FAN ZHANG

51 Prospect St
New Haven, CT 06511

E-mail: f.zhang@yale.edu
Homepage: https://fanzhang.me

CURRENT POSITIONS

Assistant Professor July 2022 – *present*
Department of Computer Science, Yale University, New Haven, CT, USA

Affiliations: The Initiative for Cryptocurrencies and Contracts (IC3), NSF Center for Distributed Confidential Computing (CDCC), Center for Algorithms, Data, and Market Design at Yale (CADMY).

Faculty Advisor: Chainlink Labs (2021-)

EDUCATION

Ph.D. in Computer Science 2014 – 2020
Cornell University
Thesis: *Protocols For Connecting Blockchains With Off-Chain Systems*
Advisor: Prof. Ari Juels

B.Eng. in Electronic Engineering 2010 – 2014
Tsinghua University, China

RESEARCH

I'm broadly interested in computer security and applied cryptography, especially techniques that enable Secure Decentralized Systems.

Impact: My research has led to direct industry adoption. DECO is part of Chainlink's Platform Privacy Suite. Town Crier has have been licensed to Chainlink. In addition, at least ten startup companies are building variants of these works, collectively known as zkTLS. Ekiden is used in Oasis Labs' products. ZipNet is being implemented by Flashbots. zkBridge is implemented by Polyhedra Network.

AWARDS

- USENIX Security Test of Time Award, "Stealing Machine Learning Models via Prediction APIs" 2026
- Notable Reviewer Award, USENIX Security 25 2025
- Gift from Flashbots 2025
- NSF award for "PDaSP Track 2: Confidential Genome Imputation and Analytics (CoGIA)" 2025
- IC3 Research Grant 2025
- Ethereum Academic Grant (with Fatima and Giannis) 2025
- Ethereum Academic Grant (with Jiasun Li and Aviv Yaish) 2025
- Sui Academic Research Award 2024
- Ethereum Academic Grant (with Mengqian Zhang) 2024
- zkGrant from Ethereum Foundation (with Wenhao Wang) 2024
- MEV Fellowship Grants from Flashbots 2023
- Yale Roberts Innovation Fund Award 2023
- NSF award for "SaTC: Frontiers: Center for Distributed Confidential Computing (CDCC)" 2022

- Ethereum Academic Grant: *Catching the ephemeral: Understanding blockchains through mempool data* 2022
- Ethereum Academic Grant: *Disentangling Transaction Privacy and Consensus in Ethereum* 2022
- Ethereum Academic Grant: *Understanding Waiting Time in Transaction Fee Mechanisms* 2022
- IBM PhD Fellowship Award 2018-2020
- Academic Excellence Scholarship, Tsinghua University, China 2013
- National Scholarship, the Ministry of Education of China 2012
- Freshman Scholarship, Tsinghua University, China 2010

PUBLICATIONS

Bibliometrics from Google Scholar: citations = 7201, h-index = 23, i10-index = 30 (as of August 2025).

Manuscripts and preprints

7. Sarah Allen, Pranay Anchuri, James Austgen, Maryam Bahrani, Samuel Breckenridge, Aaron Buchwald, Christian Cachin, Andres Fabrega, Jared Fernandez, James Hsin-yu Chiang, Marwa Mouallem, Roi Bar-Zur, Neil DeSilva, Ittay Eyal, Giulia Fanti, Ari Juels, Andrew Miller, Christian Sillaber, Dani Vilardell, Pramod Viswanath, Wenhao Wang, Matt Weinberg, Sen Yang, Jianzhu Yao, and **Fan Zhang**. *Crypto x AI, AI x Crypto: A Survey*. Edited by Giulia Fanti and Ari Juels. 2026. arXiv: 2606.13892

6. Katerina Sotiraki, Yunhao Wang, and **Fan Zhang**. *Dinocchio: Distributed Prover for Ring Arithmetic*. Cryptology ePrint Archive, Paper 2026/159. 2026

5. Ioannis Kaklamanis, Wenhao Wang, Harjasleen Malvai, and **Fan Zhang**. *Verifiable Aggregate Receipts with Applications to User Engagement Auditing*. Cryptology ePrint Archive, Paper 2025/2330. 2025

4. Ignacy Nieweglowski, Aviv Yaish, Fahad Saleh, and **Fan Zhang**. *PoliFi Tokens and the Trump Effect*. 2025. arXiv: 2512.06036

