

5th Conference on Advances in Financial Technologies

AFT 2023, October 23-25, 2023, Princeton, NJ, USA

Edited by

Joseph Bonneau

S. Matthew Weinberg



Editors

Joseph Bonneau

New York University, NY, USA
jcb@cs.nyu.edu

S. Matthew Weinberg 

Princeton University, NJ, USA
smweinberg@princeton.edu

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; Theory of computation → Algorithmic mechanism design; Applied computing → Economics; Applied computing → Digital cash

ISBN 978-3-95977-303-4

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/978-3-95977-303-4>.

Publication date

October, 2023

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.2023.0

ISBN 978-3-95977-303-4

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 (*Chair*, Reykjavik University, IS and Gran Sasso Science Institute, IT)
- Christel Baier (TU Dresden, DE)
- Roberto Di Cosmo (Inria and Université de Paris, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Daniel Král' (Masaryk University, Brno, CZ)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (University of Oxford, GB)
- 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>

■ Contents

Preface	
<i>Joseph Bonneau and S. Matthew Weinberg</i>	0:ix
Program Committee	
.....	0:xi–0:xii
Steering Committee	
.....	0:xiii
External Reviewers	
.....	0:xv
Authors	
.....	0:xvii–0:xix

Regular Papers

Privacy-Preserving Transactions with Verifiable Local Differential Privacy	
<i>Danielle Mousowitz Davidow, Yacov Manevich, and Eran Toch</i>	1:1–1:23
Correct Cryptocurrency ASIC Pricing: Are Miners Overpaying?	
<i>Aviv Yaish and Aviv Zohar</i>	2:1–2:25
F3B: A Low-Overhead Blockchain Architecture with Per-Transaction Front-Running Protection	
<i>Haoqian Zhang, Louis-Henri Merino, Ziyang Qu, Mahsa Bastankhah, Vero Estrada-Galiñanes, and Bryan Ford</i>	3:1–3:23
Designing Multidimensional Blockchain Fee Markets	
<i>Theo Diamandis, Alex Evans, Tarun Chitra, and Guillermo Angeris</i>	4:1–4:23
Security Analysis of Filecoin’s Expected Consensus in the Byzantine vs Honest Model	
<i>Xuechao Wang, Sarah Azouvi, and Marko Vukolić</i>	5:1–5:21
Tailstorm: A Secure and Fair Blockchain for Cash Transactions	
<i>Patrik Keller, Ben Glickenshaus, George Bissias, and Gregory Griffith</i>	6:1–6:26
STROBE: Streaming Threshold Random Beacons	
<i>Donald Beaver, Konstantinos Chalkias, Mahimna Kelkar, Lefteris Kokoris-Kogias, Kevin Lewi, Ladi de Naurois, Valeria Nikolaenko, Arnab Roy, and Alberto Sonnino</i>	7:1–7:16
User Participation in Cryptocurrency Derivative Markets	
<i>Daisuke Kawai, Bryan Routledge, Kyle Soska, Ariel Zetlin-Jones, and Nicolas Christin</i>	8:1–8:24
DeFi Lending During The Merge	
<i>Lioba Heimbach, Eric Schertenleib, and Roger Wattenhofer</i>	9:1–9:25
FairPoS: Input Fairness in Permissionless Consensus	
<i>James Hsin-yu Chiang, Bernardo David, Ittay Eyal, and Tiantian Gong</i>	10:1–10:23

5th Conference on Advances in Financial Technologies (AFT 2023).

