

# Ertem Nusret Tas

---

## Education

<i>09/2019— 08/2024 (expected)</i>	<b>Ph.D in Electrical Engineering</b> Stanford University (SU) GPA: 4.0/4 Advisor: David Tse
<i>09/2018— 09/2019</i>	<b>MEng in Electrical Engineering and Computer Science</b> Massachusetts Institute of Technology (MIT) Advisor: Eytan Modiano
<i>09/2015— 06/2018</i>	<b>B.S in Electrical Engineering and Computer Science</b> Massachusetts Institute of Technology (MIT) GPA: 5.0/5
<i>09/2015— 06/2018</i>	<b>Minor in Economics</b> Massachusetts Institute of Technology (MIT)

## Research

<i>09/2019— present</i>	<b>Stanford University (SU)</b> Security of Blockchain Systems [1, 3-18, 20, 22, 23] Supervised by Prof. David Tse
<i>09/2018— 08/2019</i>	<b>Massachusetts Institute of Technology (MIT)</b> Coflow Scheduling in Cross-bar Switches [21] Supervised by Prof. Eytan Modiano
<i>09/2016— 05/2017</i>	<b>Massachusetts Institute of Technology (MIT)</b> Infrared Sensors based on Graphene Flake Films Supervised by Prof. Tomas Palacios

## Experience

<i>06/2023— 08/2023</i>	<b>a16z crypto</b> Intern	New York, NY
	• Summer intern at a16z crypto research [19].	
<i>06/2022— 09/2022</i>	<b>BabylonChain</b> Intern	Stanford, CA

- Worked on the design of BabylonChain’s architecture and wrote blog posts introducing its main features [28-30].

06/2021—  
09/2021

**Celestia (Lazyledger)**  
Intern

Stanford, CA

- Worked on fraud proof implementation in Go and formalizing rollups for scaling the throughput of blockchains [2, 24-27].

06/2018—  
08/2018

**Apple Inc.**  
Intern

Austin, TX

- Worked in the Silicon Eng. Group Formal Verification Team.

06/2017—  
08/2017

**NetApp Inc.**  
Intern

Research Triangle Park, NC

- Worked on the implementation of PCIe Non-Transparent Bridge (NTB) driver support in Intel’s Skylake processor.

05/2016—  
08/2016

**Linear Technology**  
Intern

North Chelmsford, MA

- Developed a USB-C powered power path manager.

**Teaching**  
10/2022—  
10/2023

**Lecturer**  
Stanford

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

04/2023—  
06/2023

**Teaching Assistant**  
Stanford

- Worked as a teaching assistant in the Information Theory (EE 276) course.

02/2018—  
05/2018

**Teaching Assistant**  
MIT

- Worked as an undergraduate teaching assistant in the Math for Computer Science (6.046J) course.

**Publications**  
**Preprints:**

- [1] J. Neu<sup>‡</sup>, E. N. Tas<sup>‡</sup>, and D. Tse<sup>‡</sup>. “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] R. Sarenche<sup>‡</sup>, E. N. Tas<sup>‡</sup>, B. Monnot, C. Schwarz-Schilling, and B. Preneel. “Breaking the Balance of Power: Commitment Attacks on Ethereum’s Reward Mechanism”. arXiv:2407.19479. July 2024.
- [5] X. Dong<sup>‡</sup>, O. S. Thyfronitis Litos<sup>‡</sup>, E. N. Tas<sup>‡</sup>, D. Tse<sup>‡</sup>, R. L. Woll<sup>‡</sup>, L. Yang<sup>‡</sup>, and M. Yu<sup>‡</sup>. “Remote Staking with Economic Safety”. arXiv:2408.01896. Aug. 2024.