3. Jayamine Alupotha, Mariarosaria Barbaraci, Ioannis Kaklamanis, Abhimanyu Rawat, Christian Cachin, and **Fan Zhang**. *Anonymous Self-Credentials and their Application to Single-Sign-On*. Cryptology ePrint Archive, Paper 2025/618. 2025

2. Sarisht Wadhwa, Julian Ma, Thomas Thiery, Barnabe Monnot, Luca Zanolini, **Fan Zhang**, and Kartik Nayak. *AUCIL: An Inclusion List Design for Rational Parties*. Cryptology ePrint Archive, Paper 2025/194. 2025

1. Ioannis Kaklamanis and **Fan Zhang**. CRATE*: Cross-Rollup Atomic Transaction Execution*. 2025. arXiv: 2502.04659 [cs.CR]

Conference papers

39. Katerina Sotiraki, Yunhao Wang, and **Fan Zhang**. "Encore: Aggregatable FHE-over-SNARK with Constant Proof Size". In: *2027 IEEE Symposium on Security and Privacy (SP)* (May 17–19, 2027). To appear. IEEE, 2027

38. Mengqian Zhang, Sen Yang, Kartik Nayak, and **Fan Zhang**. "Boost+: Equitable, Incentive-Compatible Block Building". In: *Network and Distributed System Security Symposium*. To appear. 2027. arXiv: 2602.04007

37. Haofei Liang, Zeyu Liu, Yunhao Wang, Xiang Xie, Yu Yu, and **Fan Zhang**. "Relect: Single Secret Leader Election via FHE with Reduced Computation and Communication and Transparent Setup". In: *ACM Conference on Computer and Communications Security*. To appear. 2026

36. Fatima Elsheimy, Ioannis Kaklamanis, Sarisht Wadhwa, Charalampos Papamanthou, and **Fan Zhang**. "Censorship Resistance vs Throughput in Multi-Proposer BFT Protocols". In: *ACM Conference on Computer and Communications Security*. To appear. 2026

35. Sen Yang, Kaihua Qin, Aviv Yaish, and **Fan Zhang**. "Insecurity Through Obscurity: Veiled Vulnerabilities in Closed-Source Contracts". In: *ACM Conference on Computer and Communications Security*. To appear. 2026

34. Sarisht Wadhwa, Aviv Yaish, **Fan Zhang**, and Kartik Nayak. "Perils of Parallelism: Transaction Fee Mechanisms under Execution Uncertainty". In: *USENIX Security Symposium*. 2026

33. Sen Yang, Burak Öz, Fei Wu, and **Fan Zhang**. "Geographical Centralization Resilience in Ethereum's Block-Building Paradigms". In: *ACM SIGMETRICS*. 2026

32. Wenhao Wang, Aditya Saraf, Lioba Heimbach, Kushal Babel, and **Fan Zhang**. "Blockspace Under Pressure: An Analysis of Spam MEV on High-Throughput Blockchains". In: *Science of Blockchain Conference*. 2026

31. Wenhao Wang, Fangyan Shi, Dani Vilardell, and **Fan Zhang**. "Cirrus: Performant and Accountable Distributed SNARK". in: *Network and Distributed System Security Symposium*. 2026

30. Mengqian Zhang, Sen Yang, and **Fan Zhang**. "RediSwap: MEV Redistribution Mechanism for CFMMs". In: *Proceedings of the 2025 Workshop on Decentralized Finance and Security*. DeFi '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 27–36. ISBN: 9798400719042

29. Hongbo Chen, Quan Zhou, Sen Yang, Xing Han, **Fan Zhang**, Danfeng Zhang, and Xiaofeng Wang. "AGORA: Open More and Trust Less in Binary Verification Service". In: *OOPSLA*. 2025

28. Yunhao Wang and **Fan Zhang**. "Qelect: lattice-based single secret leader election made practical". In: *Proceedings of the 34th USENIX Conference on Security Symposium*. SEC '25. Seattle, WA, USA: USENIX Association, 2025. ISBN: 978-1-939133-52-6

27. Michael Rosenberg, Maurice Shih, Zhenyu Zhao, Rui Wang, Ian Miers, and **Fan Zhang**. "ZIPNet: Low-bandwidth anonymous broadcast from (dis)Trusted Execution Environments". In: *Proc. Priv. Enhancing Technol.* 2025.2 (2025), pp. 211–225