Editors: Joseph Bonneau and S. Matthew Weinberg

Leibniz International Proceedings in Informatics



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

Correlated-Output Differential Privacy and Applications to Dark Pools <i>James Hsin-yu Chiang, Bernardo David, Mariana Gama, and Christian Janos Lebeda</i>	11:1–11:23
SoK: Privacy-Enhancing Technologies in Finance <i>Carsten Baum, James Hsin-yu Chiang, Bernardo David, and Tore Kasper Frederiksen</i>	12:1–12:30
Decentralization Cheapens Corruptive Majority Attacks <i>Stephen H. Newman</i>	13:1–13:19
Proofs of Proof-Of-Stake with Sublinear Complexity <i>Shresth Agrawal, Joachim Neu, Ertem Nusret Tas, and Dionysis Zindros</i>	14:1–14:24
Condorcet Attack Against Fair Transaction Ordering <i>Mohammad Amin Vafadar and Majid Khabbazian</i>	15:1–15:21
Pay Less for Your Privacy: Towards Cost-Effective On-Chain Mixers <i>Zhipeng Wang, Marko Cirkovic, Duc V. Le, William Knottenbelt, and Christian Cachin</i>	16:1–16:25
Non-Atomic Payment Splitting in Channel Networks <i>Stefan Dziembowski and Paweł Kędzior</i>	17:1–17:23
Revisiting the Nova Proof System on a Cycle of Curves <i>Wilson D. Nguyen, Dan Boneh, and Srinath Setty</i>	18:1–18:22
Censorship Resistance in On-Chain Auctions <i>Elijah Fox, Malleesh M. Pai, and Max Resnick</i>	19:1–19:20
The Centralizing Effects of Private Order Flow on Proposer-Builder Separation <i>Tivas Gupta, Malleesh M. Pai, and Max Resnick</i>	20:1–20:15
When Bidders Are DAOs <i>Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden</i>	21:1–21:21
Fast and Furious Withdrawals from Optimistic Rollups <i>Mahsa Moosavi, Mehdi Salehi, Daniel Goldman, and Jeremy Clark</i>	22:1–22:17
Buying Time: Latency Racing vs. Bidding for Transaction Ordering <i>Akaki Mamageishvili, Mahimna Kelkar, Jan Christoph Schlegel, and Edward W. Felten</i>	23:1–23:22
Batching Trades on Automated Market Makers <i>Andrea Canidio and Robin Fritsch</i>	24:1–24:17
Strategic Liquidity Provision in Uniswap V3 <i>Zhou Fan, Francisco Marmolejo-Cossio, Daniel Moroz, Michael Neuder, Rithvik Rao, and David C. Parkes</i>	25:1–25:22
Post-Quantum Single Secret Leader Election (SSLE) from Publicly Re-Randomizable Commitments <i>Dan Boneh, Aditi Partap, and Lior Rotem</i>	26:1–26:23
Liquidity Management Attacks on Lending Markets <i>Alireza Arjmand and Majid Khabbazian</i>	27:1–27:21

Analysis of CryptoNote Transaction Graphs Using the Dulmage-Mendelsohn
Decomposition
Saravanan Vijayakumaran 28:1–28:22

Vector Commitments with Efficient Updates
Ertim Nusret Tas and Dan Boneh 29:1–29:23

Time Is Money: Strategic Timing Games in Proof-Of-Stake Protocols
*Caspar Schwarz-Schilling, Fahad Saleh, Thomas Thiery, Jennifer Pan,
Nihar Shah, and Barnabé Monnot* 30:1–30:17

Practical Large-Scale Proof-Of-Stake Asynchronous Total-Order Broadcast
Orestis Alpos, Christian Cachin, Simon Holmgard Kamp, and Jesper Buus Nielsen 31:1–31:22

■ Preface

This volume contains 31 papers selected out of 100 submissions for the 5th Conference on Advances in Financial Technologies (AFT ‘23) held on October 23–25, 2023. Each paper received detailed reviews by several program committee members and external reviewers.

The conference was held at Princeton University in Princeton, NJ. Each accepted paper was presented via a 15-minute live presentation, followed by a 5-minute question/answer period with the audience.

Two full-day workshops were co-located with AFT on October 26. Aniket Kate and Andrew Miller co-organized the workshop on Decentralized Credit Networks (DCN), and Christian Cachin and Giuliano Losa co-organized the workshop on Heterogeneous Trust in Distributed Systems (HTDS).

We would like to thank all Program Committee members and subreviewers 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, and especially Ittay Eyal, for their support and guidance throughout the process.

We are also extremely thankful to our industry sponsors, whose financial support is essential to running AFT:

- a16z Crypto (gold-level)
- Ava Labs (gold-level)
- IC3 (silver-level)
- IOHK (silver-level)
- DeCenter (silver-level)
- StarkWare (silver-level)

We also thank the IACR for granting AFT ‘in cooperation’ status.

Finally, we would like to thank all of the staff at Princeton University who made this event possible, and especially Elizabeth Wang, Michele Brown, and Mitra Kelly.