### Conference Papers:

- [6] A. Dembo<sup>‡</sup>, S. Kannan<sup>‡</sup>, E. N. Tas<sup>‡</sup>, D. Tse<sup>‡</sup>, P. Viswanath<sup>‡</sup>, X. Wang<sup>‡</sup>, and O. Zeitouni<sup>‡</sup>. “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.
- [7] J. Neu<sup>‡</sup>, E. N. Tas<sup>‡</sup>, and D. Tse<sup>‡</sup>. “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.
- [8] J. Neu<sup>‡</sup>, E. N. Tas<sup>‡</sup>, and D. Tse<sup>‡</sup>. “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.
- [9] 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.
- [10] J. Neu<sup>‡</sup> and E. N. Tas<sup>‡</sup>. “Two Attacks On Proof-of-Stake GHOST/Ethereum”. In: *2022 Workshop on Developments in Consensus*. arXiv:2203.01315. March 2022.
- [11] 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.
- [12] 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.
- [13] 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.

---

<sup>‡</sup> Listed alphabetically.

<sup>†</sup> Contributed equally and listed alphabetically.

- [14] 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.
- [15] E. N. Tas, and D. Boneh. “Vector Commitments with Efficient Updates”. In: *Advances in Financial Technologies 2023 (AFT ’23)*. arXiv:2307.04085. July 2023.
- [16] 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.
- [17] F. D’Amato<sup>‡</sup>, J. Neu<sup>‡</sup>, E. N. Tas<sup>‡</sup>, and D. Tse<sup>‡</sup>. “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.
- [18] J. Neu<sup>‡</sup>, E. N. Tas<sup>‡</sup>, 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.
- [19] 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 ’20)*. ePrint:2024/418. March 2024.
- [20] E. N. Tas<sup>‡</sup>, D. Tse<sup>‡</sup>, and Y. Wang<sup>‡</sup>. ‘A Circuit Approach to Constructing Blockchains on Blockchains”. In: *Advances in Financial Technologies 2024 (AFT ’24)*. arXiv:2402.00220. Aug. 2024.

#### **MEng Thesis:**

- [21] E. N. Tas. “Coflow scheduling in data center networks”. M. Eng. Thesis. Sept. 2019.

#### **Blog Posts:**

- [22] J. Neu, E. N. Tas, and D. Tse. “Avalanche Attack on Proof-of-Stake GHOST”. Ethereum Research. Jan. 2022
- [23] J. Neu, E. N. Tas, and D. Tse. “Balancing Attack: LMD Edition”. Ethereum Research. Jan. 2022
- [24] E. N. Tas, and N. Vaziri. “Rollups on Celestia”. Celestia Forum. Sep. 2021
- [25] E. N. Tas, and N. Vaziri. “Spamming Attacks on Rollups”. Celestia Forum. Sep. 2021
- [26] E. N. Tas, and N. Vaziri. “Woods Attack on Celestia”. Celestia Forum. Sep. 2021
- [27] M. Al-Bassam, E. N. Tas, and N. Vaziri. “Rollups as Sovereign Chains”. Celestia Blog. July 2022
- [28] E. N. Tas, K. Nazirkhanova, and D. Tse. “Babylon: Bitcoin Security for Cosmos and beyond”. Substack BabylonChain. Sept. 2022
- [29] E. N. Tas. “Why is Stake Unbonding so Slow?”. Substack BabylonChain. Sept. 2022
- [30] 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**      New York, NY  
Workshop Organizer

*06/2022—  
06/2024*      **Information Systems Lab. (ISL) Colloquium**      Stanford, CA  
Colloquium Organizer

*09/2016—  
05/2017*      **Gordon MIT Leadership Program**      Cambridge, MA  
Gordon Engineering Leader

*09/2016—  
05/2017*      **MIT Turkish Student Association**      Cambridge, MA  
President

*03/2018—  
03/2019*      **MIT Tau Beta Pi (TBP)**      Cambridge, MA  
Secretary and Community Service Chair

*05/2018—  
05/2019*      **MIT Eta Kappa Nu (HKN)**      Cambridge, MA  
Secretary