26. Sen Yang, Kartik Nayak, and **Fan Zhang**. "Decentralization of Ethereum's Builder Market". In: 2025 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, May 1, 2025, pp. 1512–1530. ISBN: 979-8-3315-2236-0

25. Wenhao Wang, Lulu Zhou, Aviv Yaish, **Fan Zhang**, Ben Fisch, and Benjamin Livshits. "*Proo*ϕ: A ZKP Market Mechanism". In: *Financial Cryptography and Data Security - 29th International Conference, FC 2025, Miyakojima, Japan, April 14-18, 2025, Revised Selected Papers, Part I*. ed. by Christina Garman and Pedro Moreno-Sanchez. Vol. 15751. Lecture Notes in Computer Science. Springer, Apr. 2025, pp. 180–196

24. Sen Yang, **Fan Zhang**, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. "SoK: MEV Countermeasures". In: *Proceedings of the Workshop on Decentralized Finance and Security*. DeFi '24. Salt Lake City, UT, USA: Association for Computing Machinery, 2024, pp. 21–30. ISBN: 9798400712272

23. Chon Kit Lao, Sophie Zhou, Luyao Zhang, **Fan Zhang**, and Kanye Ye Wang. "Unpacking Long-Latency Transactions in Ethereum". In: *Proceedings of the Workshop on Decentralized Finance and Security*. DeFi '24. Salt Lake City, UT, USA: Association for Computing Machinery, 2024, pp. 11–20. ISBN: 9798400712272

22. Lulu Zhou, Zeyu Liu, **Fan Zhang**, and Michael K. Reiter. "CrudiTEE: A Stick-And-Carrot Approach to Building Trustworthy Cryptocurrency Wallets with TEEs". In: *LIPIcs, Volume 316, AFT 2024* 316 (2024), 16:1–16:25. ISSN: 1868-8969

21. Michael Mirkin, Lulu Zhou, Ittay Eyal, and **Fan Zhang**. "Sprints: Intermittent Blockchain PoW Mining". In: *USENIX Security*. 2024

20. Sarisht Wadhwa, Luca Zanolini, Francesco D'Amato, Aditya Asgaonkar, **Fan Zhang**, and Kartik Nayak. "Breaking the Chains of Rationality: Understanding the Limitations to and Obtaining Order Policy Enforcement". In: *ACM CCS*. 2024

19. Weijie Wang, Yujie Lu, Charalampos Papamanthou, and **Fan Zhang**. "The Locality of Memory Checking". In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*. Ed. by Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda. ACM, 2023, pp. 1820–1834

18. Rongwu Xu, Sen Yang, **Fan Zhang**, and Zhixuan Fang. "MISO: Legacy-compatible Privacy-preserving Single Sign-on using Trusted Execution Environments". In: *8th IEEE European Symposium on Security and Privacy, EuroS&P 2023, Delft, Netherlands, July 3-7, 2023*. IEEE, 2023, pp. 352–372

17. Jianyi Zhang, Ang Li, Minxue Tang, Jingwei Sun, Xiang Chen, **Fan Zhang**, Changyou Chen, Yiran Chen, and Hai Li. "Fed-CBS: A Heterogeneity-Aware Client Sampling Mechanism for Federated Learning via Class-Imbalance Reduction". In: *Proceedings of the 40th International Conference on Machine Learning*. International Conference on Machine Learning. PMLR, July 3, 2023, pp. 41354–41381

16. Sarisht Wadhwa, Jannis Stoeter, **Fan Zhang**, and Kartik Nayak. "He-HTLC: Revisiting Incentives in HTLC". in: *Network and Distributed System Security (NDSS) Symposium 2023*. San Diego, CA, USA, 2023

15. Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, **Fan Zhang**, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. "zkBridge: Trustless Cross-chain Bridges Made Practical". In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022*. ACM, 2022, pp. 3003–3017

14. Yulin Liu, Yuxuan Lu, Kartik Nayak, **Fan Zhang**, Luyao Zhang, and Yinhong Zhao. "Empirical Analysis of EIP-1559: Transaction Fees, Waiting Times, and Consensus Security". In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM, 2022, pp. 2099–2113

13. Deepak Maram, Harjasleen Malvai, **Fan Zhang**, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability". In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 1348–1366

