Ertem Nusret Tas

nusret@stanford.edu
(617) 909-7171

Education

09/2019— 06/2025 (expected) **Ph.D in Electrical Engineering**
Stanford University (SU)
GPA: 4.0/4
Advisors: David Tse and Dan Boneh

09/2018— 09/2019 **MEng in Electrical Engineering and Computer Science**
Massachusetts Institute of Technology (MIT)
Advisor: Eytan Modiano

09/2015— 06/2018 **B.S in Electrical Engineering and Computer Science**
Massachusetts Institute of Technology (MIT)
GPA: 5.0/5

09/2015— 06/2018 **Minor in Economics**
Massachusetts Institute of Technology (MIT)

Research

09/2019— present **Stanford University (SU)**
Security of Blockchain Systems [1, 3-19, 21, 22, 24, 25]
Supervised by Prof. David Tse and Dan Boneh

09/2018— 08/2019 **Massachusetts Institute of Technology (MIT)**
Coflow Scheduling in Cross-bar Switches [23]
Supervised by Prof. Eytan Modiano

09/2016— 05/2017 **Massachusetts Institute of Technology (MIT)**
Infrared Sensors based on Graphene Flake Films
Supervised by Prof. Tomas Palacios

Experience

06/2023— 08/2023 **a16z crypto research** New York, NY
Intern

06/2022— 09/2022 **BabylonChain** Stanford, CA
Intern

06/2021— 09/2021 **Celestia (Lazyledger)** Stanford, CA
Intern

06/2018— 08/2018 **Apple Inc.** Austin, TX
Intern at the Silicon Eng. Group Formal Verification Team

06/2017— **NetApp Inc.** Research Triangle Park, NC
08/2017 Intern

05/2016— **Linear Technology** North Chelmsford, MA
08/2016 Intern

Teaching

10/2022— **Lecturer**
10/2023 Stanford

- Gave three lectures on consensus protocols in Cryptocurrencies and Blockchain Technologies (CS 251) in Fall 2022 and 2023.

04/2023— **Teaching Assistant for Information Theory (EE 276)**
06/2023 Stanford

02/2018— **Teaching Assistant for Math for Computer Science (6.046J)**
05/2018 MIT

Publications

Preprints:

[1] J. Neu†, E. N. Tas†, and D. Tse†. "Snap-and-Chat Protocols: Systems Aspects". arXiv:2010.10447. Sept. 2020.

[2] E. N. Tas, J. Adler, M. Al-Bassam, I. Khoffi, D. Tse, and N. Vaziri. "Accountable Safety for Rollups". Presented at: *The Science of Blockchain Conference 2022 (SBC '22)* arXiv:2210.15017. Oct. 2022.

[3] E. N. Tas, R. Han, D. Tse, F. Yu, and K. Nazirkhanova. "Interchain Timestamping for Mesh Security". arXiv:2305.07830. May 2023. (Online version of [20])

[4] X. Dong‡, O. S. Thyfronitis Litos‡, E. N. Tas‡, D. Tse‡, R. L. Woll‡, L. Yang‡, and M. Yu‡. "Remote Staking with Economic Safety". arXiv:2408.01896. Aug. 2024.

[5] Y. Efron†, E. N. Tas†. "Dynamically Available Common Subset". ePrint:2025/016. Jan. 2025.

Conference Papers:

[6] R. Sarenche‡, E. N. Tas‡, B. Monnot, C. Schwarz-Schilling, and B. Preneel. "Breaking the Balance of Power: Commitment Attacks on Ethereum's Reward Mechanism". In: *2025 IEEE European Symposium on Security and Privacy (Euro S&P'25)*. arXiv: 2407.19479. July 2024.

[7] A. Dembo‡, S. Kannan‡, E. N. Tas‡, D. Tse‡, P. Viswanath‡, X. Wang‡, and O. Zeitouni‡. "Everything is a Race and Nakamoto Always Wins". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*. arXiv:2005.10484. Oct. 2020.

[8] J. Neu†, E. N. Tas†, and D. Tse†. "Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma". In: *Proceedings of the 2021 IEEE Symposium on Security and Privacy (IEEE S&P '21)*. arXiv:2009.04987. May. 2021.

‡ Listed alphabetically.
† Contributed equally and listed alphbetically.

[9] J. Neu[†], E. N. Tas[†], and D. Tse[†]. "The Availability-Accountability Dilemma and its Resolution via Accountability Gadgets". In: *Proceedings of 26th International Conference on Financial Cryptography and Data Security (FC'22)*. arXiv:2105.06075. May. 2021.

[10] C. Schwarz-Schilling, J. Neu, B. Monnot, A. Asgaonkar, E. N. Tas, and D. Tse. "Three Attacks on Proof-of-Stake Ethereum". In: *Proceedings of 26th International Conference on Financial Cryptography and Data Security (FC'22)*. arXiv:2110.10086. Oct. 2021.

[11] J. Neu[†] and E. N. Tas[†]. "Two Attacks On Proof-of-Stake GHOST/Ethereum". In: *2022 Workshop on Developments in Consensus*. arXiv:2203.01315. March 2022.

[12] E. N. Tas, D. Tse, F. Gai, S. Kannan, M.A. Maddah-Ali, and F. Yu. "Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities". In: *Proceedings of the 2023 IEEE Symposium on Security and Privacy (IEEE S&P '23)*. arXiv:2207.08392. Aug. 2022.