■ Program Committee

Aggelos Kiayias, University of Edinburgh
Alberto Sonnino, Meta
Alexander Spiegelman, Aptos
Andrew Hall, Stanford University
Andrew Lewis-Pye, London School of Economics
Andrew Miller, University of Illinois Urbana-Champaign
Anthony Lee Zhang, University of Chicago Booth School of Business
Ari Juels, Cornell Tech
Arthur Gervais, University College London
Aviad Rubinfeld, Stanford University
Barnabe Monnot, Ethereum Foundation
Benedikt Bünz, New York University
Bo Waggoner, University of Colorado Boulder
Charalampos Papamanthou, Yale University
Chenghan Zhou, Princeton University
Ciamac Moallemi, Columbia University Graduate School of Business
Clara Shikhelman, Chaincode Labs
Edgar Weippl, University of Vienna
Elli Androulaki, IBM Research
Ethan Heilman, Boston University & BastionZero
Fahad Saleh, Wake Forest University
Fan Zhang, Duke University
Foteini Baldimtsi, George Mason University
Francisco Marmolejo-Cossio, Harvard University
Geoffrey Ramseyer, Stanford University
Georgios Pilouras, Singapore University of Technology and Design
Ghassan Karame, NEC Laboratories Europe
Guillermo Angeris, Bain Capital
Guy Goren, Technion
Hong-Sheng Zhou, Virginia Commonwealth University
Ittay Eyal, Technion
Jacob Leshno, University of Chicago Booth School of Business
Jason Milionis, Columbia University
Jeremy Clark, Concordia University
Jiasun Li, George Mason University
Jing Chen, Algorand
Julien Prat, Ecole Polytechnique
Justin Thaler, Georgetown University & a16z crypto
Konstantinos Chalkias, Mysten Labs
Romaric Ludinard, IMT Atlantique / IRISA
Malte Moser, Chainalysis
Marco Reuter, University of Mannheim
Marie Vasek, University College London
Marko Vukolić, IBM
Maryam Bahrani, a16z crypto
Matheus Venturyne Xavier Ferreira, Harvard University
Nicolas Christin, Carnegie-Mellon University
Nirvan Tyagi, Cornell University
Patrick McCorry, Infura
Patrick O'Grady, Avalanche
Pramod Viswanath, University of Illinois, Urbana-Champaign
Pranav Garimidi, a16z crypto
Qiang Tang, University of Sydney
Rafael Pass, Cornell

5th Conference on Advances in Financial Technologies (AFT 2023).

Editors: Joseph Bonneau and S. Matthew Weinberg



Leibniz International Proceedings in Informatics

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

0:xii Program Committee

Rainer Böhme, University of Innsbruck

Sara Tucci-Piergiovanni, Polytechnique

Scott Kominers, Harvard University Business School

Shaanan Cohney, University of Melbourne

Tarun Chitra, Gauntlet

Tyler Moore, University of Tulsa

Valeria Nikolaenko, a16z crypto

Vasilis Zikas, Purdue University

Victor Luchangco, Algorand

Wanyi Dai Li, Lightspark

Will Cong, Cornell University & DEFT Lab & NBER

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

Satoshi Nakamoto (pending confirmation)

Maureen O'Hara, Cornell University

Tim Roughgarden, Columbia University &
a16z Crypto

Eli Ben Sasson, Technion & StarkWare

Emin Gun Sirer (co-chair), Cornell
University & Avalanche

Sarah Meiklejohn ('20 PC chair), UCL

Abhi Shelat ('20 PC chair), Northeastern
University

Foteini Baldimtsi ('21 PC chair), George
Mason 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

5th Conference on Advances in Financial Technologies (AFT 2023).
Editors: Joseph Bonneau and S. Matthew Weinberg



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

■ External Reviewers

Adithya Bhat, Purdue University
Alejandro Ranchal-Pedrosa, Protocol Labs
Aljosha Judmayer, SBA Research
Amirreza Sarencheh, University of
Edinburgh & IOHK
Angelo De Caro, IBM Zurich
Antonella Del Pozzo, CEA LIST
Balaji Arun, Aptos
Eliza Oak, Yale University
Ertem Nusret Tas, Stanford University
Hanwen Feng, University of Sydney
Ioannis Tzannetos, NTUA
Istvan Seres, Eotvos Lorand University
Mahimna Kelkar, Cornell University
Marc Roeschlin, IOG
Muhammad Ishaq, Purdue University
Nicholas Stifter, TU Wien
Philip Lazos, IOHK
Pouriya Zarbafian, University of Sydney
Tuanir Franca Rezende, CEA LIST
Yacov Manevich, IBM Research Zurich
Yu Shen, University of Edinburgh
Yu Wei, Purdue University
Zhuolun Xiang, Aptos