12. **Fan Zhang**, Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. "DECO: Liberating Web Data Using Decentralized Oracles for TLS". in: *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM, 2020, pp. 1919–1938

11. Mahimna Kelkar, **Fan Zhang**, Steven Goldfeder, and Ari Juels. "Order-Fairness for Byzantine Consensus". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*. ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Lecture Notes in Computer Science. Springer, 2020, pp. 451–480

10. Sai Krishna Deepak Maram, **Fan Zhang**, Lun Wang, Andrew Low, Yupeng Zhang, Ari Juels, and Dawn Song. "CHURP: Dynamic-Committee Proactive Secret Sharing". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. Ed. by Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz. ACM, 2019, pp. 2369–2386

9. Raymond Cheng, **Fan Zhang**, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song. "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts". In: *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*. IEEE, 2019, pp. 185–200

8. **Fan Zhang**, Philip Daian, Iddo Bentov, Ian Miers, and Ari Juels. "Paralysis Proofs: Secure Dynamic Access Structures for Cryptocurrency Custody and More". In: *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019*. ACM, 2019, pp. 1–15

7. Iddo Bentov, Yan Ji, **Fan Zhang**, Lorenz Breidenbach, Philip Daian, and Ari Juels. "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. Ed. by Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz. ACM, 2019, pp. 1521–1538

6. **Fan Zhang**, Ittay Eyal, Robert Escriva, Ari Juels, and Robbert van Renesse. "REM: Resource-Efficient Mining for Blockchains". In: *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*. Ed. by Engin Kirda and Thomas Ristenpart. USENIX Association, 2017, pp. 1427–1444

5. Florian Tramèr, **Fan Zhang**, Huang Lin, Jean-Pierre Hubaux, Ari Juels, and Elaine Shi. "Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge". In: *2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017*. IEEE, 2017, pp. 19–34

4. Ethan Cecchetti, **Fan Zhang**, Yan Ji, Ahmed E. Kosba, Ari Juels, and Elaine Shi. "Solidus: Confidential Distributed Ledger Transactions via PVORM". in: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. Ed. by Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu. ACM, 2017, pp. 701–717

3. Florian Tramèr, **Fan Zhang**, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Stealing Machine Learning Models via Prediction APIs". In: *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*. Ed. by Thorsten Holz and Stefan Savage. USENIX Association, 2016, pp. 601–618

2. **Fan Zhang**, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. "Town Crier: An Authenticated Data Feed for Smart Contracts". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. ACM, 2016, pp. 270–282

1. Longqi Yang, Yin Cui, **Fan Zhang**, John P. Pollak, Serge J. Belongie, and Deborah Estrin. "PlateClick: Bootstrapping Food Preferences Through an Adaptive Visual Interface". In: *Proceedings of the 24th ACM International Conference on Information and Knowledge Management, CIKM 2015, Melbourne, VIC, Australia, October 19 - 23, 2015*. Ed. by James Bailey, Alistair Moffat, Charu C. Aggarwal, Maarten de Rijke, Ravi Kumar, Vanessa Murdock, Timos K. Sellis, and Jeffrey Xu Yu. ACM, 2015, pp. 183–192

Journal articles

2. Jian Liu, Peilun Li, **Fan Zhang**, and Kui Ren. " monoCashmonoCash: A Channel-Free Payment Network via Trusted Monotonic Counters ". In: *IEEE Transactions on Dependable and Secure Computing* 21.05 (Sept. 2024), pp. 4770–4783. ISSN: 1941-0018

1. **Fan Zhang**, Warren He, Raymond Cheng, Jernej Kos, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song. "The Ekiden Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts". In: *IEEE Secur. Priv.* 18.3 (2020), pp. 17–27

Tech reports

2. Sen Yang, **Fan Zhang**, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. *SoK: MEV Countermeasures: Theory and Practice*. Dec. 9, 2022. arXiv: 2212.05111 [cs]. URL: http://arxiv.org/abs/2212.05111 (visited on 06/08/2023). preprint

1. Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and **Fan Zhang**. *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations*. Working Paper 27634. (Authors are orderred alphabetically by last names.) National Bureau of Economic Research, Aug. 2020

Patents

4. **Fan Zhang**, Sai Krishna Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. "Decentralized Techniques for Verification of Data in Transport Layer Security and Other Contexts". U.S. pat. 11997107B2. Cornell University. May 28, 2024

