Sarisht Wadhwa

sarisht.wadhwa@duke.edu · sarisht.github.io/ · +1(984)377-1996 · sarisht-wadhwa

Summary

My research develops secure and incentive-compatible mechanisms for decentralized systems, with a particular focus on censorship resistance, transaction ordering, and fair transaction fee mechanism design on blockchains. I study how cryptographic tools and algorithmic game theory can be combined to address real-world challenges in decentralized finance and distributed protocol design. I have had the privelege to work with wonderful collaborators from Ethereum Research, Flashbots, Category Labs and Common Prefix.

Education

Ph.D. *Major: Computer Science*
Thesis: *Security of Blockchains with Rational Entities* Aug 2021 - May 2026
Duke University, North Carolina

Dual B.Tech./M.Tech. *Major: Computer Science* July 2014 - June 2019
Indian Institute of Technology (IIT), Delhi

Publications

$*$ represents equal contribution, $\alpha\beta$ represents alphabetical order

1. **Wadhwa, S.***, Yaish, A.*, Zhang, F., Nayak, K. (2026). *Perils of Parallelism: Transaction Fee Mechanism with Uncertain Execution.* e-print online, To appear in the proceedings of the 35th USENIX Security Symposium, 2026

2. Elsheimy, F.*, Kaklamanis, I.*, **Wadhwa, S.***, Papamanthou, C., Zhang, F. (2026). *Censorship Resistance vs Throughput in Multi-Proposer BFT Protocols.* e-print online, To appear in proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS).

3. $^{\alpha\beta}$Alpos, O., Heimbach, L., Nayak, K., **Wadhwa, S.** (2025). *Censorship-Resistant Sealed-Bid Auctions on Blockchains.* e-print online.

4. Passerat-Palmbach, J. and **Wadhwa, S.** (2025). *Differentially Private aggregate hints in mev-share.* arXiv preprint online.

5. **Wadhwa, S.**, Ma, J., Thiery, T., Mannot, B., Zanolini L., Zhang, F., and Nayak, K. (2024). *AUCIL: An inclusion list design for rational parties.* e-print online.

6. **Wadhwa, S.**, Zanolini, L., D'Amato F., Asgaonkar, A., Fang, C., Zhang, F., and Nayak, K. (2023). *Data Independent Order Policy Enforcement: Limitations and Solutions.* In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS).

7. **Wadhwa, S.***, Stöter, J.*, Zhang, F., Nayak, K. (2022). *He-HTLC: Revisiting Incentives in HTLC.* In proceedings of the 2023 Network and Distributed Systems Symposium (NDSS).

8. **Wadhwa, S.**, Prasad, A., Ranu, S., Bagchi, A., Bedathur, S. *Efficiently answering regular simple path queries on large labeled networks.* In Proceedings of the 2019 International Conference on Management of Data (SIGMOD).

Grants and Awards

- **IC3 Summer Camp 2025:** Won the first prize among eight projects. Project: Proposed an elastic restaking design that achieves application dependent security and computed how stake should be divided amongst all such applications.
- **Ethereum Research Grant 2024:** Received a grant to work on improving censorship resistance of Ethereum.
- **Samsung Research Excellence 2021:** Won Samsung's research excellence award in 2021 for research in camera systems.
- **Microsoft Travel Scholarship 2019:** Funded by Microsoft Research to attend the 2019 ACM SIGMOD Conference in Amsterdam, Netherlands.

Service

- **Program Committee:**
  - ACM CCS 2026
  - ACM EC 2026
  - CAAW 2026 (Co located with FC 2026)
  - Agentic Markets Workshop at ICML 2024
  - DEFI Workshop 2024 (Co-located with ACM CCS 2024)

- **External Reviewer:**
  - IEEE SP 2024, 2025, 2026
  - FC 2025, 2026
  - AFT 2022, 2026

Talks

- *Perils of Parallelism*
  - IC3 Summer Camp (June 2026)
  - Designing DeFi (D^2) (May 2026)
  - Yale Applied Cryptography Lab (April 2026)
  - Columbia Crypto-economics Workshop (CCE) (December 2025)
- *AUCIL: An Inclusion List Design for Rational Parties*
  - Yale Applied Cryptography Lab (October 2025)
  - MEV Workshop at Science of Blockchain Conference (July 2025)
- *Data Independent Order Policy Enforcement*
  - University of Michigan Visit (April 2026)
  - ACM Conference on Computer and Communications Security (CCS) (October 2024)
  - DeFi Workshop at ACM Conference on Economics and Computation (July 2024)
  - Yale Security Group (July 2024)
  - Duke Patent Office Visit Day (June 2024)
- *He-HTLC: Revisiting Incentives in HTLC*
  - Network and Distributed System Security Symposium (February 2023)
  - Science of Blockchain Conference (SBC) (August 2022)
  - Crypto Economics Security Conference (October 2022)

Blog Posts

- *Block Building is Not Just Knapsack* (*Eth Research*).
- *AUCIL: An Auction-Based Inclusion List Design for Enhanced Censorship Resistance on Ethereum* (*Eth Research*).