenomics

Session 7: Mechanism Design for Fees and Markets

Session 8: Empirical Analysis and MEV

Session 9: Scalability and Interoperability

Session 10: Cryptocurrency Markets and Adoption

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

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

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
LIPICS 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

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

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

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 Brugeres (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
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Majid Khabbazian (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 Koutsoupias (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)
LTCI, Telecom Paris, Institut Polytechnique de Paris, France

Victor Languille (3)
LTCI, Telecom Paris, Institut Polytechnique de Paris, France; EDF R&D, Paris, France

Philip Lazos (22)
London, UK

Andrew Lewis-Pye (15, 18)
London Schoool 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

Mallesh 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