3. Iddo Bentov, Ari Juels, **Fan Zhang**, Philip Daian, and Lorenz Breidenbach. "Real-time cryptocurrency exchange using trusted hardware". Cornell University. US Patent App. 16/198,223. 2017

2. **Fan Zhang**, Ethan Cecchetti, Kyle Croman, Ari Juels, and Runting Shi. "Authenticated data feed for blockchains". Cornell University. US Patent No. 11829998. 2017

1. Jun Bi, **Fan Zhang**, and Yonghong Fu. "Horizontal direction communication method for heterogeneous SDN and SDN system". CN Patent ZL 2015 1 0041960.7. 2015

GRANTS

15. Gift from Flashbots, PI, October 2025.

14. NSF Award 2452612: "PDaSP Track 2: Confidential Genome Imputation and Analytics (CoGIA)", Co-PI, August 2025.

13. IC3 Research Grant, PI, July 2025.

12. Ethereum Academic Grant: *Censorship-Resistance vs Throughput in Multi-Proposer Protocols*, PI (with graduate students Fatima and Giannis), July 2025.

11. Ethereum Academic Grant: *A Cryptographic Cookbook for Mechanism Designers*, Co-PI (with Jiasun Li and Aviv Yaish), July 2025.

10. Uniswap Foundation TLDR Fellowship: Co-PI (with postdoc Mengqian Zhang), July 2024.

9. Sui Academic Research Award: PI, June 2024.

8. Ethereum Academic Grant: *Understanding and Enhancing Efficiency and Robustness in MEV-Boost Auctions*, Co-PI (with postdoc Mengqian Zhang), May 2024.

7. zkGrant from Ethereum Foundation: *Cirrus: Performant and Robust Distributed SNARK Generation via Computation Delegation*. PI, May 2024.

6. Gift from Flashbots. PI, 2023.

5. Yale Roberts Innovation Fund Award. PI, 2023.

4. NSF SaTC: "Frontiers: Center for Distributed Confidential Computing (CDCC)", Co-PI, August 2022.

3. Ethereum Academic Grant: *Disentangling Transaction Privacy and Consensus in Ethereum*, Co-PI (with Kartik Nayak (Duke)), August 2022.

2. Ethereum Academic Grant: *Catching the ephemeral: Understanding blockchains through mempool data.* Co-PI with Kartik Nayak (Duke), August 2022.

1. Ethereum Academic Grant: *Understanding Waiting Time in Transaction Fee Mechanisms*, Co-PI (with Luyao Zhang (DKU)), August 2022.

TEACHING AND ADVISING

Courses

- *CPSC 3640: Decentralized Payments, Contracts, and Finance for Humans and AI* Fall 2026
- *CPSC 444/544: Real-World Cryptography* Spring 2026
- *CPSC 444/544: Real-World Cryptography* Spring 2025
- *CPSC 466/566: Blockchain and Cryptocurrency* Fall 2024
- *CPSC 466/566: Blockchain and Cryptocurrency* Spring 2024
- *CPSC 364: Introduction to Blockchains, Cryptocurrencies, and Smart Contracts* Fall 2023
- *CPSC 666: Secure Decentralized Systems* Spring 2023

Current Ph.D. students

- Sen Yang (2022-)
- Giannis Kaklamanis (2023-)
- Wenhao Wang (2023-)
- Yunhao Wang (2023-)

Doctoral dissertation committees

- Zhenliang Lu. Thesis: *Towards Optimal and Practical Asynchronous Byzantine Fault Tolerant Protocols*. The University of Sydney. 2023.
- Jinyuan Jia. Duke University. 2022; now Assistant Professor at Penn State.
- Taylor A. Hardin. Dartmouth. 2022.

Area exams committees

- Fatima Elsheimy
- Josh Beal
- Grace Jia
- Mahdi Soleimani
- Weijie Wang
- Arthur Lazaretti

Master's thesis committees

- Yunhao Wang. Thesis: *Group Oblivious Message Retrieval*. Columbia University, 2023.

