Fan Zhang

E-mail: fanz@cs.duke.edu
Homepage: https://fanzhang.me

Current Position

Assistant Professor *Starting 2021 Fall*
Department of Computer Science, Duke University

Senior Researcher August, 2020-*present*
ChainLink

Education

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

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

Research

I am broadly interested in computer security, privacy, applied cryptography, and distributed computing. My recent focus has been the security/privacy problems in decentralized systems, especially those enabled by blockchain protocols and trusted execution environments.

Industry adoption. My research has led to direct industry adoption. Town Crier [CCS16] was licensed from Cornell by Chainlink. Ekiden [EuroSP19] is used in Oasis Labs' products. CHURP [CCS19a] is on Oasis Labs product roadmap. DECO [CCS20] is under licensing negotiation.

Publications

Bibliometrics can be found in Google Scholar. **Papers denoted * means authors are ordered alphabetically by last name**.

Manuscripts

[ACE+20] 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

[SP21] 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: *IEEE Symposium on Security and Privacy*. 2021.

[CCS20] **Fan Zhang**, Sai Krishna Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. "DECO: Liberating Web Data Using Decentralized Oracles for TLS". In: *ACM CCS. To appear*. 2020.

[Crypto20] Mahimna Kelkar, **Fan Zhang**, Steven Goldfeder, and Ari Juels. "Order-Fairness for Byzantine Consensus". In: *Advances in Cryptology - CRYPTO*. Springer, 2020, pp. 451–480.

[CCS19a] 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*. ACM, 2019, pp. 2369–2386.

[EuroSP19] 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.

[AFT19] **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.

[CCS19b] 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*. ACM, 2019, pp. 1521–1538.

[UseSec17] **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*. USENIX Association, 2017, pp. 1427–1444.

[EuroSP17] 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.

[CCS17] 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*. ACM, 2017, pp. 701–717.

[UseSec16] 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*. USENIX Association, 2016, pp. 601–618.

[CCS16] **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*. ACM, 2016, pp. 270–282.

[CIKM15] 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*. ACM, 2015, pp. 183–192.

Journal articles

[ZHC+20] F. Zhang, W. He, R. Cheng, J. Kos, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song. "The Ekiden Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts". In: *IEEE Security Privacy* 18.3 (2020), pp. 17–27.

Patents and patent applications

[ZCC+17] **Fan Zhang**, Ethan Cecchetti, Kyle Croman, Ari Juels, and Runting Shi. "Authenticated data feed for blockchains". Cornell University. US Patent App. 15/615,216. 2017.

[BJZ+17] 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.

[BZF15] Jun Bi, **Fan Zhang**, and Yonghong Fu. "Horizontal direction communication method for heterogeneous SDN (Self-defending network) and SDN system". CN Patent `ZL 2015 1 0041960.7`. 2015.

Awards

- 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

Employment

ChainLink/SmartContract Inc. Aug 2020 – present
Senior Researcher New York, NY

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

Oasis Labs May 2018 – Aug 2018
Research Scientist Berkeley, CA

Security & Privacy Research, Intel Labs Jul 2017 – Aug 2017
Researcher Hillsboro, OR

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

Teaching Experience

- TA for CS5435: Security and Privacy in the Wild 2015, Fall
- TA for CS5300: the Architecture of Large-scale Information Systems 2015, Spring
- TA for CS4410: Operating Systems 2014 Fall

Invited Talks

CanDID: Can-Do Decentralized Identity

- 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 — Jan 2020

Connecting Blockchains to the Real World

- IC3 Webinar — August 2020
- Rutgers University — April 2020 (cancelled)
- Purdue University — March 2020 (cancelled)
- 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 — Feb 2020
- Penn State — Feb 2020
- University at Buffalo — Feb 2020
- CISPA—Helmholtz Center for Information Security, Saarbrücken, Germany — Nov 2019
- ETH Zürich — Oct 2019
- IBM PhD fellow talk at IBM Watson Research Center. — Sep 2019

CHURP: Proactive Secret Sharing with Dynamic Committee

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

On Trusted Hardware and Blockchain Hybridization

- Northeastern University, Cybersecurity Speaker Series — Jan 2019
- MIT, CSAIL — Nov 2018
- New York University, CS Colloquium — Oct 2018

Paralysis Proof

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

REM

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

Town Crier

- Silicon Valley Ethereum Meetup, Santa Clara, CA — Aug 2017
- IC3 Retreat, San Francisco, CA — Mar 2017
- CCS'16, Vienna, Austria — Oct 2016
- IC3 Retreat, New York City — May 2016

Professional Activity

- **Program Committee**: BITCOIN'18 (collocated with Financial Crypto 2018), Financial Crypto (FC) 2021.
- **Reviewer**: USENIX Security (2016), ACM Computing Surveys (2018), Nature Sustainability (2018), TCC (2019), FC (2019), CCS (2020), CRYPTO (2020). IEEE Transactions on Dependable and Secure Computing (2020), ACM Transactions on Privacy and Security (2020).

Software Artifacts

See my Github for an up-to-date list.

- DECO: A privacy-preserving oracle protocol for TLS. See http://deco.works.
- Town Crier: an Authenticated Data Feed For Smart Contracts. See http://www.town-crier.org.
- CHURP: Dynamic-Committee Proactive Secret Sharing. See http://www.churp.io.
- mbedtls-SGX: a SGX-friendly TLS stack (ported from mbedtls). At http://github.com/bl4ck5un/mbedtls-SGX

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 Saturday 17th October, 2020.