■ List of Authors

- Shresth Agrawal  (14)
Technische Universität München, Germany
- Orestis Alpos (31)
University of Bern, Switzerland
- Guillermo Angeris (4)
Bain Capital Crypto, San Francisco, CA, USA
- Alireza Arjmand  (27)
University of Alberta, Edmonton, Canada
- Sarah Azouvi  (5)
Protocol Labs, San Francisco, CA, USA
- Maryam Bahrani (21)
a16z Crypto, New York, NY, USA
- Mahsa Bastankhah (3)
École Polytechnique Fédérale de Lausanne,
Switzerland
- Carsten Baum (12)
Technical University of Denmark, Lyngby,
Denmark
- Donald Beaver (7)
Independent Scholar, Pittsburgh, PA, USA
- George Bissias (6)
University of Massachusetts Amherst, MA, USA
- Dan Boneh  (18, 26, 29)
Stanford University, CA, USA
- Andrea Canidio  (24)
CoW Protocol, Lisbon, Portugal
- Konstantinos Chalkias (7)
Mysten Labs, Palo Alto, CA, USA
- James Hsin-yu Chiang  (10, 11, 12)
Aarhus University, Denmark
- Tarun Chitra (4)
Gauntlet, New York, NY, USA
- Nicolas Christin  (8)
Carnegie Mellon University, Pittsburgh, PA,
USA
- Marko Cirkovic (16)
University of Bern, Switzerland
- Jeremy Clark  (22)
Concordia University, Montreal, Canada
- Bernardo David (10, 11, 12)
IT University of Copenhagen, Denmark
- Ladi de Naurois (7)
Washington DC, USA
- Theo Diamandis (4)
MIT CSAIL, Cambridge, MA, USA
- Stefan Dziembowski  (17)
University of Warsaw, Poland; IDEAS NCBR,
Warsaw, Poland
- Vero Estrada-Galiñanes (3)
École Polytechnique Fédérale de Lausanne,
Switzerland
- Alex Evans (4)
Bain Capital Crypto, San Francisco, CA, USA
- Ittay Eyal  (10)
Technion, Haifa, Israel
- Zhou Fan (25)
Harvard University, Cambridge, MA, USA
- Edward W. Felten (23)
Offchain Labs, Washington, D.C., USA
- Bryan Ford (3)
École Polytechnique Fédérale de Lausanne,
Switzerland
- Elijah Fox (19)
Duality Labs, New York, NY, USA, USA
- Tore Kasper Frederiksen (12)
Zama, Paris, France
- Robin Fritsch (24)
Cow Protocol, Lisbon, Portugal; ETH Zürich,
Switzerland
- Mariana Gama  (11)
COSIC, KU Leuven, Belgium
- Pranav Garimidi (21)
a16z Crypto, New York, NY, USA
- Ben Glickenhau (6)
University of Massachusetts Amherst, MA, USA
- Daniel Goldman (22)
OffchainLabs, Princeton, NJ, USA
- Tiantian Gong  (10)
Purdue University, West Lafayette, IN, USA
- Gregory Griffith (6)
Bitcoin Unlimited
- Tivas Gupta (20)
Special Mechanisms Group, USA

5th Conference on Advances in Financial Technologies (AFT 2023).