Undergrad mentees (490 projects)

- Tarun Kota. *Design and Evaluation of Multi-Agent AI Oracle Systems for Prediction Market Resolution*. **Outstanding Senior Project Award.** Spring 2026
- Roshan Palakkal 2025 Fall
- Inssia Ahmed 2025 Fall
- Sophia Zhou 2025 Fall

- Yiğit Kılıçoğlu 2024 Fall
- Yuhang Cui. *Blockchain-Based Bug Bounty System for Genomic Data* Spring 2024
- Andrew Wang. *Designing and Building a Keyless Wallet with Signature Oracles* Fall 2023
- Megha Joshi. Title: *A Decentralized Need for Speed: An Empirical Investigation into Transaction Latency and Construction of Predictive Machine Learning Models for Blockchain* Spring 2023
- Justin Ye. Title: *An Empirical Exploration of MEV Block Auctions on Ethereum* Spring 2023

Research interns

- Jiayu Liu 2026
- Yoshi Sato, now Ph.D. student at Yale 2025
- Yanxin Pang, now Ph.D. student at Georgia Tech 2024
- Fangyan Shi 2024
- Rui Wang (MS student), now Ph.D. student at Purdue 2023
- Yixiao Wang, now MS student at Cornell 2023
- Chengrui Fang 2023
- Zhenyu Zhao, now Ph.D. student at HKUST Crypto-Fintech Lab 2023
- Rongwu Xu, now Ph.D. student at UW 2022
- Zerui Cheng, now Ph.D. student at Princeton 2022
- Shutong Qu 2022
- Yuxuan Lu, now Ph.D. student at Peking University 2021

Alumni

- Aviv Yaish (Postdoc Associate, 2024-2026), now Assistant Professor at Georgia Institute of Technology
- Tiantian Gong (Postdoc Associate, 2025-2026), now Assistant Professor at Nanyang Technological University
- Sarisht Wadhwa (Duke Ph.D., 2021-2026; co-advised with Kartik Nayak), now Postdoctoral Researcher at the University of Michigan
- Lulu Zhou (2021-2024), now at EigenLayer
- Yujie Lu (2022-2024, co-advised with Charalampos (Babis) Papamanthou)
- Mengqian Zhang (Postdoc Associate, 2023-2025), now Postdoctoral Researcher at CMU
- Kaihua Qin (Postdoctoral Researcher, 2023-2025), now Assistant Professor at the University of Warwick

PROFESSIONAL SERVICES

Program committee chairs

- ACM CCS Workshop on DeFi and Security 2023 (co-chair with Kaihua Qin)
- ACM CCS Workshop on DeFi and Security 2022 (co-chair with Patrick McCorry)

Program committee members

- Asiacrypt 2026
- USENIX Security 2023, 2024, 2025, 2026
- ACM CCS 2021, 2022, 2023, 2024, 2025, 2026
- IEEE Symposium on Security & Privacy (Oakland) 2023
- ACM Advances in Financial Technologies (AFT) 2021, 2023, 2024,2025, 2026
- Privacy-Enhancing Technologies (PETS) 2021, 2022
- Financial Cryptography 2021, 2022, 2023
- Science of Blockchain Conference (SBC) 2021, 2022, 2023, 2024, 2025, 2026
- Designing DeFi (D^2) 2026
- The Latest in DeFi Research (TLDR) Conference 2025
- Web3 Scholars Conference 2026

- ACM CCS DeFi Workshop, 2024, 2025
- FC DeFi Workshop, 2021, 2022, 2023, 2024

Associate editor

- ACM Transactions on Privacy and Security (ToPS) 2024-

Reviewer

USENIX Security (2016), Nature Sustainability (2018), TCC (2019), FC (2019), CCS (2020), CRYPTO (2020). IEEE Transactions on Dependable and Secure Computing, ACM Transactions on Privacy and Security, ACM Computing Surveys, ACM Transactions on Networks

Other services

- NSF Panelist — March 2023

Department services

- Summer Internship Program — 2025, 2026
- Visit day organizer — 2025, 2026
- Colloquium czar — 2024
- PhD student admission committee — 2023,2024,2025
- Faculty Search Committee — 2023
- Infrastructure committee — 2022

INVITED TALKS

2026

- Keynote at Shape Rotator, "*Reversing the Panopticon: Decentralized Auditing of Trusted Platforms*", March 2026
- Invited talk at DeCenter Seminar, "*Equitable, Incentive-Compatible Block Building*", Princeton, NJ, February 2026