[13] E. N. Tas, and D. Boneh. "Cryptoeconomic Security for Data Availability Committees". In: *Proceedings of 27th International Conference on Financial Cryptography and Data Security (FC' 23)*. arXiv:2208.02999. Aug. 2022.

[14] E. N. Tas, R. Han, D. Tse, and F. Yu. "Interchain Timestamping for Mesh Security". In: *2023 ACM Conference on Computer and Communications Security (CCS '23)*. May 2023.

[15] S. Agrawal, J. Neu, E. N. Tas, and D. Zindros. "Proofs of Proof-of-Stake with Sublinear Complexity". In: *Advances in Financial Technologies 2023 (AFT '23)*. arXiv:2209.08673. Sept. 2022.

[16] E. N. Tas, and D. Boneh. "Vector Commitments with Efficient Updates". In: *Advances in Financial Technologies 2023 (AFT '23)*. arXiv:2307.04085. July 2023.

[17] E. N. Tas, D. Zindros, L. Yang, and D. Tse. "Light Clients for Lazy Blockchains". In: *28th International Conference on Financial Cryptography and Data Security (FC'24)*. arXiv:2203.15968. March 2022.

[18] F. D'Amato[‡], J. Neu[‡], E. N. Tas[‡], and D. Tse[‡]. "No More Attacks on Proof-of-Stake Ethereum?". In: *28th International Conference on Financial Cryptography and Data Security (FC'24)*. arXiv:2209.03255. Sept. 2022.

[19] J. Neu[‡], E. N. Tas[‡], and D. Tse. "Short Paper: Accountable Safety Implies Finality". "https://eprint.iacr.org/2023/1301". In: *28th International Conference on Financial Cryptography and Data Security (FC'24)*. ePrint:2023/1301. Sept. 2023.

[20] E. N. Tas, I. A. Seres, Y. Zhang, M. Melczer, M. Kelkar, J. Bonneau and V. Nikolaenko. 'Atomic and Fair Data Exchange via Blockchain". In: *2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*. ePrint:2024/418. March 2024. (**Distinguished paper award at CCS '24**)

[21] E. N. Tas[‡], D. Tse[‡], and Y. Wang[‡]. 'A Circuit Approach to Constructing Blockchains on Blockchains". In: *Advances in Financial Technologies 2024 (AFT '24)*. arXiv:2402.00220. Aug. 2024.

[22] S. Sridhar[†], E. N. Tas[†], J. Neu, D. Zindros and D. Tse. "Consensus Under Adversary Majority Done Right". "https://eprint.iacr.org/2024/1799". In: *29th International Conference on Financial Cryptography and Data Security (FC'25)*. ePrint:2023/1301. Nov. 2024.

MEng Thesis:

[23] E. N. Tas. "Coflow scheduling in data center networks". M. Eng. Thesis. Sept. 2019.

Blog Posts:

[24] J. Neu, E. N. Tas, and D. Tse. "Avalanche Attack on Proof-of-Stake GHOST". Ethereum Research. Jan. 2022

[25] J. Neu, E. N. Tas, and D. Tse. "Balancing Attack: LMD Edition". Ethereum Research. Jan. 2022

[26] E. N. Tas, and N. Vaziri. "Rollups on Celestia". Celestia Forum. Sep. 2021

[27] E. N. Tas, and N. Vaziri. "Spamming Attacks on Rollups". Celestia Forum. Sep. 2021

[28] E. N. Tas, and N. Vaziri. "Woods Attack on Celestia". Celestia Forum. Sep. 2021

[29] M. Al-Bassam, E. N. Tas, and N. Vaziri. "Rollups as Sovereign Chains". Celestia Blog. July 2022

[30] E. N. Tas, K. Nazirkhanova, and D. Tse. "Babylon: Bitcoin Security for Cosmos and beyond". Substack BabylonChain. Sept. 2022

[31] E. N. Tas. "Why is Stake Unbonding so Slow?". Substack BabylonChain. Sept. 2022

[32] E. N. Tas, and K. Nazirkhanova. "Babylon for Fast Stake Unbonding". Substack BabylonChain. Sept. 2022

Honors and Awards

- Silver medalist in 2014 International Physics Olympiad (IPhO).
- Ranked 1st among 2 million participants in the University Entrance Exam of Turkey.
- Landsman Undergraduate Research and Innovation Scholar at MIT SuperUROP (Undergraduate Research Opportunities Program), 2016-2017.
- Member of Mass Beta chapter of Tau Beta Pi (TBP).
- Member of Beta Theta chapter of Eta Kappa Nu. (HKN).
- Winner of the Niantic Augmented Reality Prize at 2018 HackMIT.
- Finalist for the 2022 Meta PhD Research Fellowship in Blockchain and Cryptoeconomics.

Leadership and Activities

08/2024—08/2024	**Science and Engineering of Consensus 2024** Workshop Organizer	New York, NY
06/2022—06/2024	**Information Systems Lab. (ISL) Colloquium** Colloquium Organizer	Stanford, CA

09/2016— *05/2017*	**Gordon MIT Leadership Program** Gordon Engineering Leader	Cambridge, MA
09/2016— *05/2017*	**MIT Turkish Student Association** President	Cambridge, MA
03/2018— *03/2019*	**MIT Tau Beta Pi (TBP)** Secretary and Community Service Chair	Cambridge, MA
05/2018— *05/2019*	**MIT Eta Kappa Nu (HKN)** Secretary	Cambridge, MA