Editors: Joseph Boneau and S. Matthew Weinberg




Leibniz International Proceedings in Informatics

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

- Lioba Heimbach  (9)
ETH Zürich, Switzerland
- Simon Holmgaard Kamp (31)
Aarhus University, Denmark
- Daisuke Kawai  (8)
Carnegie Mellon University, Pittsburgh, PA, USA
- Mahimna Kelkar (7, 23)
Cornell University, New York City, NY, USA
- Patrik Keller (6)
Universität Innsbruck, Austria
- Majid Khabbazian  (15, 27)
University of Alberta, Edmonton, Canada
- William Knottenbelt (16)
Imperial College London, UK
- Lefteris Kokoris-Kogias (7)
Mysten Labs, London, UK; IST Austria, Klosterneuburg, Austria
- Paweł Kędzior  (17)
University of Warsaw, Poland
- Duc V. Le (16)
Visa Research, Sunnyvale, CA, USA
- Christian Janos Lebeda  (11)
IT University of Copenhagen, Denmark; Basic Algorithms Research Copenhagen, Denmark
- Kevin Lewi (7)
Meta Platforms, Inc., Menlo Park, CA, USA
- Akaki Mamagishvili (23)
Offchain Labs, Zürich, Switzerland
- Yacov Manevich  (1)
IBM Research - Zürich, Switzerland
- Francisco Marmolejo-Cossio (25)
Harvard University, Cambridge, MA, USA; IOG, USA
- Louis-Henri Merino (3)
École Polytechnique Fédérale de Lausanne, Switzerland
- Barnabé Monnot  (30)
Ethereum Foundation, Berlin, Germany
- Mahsa Moosavi (22)
Concordia University, Montreal, Canada; OffchainLabs, Princeton, NJ, USA
- Daniel Moroz (25)
Harvard University, Cambridge, MA, USA
- Danielle Movsowitz Davidow  (1)
Tel-Aviv University, Israel
- Joachim Neu  (14)
Stanford University, CA, USA
- Michael Neuder (25)
Harvard University, Cambridge, MA, USA
- Stephen H. Newman (13)
Princeton University, NJ, USA
- Wilson D. Nguyen (18)
Stanford University, CA, USA
- Jesper Buus Nielsen (31)
Aarhus University, Denmark
- Valeria Nikolaenko (7)
a16z crypto, Palo Alto, CA, USA
- Mallesh M. Pai  (19, 20)
Department of Economics, Rice University, Houston, TX, USA; Special Mechanisms Group, USA
- Jennifer Pan (30)
Jump Crypto, Chicago, IL, USA
- David C. Parkes (25)
Harvard University, Cambridge, MA, USA
- Aditi Partap (26)
Stanford University, CA, USA
- Ziyan Qu (3)
École Polytechnique Fédérale de Lausanne, Switzerland
- Rithvik Rao (25)
Harvard University, Cambridge, MA, USA
- Max Resnick  (19, 20)
Special Mechanisms Group, USA
- Lior Rotem (26)
Stanford University, CA, USA
- Tim Roughgarden (21)
a16z Crypto, New York, NY, USA; Columbia University, New York, NY, USA
- Bryan Routledge  (8)
Carnegie Mellon University, Pittsburgh, PA, USA
- Arnab Roy (7)
Mysten Labs, Palo Alto, CA, USA
- Fahad Saleh  (30)
Wake Forest University, Winston Salem, NC, USA

Mehdi Salehi (22)
OffchainLabs, Princeton, NJ, USA

Eric Schertenleib  (9)
ETH Zürich, Switzerland

Jan Christoph Schlegel (23)
City, University of London, UK

Caspar Schwarz-Schilling  (30)
Ethereum Foundation, Berlin, Germany

Srinath Setty (18)
Microsoft Research, Redmond, WA, USA

Nihar Shah (30)
Jump Crypto, Chicago, IL, USA


Alberto Sonnino (7)
Mysten Labs, London, UK; University College
London, UK


Kyle Soska  (8)
Ramiel Capital, New York, NY, USA


Ertem Nusret Tas  (14, 29)
Stanford University, CA, USA

Thomas Thiery  (30)
Ethereum Foundation, Lyon, France

Eran Toch  (1)
Tel-Aviv University, Israel


Mohammad Amin Vafadar  (15)
University of Alberta, Edmonton, Canada


Saravanan Vijayakumaran  (28)
Department of Electrical Engineering, Indian
Institute of Technology Bombay, Mumbai, India

Marko Vukolić  (5)
Protocol Labs, San Francisco, CA, USA

Xuechao Wang  (5)
Thrust of Financial Technology, HKUST(GZ),
Guangzhou, China


Zhipeng Wang (16)
Imperial College London, UK


Roger Wattenhofer  (9)
ETH Zürich, Switzerland

Aviv Yaish  (2)
The Hebrew University of Jerusalem, Israel

Ariel Zetlin-Jones  (8)
Carnegie Mellon University, Pittsburgh, PA,
USA

Haoqian Zhang (3)
École Polytechnique Fédérale de Lausanne,
Switzerland

Dionysis Zindros  (14)
Stanford University, CA, USA

Aviv Zohar  (2)
The Hebrew University of Jerusalem, Israel