2025

- Invited talk at CBER Crafting the Cryptoeconomy Conference, "*Overview of Oracles*", October 2025
- Invited talk at ETH NYC'25, "*Oracles, 'zkTLS', and Data Liberation*", August 2025
- Invited talk at NoConsensus.wtf 2025 @ SBC, "*ZipNet*", August 2025
- Invited talk at IC3 Blockchain Camp, "*DECO: Oracles, 'zkTLS', and Data Liberation*", June 2025

2024

- Invited talk at Dagstuhl Seminar on Secure Distributed Computing, "*Merry TEEs and Secure Distributed Computing*", Germany, September 2024
- Invited talk at SBC MEV Workshop 2024, "*Using TEEs without trusting them*", August 2024
- Guest lecture at Berkeley DeFi MOOC, "*Decentralization of Ethereum's builder market*", October 2024
- Invited talk at CBER Crafting the Cryptoeconomy Conference, "*Decentralization of Ethereum's builder market*", October 2024
- Invited talk at Decentralized Science (DeSci) Seminar, "*Decentralization of Ethereum's builder market*", University of Sydney (Remote), October 2024
- Invited talk at Science of Blockchain Conference (SBC), "*Decentralization of Ethereum's builder market*", New York, NY, August 2024

- Invited talk at IC3 Blockchain Camp, "*Decentralization of Ethereum's builder market*", New York, NY, June 2024
- Invited talk at EC24 Workshop on Blockchains and Decentralized Finance, "*Decentralization of Ethereum's builder market*", July 2024

2023

- Invited talk at Confidential Computing Consortium 2023, "*Toward Trust Minimization in TEE and Applications*", April 2023
- Invited talk at IC3 Blockchain Camp, "*zkBridge*", New York, NY, August 2023

2022

- Invited talk at 1st ACE Symposium on Privacy, Accountability, Verification, and Economics of Blockchain Systems, "*zkBridge*", New Haven, CT, April 2022
- Invited talk at IC3 Blockchain Camp, "*He-HTLC: revisiting incentives in HTLC*", Ithaca, NY, August 2022
- Invited talk at a16z, "*He-HTLC: revisiting incentives in HTLC*", New York, NY, August 2022

2021

- Invited talk at The West Lake Forum on Network Security, "*CanDID: Can-Do Decentralized Identity*", Online, November 2021

2020

- Invited talk at JD Security Seminar, "*The Oracle Problem*", November 2020
- Invited talk at Annual Convention of Chinese Institute of Engineers - Greater New York Chapter, "*CanDID: Can-Do Decentralized Identity*", October 2020
- Invited talk at Empire Hacking (organized by Trail of Bits), "*CanDID: Can-Do Decentralized Identity*", October 2020
- Invited talk at W3C Credential Community Group (CCG), "*DECO: Liberating Web Data Using Decentralized Oracles for TLS*", October 2020
- Invited talk at Stanford Blockchain Conference (SBC'20), "*DECO: Liberating Web Data Using Decentralized Oracles for TLS*", Stanford University, February 2020
- Invited talk at Real World Crypto (RWC'20), "*DECO: Liberating Web Data Using Decentralized Oracles for TLS*", New York City, January 2020
- Invited talk at IC3 Webinar, "*Connecting Blockchains to the Real World*", August 2020
- Invited talk at Rutgers University, "*Connecting Blockchains to the Real World*", April 2020 (Cancelled due to COVID-19)
- Invited talk at Purdue University, "*Connecting Blockchains to the Real World*", March 2020 (Cancelled due to COVID-19)
- Invited talk at Washington University in St. Louis, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at Duke University, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at Georgetown University, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at University of Michigan, Ann Arbor, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at ETH Zurich, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at University of California, Santa Cruz, "*Connecting Blockchains to the Real World*", March 2020
- Invited talk at University of California, Santa Barbara, "*Connecting Blockchains to the Real World*", February 2020
- Invited talk at Penn State, "*Connecting Blockchains to the Real World*", February 2020
- Invited talk at University at Buffalo, "*Connecting Blockchains to the Real World*", February 2020

2019

- Invited talk at CISPA - Helmholtz Center for Information Security, "*Connecting Blockchains to the Real World*", Saarbrucken, Germany, November 2019
- Invited talk at ETH Zurich, "*Connecting Blockchains to the Real World*", October 2019
- Invited talk at IBM PhD Fellow Talk, "*Connecting Blockchains to the Real World*", IBM Watson Research Center, September 2019
- Invited talk at ACM CCS'19, "*CHURP: Proactive Secret Sharing with Dynamic Committee*", London, UK, November 2019
- Invited talk at Northeastern University, Cybersecurity Speaker Series, "*On Trusted Hardware and Blockchain Hybridization*", January 2019
- Invited talk at ACM AFT 2019, "*Paralysis Proof*", Zurich, Switzerland, October 2019

