# 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

**Senior researcher**, Chainlink Labs August 2020 – *present*

## 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
Beijing, China

## Research

My research focuses on solving security problems in real-world systems with cryptography. In particular, I am interested in decentralized systems such as blockchains, anonymous communication, and trusted execution environments (TEEs).

**Industry adoption.** My research has led to direct industry adoption. Town Crier [ZCC+16] and DECO [ZMM+20b] have been licensed to Chainlink. Ekiden [CZK+19] is used in Oasis Labs' products.

## Awards / Grants

- MEV Fellowship Grants from Flashbots 2023
- Yale Roberts Innovation Fund Award 2023
- NSF SaTC: Frontiers: Center for Distributed Confidential Computing (CDCC). With PIs from IU (Lead), CMU, Duke, OSU, Penn State, Purdue, Spelman, UIUC. 2022
- Ethereum Academic Grant for "Catching the ephemeral: Understanding blockchains through mempool data.". 2022
- Ethereum Academic Grant for "Disentangling Transaction Privacy and Consensus in Ethereum". 2022
- Ethereum Academic Grant for "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

# Teaching and Advising

## Courses

- *CPSC 466/566: Blockchain and Cryptocurrency*, Yale University — Spring 2024
- *CPSC 364: Introduction to Blockchains, Cryptocurrencies, and Smart Contracts*, Yale University — Fall 2023
- *CPSC 666: Secure Decentralized Systems*, Yale University — Spring 2023
- *CS 590.02, Cryptocurrency and Cryptography*, Duke University — Fall 2021

## Current Ph.D. Students

- Lulu Zhou (2021-)
- Sarisht Wadhwa (2021-, co-advised with Kartik Nayak)
- Sen Yang (2022-)
- Yujie Lu (2022-, co-advised with Charalampos (Babis) Papamanthou)
- 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.

## Master's thesis committees

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

## Senior Projects

- 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

# Publications

Bibliometrics can be found in Google Scholar.

## Manuscripts

4. Michael Mirkin, Lulu Zhou, Ittay Eyal, and **Fan Zhang**. *Sprints: Intermittent Blockchain PoW Mining*. Cryptology ePrint Archive, Paper 2023/626. https://eprint.iacr.org/2023/626. 2023

3. 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*. 2023. URL: https://eprint.iacr.org/2023/868 (visited on 07/14/2023). preprint

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

## Conference papers

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, Los Angeles, CA, USA, November 7-11, 2022*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. 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, Paris, France, April 26-28, 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. J. Liu, P. Li, F. Zhang, and K. Ren. "monoCash: A Channel-Free Payment Network Via Trusted Monotonic Counters". In: *IEEE Transactions on Dependable and Secure Computing* 01 (Jan. 5555), pp. 1–14. 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

### Patents and patent applications

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". Cornell University. US Patent App. 62/894,052. 2020

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

6. MEV Fellowship Grants from Flashbots. 2023.

5. Yale Roberts Innovation Fund Award. 2023.

4. NSF SaTC: Frontiers: Center for Distributed Confidential Computing (CDCC). This is a multi-institution effort, involving faculty from IU (Lead), CMU, Duke, OSU, Penn State, Purdue, Spelman, UIUC and Yale. Awarded August 2022.

3. Ethereum Foundation. *Disentangling Transaction Privacy and Consensus in Ethereum.* With Kartik Nayak (Duke). August 2022.

2. Ethereum Foundation. *Catching the ephemeral: Understanding blockchains through mempool data.* With Kartik Nayak (Duke). August 2022.

1. Ethereum Foundation. *Understanding Waiting Time in Transaction Fee Mechanisms.* With Luyao Zhang (DKU). August 2022.

## 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

- USENIX Security 2023, 2024
- IEEE Symposium on Security & Privacy (Oakland) 2023
- ACM CCS 2021, 2022, 2023, 2024
- Privacy-Enhancing Technologies (PETS) 2021, 2022
- ACM Advances in Financial Technologies (AFT) 2021, 2023, 2024
- Financial Cryptography 2021, 2022, 2023
- Science of Blockchain Conference (SBC) 2021, 2022, 2023, 2024
- FC DeFi Workshop, 2021, 2022, 2023, 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

## Employment

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

**ChainLink/SmartContract Inc.** — August 2020 – present
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

## Invited Talks

**zkBridge**

- 1st ACE Symposium on Privacy, Accountability, Verification, and Economics of Blockchain Systems April 2022
- IC3 Blockchain Camp, New York, NY — August 2023

**He-HTLC: revisiting incentives in HTLC**

- IC3 Blockchain Camp, Ithaca, NY — August 2022
- a16z, New York, NY — August 2022

**The oracle problem**

- The Oracle Problem, JD Security Seminar — November 2020

**CanDID: Can-Do Decentralized Identity**

- The West Lake Forum on Network Security — Online, November 2021
- The annual convention of Chinese Institute of Engineers - Greater New York Chapter — October 2020
- Empire Hacking (organized by Trail of Bits) — October 2020

**DECO: Liberating Web Data Using Decentralized Oracles for TLS**

- W3C Credential Community Group (CCG) — October 2020
- Stanford Blockchain Conference (SBC'20), Stanford University — February 2020
- Real World Crypto (RWC'20), New York City — January 2020

**Connecting Blockchains to the Real World**

- IC3 Webinar — August 2020
- Rutgers University — April 2020 (cancelled due to Covid19)
- Purdue University — March 2020 (cancelled due to Covid19)
- Washington University in St. Louis — March 2020
- Duke University — March 2020
- Georgetown University — March 2020
- University of Michigan, Ann Arbor — March 2020
- ETH Zürich — March 2020
- University of California, Santa Cruz — March 2020
- University of California, Santa Barbara — February 2020
- Penn State — February 2020
- University at Buffalo — February 2020
- CISPA—Helmholtz Center for Information Security, Saarbrücken, Germany — November 2019
- ETH Zürich — October 2019
- IBM PhD fellow talk at IBM Watson Research Center. — September 2019

**CHURP: Proactive Secret Sharing with Dynamic Committee**

- ACM CCS'19, London, UK — November 2019
- IC3 Bootcamp, Ithaca NY — July, 2018

**On Trusted Hardware and Blockchain Hybridization**

- Northeastern University, Cybersecurity Speaker Series — January 2019
- MIT, CSAIL — November 2018
- New York University, CS Colloquium — October 2018

**Paralysis Proof**

- ACM AFT 2019, Zürich, Switzerland — October 2019
- IC3 Retreat, New York City — May 2018
- 5th Bitcoin Workshop, Financial Crypto'18, Curacao — March 2018

**REM**

- USENIX Security'17, Vancouver BC, Canada — August 2017

**Town Crier**

- Silicon Valley Ethereum Meetup, Santa Clara, CA — August 2017
- IC3 Retreat, San Francisco, CA — March 2017
- CCS'16, Vienna, Austria — October 2016
- IC3 Retreat, 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

## 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 Tuesday 13th February, 2024.