2018

- Invited talk at MIT, CSAIL, "*On Trusted Hardware and Blockchain Hybridization*", November 2018
- Invited talk at New York University, CS Colloquium, "*On Trusted Hardware and Blockchain Hybridization*", October 2018
- Invited talk at IC3 Bootcamp, "*CHURP: Proactive Secret Sharing with Dynamic Committee*", Ithaca, NY, July 2018
- Invited talk at IC3 Retreat, "*Paralysis Proof*", New York City, May 2018
- Invited talk at 5th Bitcoin Workshop, Financial Crypto'18, "*Paralysis Proof*", Curacao, March 2018

2017

- Invited talk at USENIX Security'17, "*REM*", Vancouver, BC, Canada, August 2017
- Invited talk at Silicon Valley Ethereum Meetup, "*Town Crier*", Santa Clara, CA, August 2017
- Invited talk at IC3 Retreat, "*Town Crier*", San Francisco, CA, March 2017

2016

- Invited talk at CCS'16, "*Town Crier*", Vienna, Austria, October 2016
- Invited talk at IC3 Retreat, "*Town Crier*", New York City, May 2016

Guest lectures

- "Oracles", *CS 6431 Security and Privacy Technologies*, Cornell — Fall 2021
- "Oracles", *DeFi Security*, UC Berkeley — Spring 2021
- "Oracles", *CS 291D*, UCSB — Fall 2020

PAST EMPLOYMENT

Assistant Professor in Computer Science — June 2021 – June 2022
Duke University — Durham, NC

ChainLink/SmartContract Inc. — August 2020 – July 2021
Senior Researcher — New York, NY

Cornell University — August 2014 – August 2020
Graduate Research Assistant — Ithaca, NY (14-18) / New York, NY (18-20)

Oasis Labs — May 2018 – August 2018
Research Scientist — Berkeley, CA

Security & Privacy Research, Intel Labs — July 2017 – August 2017
Researcher — Hillsboro, OR

Intel Opensource Technology Center (01.org) June 2013 – May 2014
Intern Beijing, China

SELECTED MEDIA COVERAGE

- *Forbes*, "Chainlink's New Acquisition From Cornell University Could Transform Blockchain For Good", on August 29, 2020.
- *CoinDesk*, "Chainlink Acquires Blockchain Oracle Solution From Cornell University", on August 29, 2020.
- *CoinTelegraph*, "Chainlink acquires a privacy-preserving oracle protocol from Cornell University", on August 29, 2020.
- *PR Newswire*, "Chainlink Acquires DECO from Cornell University", on August 29, 2020.
- *MIT Technology Review*, "Blockchain smart contracts are finally good for something in the real world", on November 19, 2018.
- *Forbes*, "Cornell's Town Crier Acquired By Chainlink To Expand Decentralized Oracle Network", on November 1, 2018.
- *BitcoinExchangeGuide*, "Chainlink Blockchain Company Acquires Cornell's Town Crier to Bolster Native Smart Contract Network" on November 2, 2018.
- *Unhashed*, "Chainlink Acquires Town Crier, a Hardware-Based Oracle", on November 3, 2018.
- *Forbes*, "Big Hitter Crypto Funds Pile Into Privacy-Enhanced Smart Contract Startup Oasis Labs", on July 9, 2018.
- *BitcoinMagazine*, "Cornell IC3 Researchers Propose Solution to Bitcoin's Multisig *Paralysis* Problem", on January 19, 2018.
- *IEEE Spectrum*, "The Ridiculous Amount of Energy It Takes to Run Bitcoin", on September 28, 2017.
- *CoinDesk*, "Trust Your Oracle? Cornell Launches Tool for Confidential Blockchain Queries", on May 17, 2017.
- *MIT Technology Review*, "How Encrypted Weather Data Could Help Corporate Blockchain Dreams Come True", on May 11, 2017.
- *ETHNews*, "Town Crier Service Delivers Solid Data To Coders", on May 11, 2017.

REFERENCES

Contact information available upon request.

Updated on Thursday 15th October, 2026.