Daniel Joseph Aronoff

Massachusetts Institute of Technology
Research Affiliate, Department of Economics

Curriculum Vitae, Academics
Updated: January 2, 2026
daronoff@mit.edu |

Academic Appointments

2024– **Research Affiliate**, Department of Economics, MIT.

2022– Research Associate, The Laboratory for Economic Analysis and Design at MIT.

2022–2024 Research Scientist, MIT Media Lab.

2020– Collaborator, Digital Currency Initiative, MIT Media Lab.

Education

2022

Massachusets Institute of Technology
Ph.D in Economics
Advisors: Glenn Ellison, Robert Townsend and Nikhil Agarwal.

London School of Economics and Political Science
B.Sc in Philosophy and Economics (First Class Honors)
Tutors: Peter Urbach (Philosophy) and John Sutton (Economics).

University of Michigan
Attended
Studied Russian Intellectual History
Advisor: Arthur Mendel.

Research Interests

Financial market structure; digital currencies; cryptography; environmental market design.

Publications

Journal Articles

Books and Chapters

Aronoff, D. and I. Ardis (2024). ADESS: A Proof-of-Work Protocol to Deter Double-Spend Attacks. *Advances in Information and Communication*. Ed. by K. Arai. Vol. 920. Lecture Notes in Networks and Systems. FICC 2024 Berlin. Cham: Springer, pp. 131–157. Link PDF.

Aronoff, D. (2016a). *A Theory of Accumulation and Secular Stagnation*. New York, NY: Palgrave Pivot. Link.

— (2016b). *The Financial Crisis Reconsidered: The Mercantilist Origin of Secular Stagnation and Boom-Bust Cycles*. New York, NY: Palgrave Macmillan New York. Link.

Conference Proceedings

Aronoff, D., A. Bhat, P. Chatzigiannis, M. Minaei, S. Raghuraman, R. M. Townsend, and N. X.-Y. Zhang (2025b). SoK: Fully-homomorphic encryption in smart contracts. Conference Poster. FHE.org2025 Sophia, Bulgaria. Link.

Aronoff, D. (2024a). ADESS: A Proof-of-Work Protocol to Deter Double-Spend Attacks. Conference slides. FICC2024 Berlin. Link.

Working Papers / Preprints

Aronoff, D. (2025a). Mechanism Design for Hashrate Externalities:
Implementing Optimal Security in Proof-of-Work. unpublished manuscript MIT. Link.

Aronoff, D. (2025b). NetWrap: Technology to Preserve Counterparty Risk in Multilateral Netting. unpublished manuscript. .

Aronoff, D., A. Bhat, P. Chatzigiannis, M. Minaei, S. Raghuraman, R. M. Townsend, and N. X.-Y. Zhang (2025a). SoK: Fully-homomorphic encryption in smart contracts. Cryptology ePrint Archive, Paper 2025/527. Link.

Aronoff, D. and R. M. Townsend (2025). A Smart-Contract to Resolve Multiple Equilibrium in an Intermediated Repo Trade. arXiv preprint. Link.

Aronoff, D., R. M. Townsend, and M. Virza (2025). TradeMech: Multilateral Netting Without Altering Counterparty Risk. unpublished manuscript, MIT. .

Aronoff, D. J., R. M. Townsend, and M. Virza (2025). *RepoMech: A Method to Reduce the Balance-Sheet Impact of Repo Intermediation*. Link.

Aronoff, D. (2024d). Targeted Nakamoto: A Bitcoin Protocol to Balance Network Security and Carbon Emissions. arXiv preprint, version 4. Link.

Aronoff, D. and W. Rafey (2023). Conservation Priorities and Environmental Offsets: Markets for Florida Wetlands. NBER Working Paper. Link.

Moroz, D. J., D. J. Aronoff, N. Narula, and D. C. Parkes (2020). Double-Spend Counterattacks: Threat of Retaliation in Proof-of-Work Systems. arXiv preprint. Link.

Thesis

Aronoff, D. (2022). "Essays on Incentive Designs to Improve Market Performance". PhD thesis; available from MIT DSpace. PhD thesis. Cambridge, MA, USA: Massachusetts Institute of Technology. Link.

Recorded Talks and Video Presentations

Daniel Aronoff and Madars Virza (Oct. 2025). *AI-Driven, Post-Quantum Data Privacy Research Spotlight*. Presentation at MIT-ILP conference Securing the Future: AI-Driven Post-Quantum Data Privacy. Link.

Aronoff, D. (June 2024b). *Incorporating Cryptographic Methods in Economics*. Presentation MIT-ILP NextGen Security Conference. Link.

Aronoff, D., J. Flynn, and E. Golding (Nov. 2023). *R&D Fintech Innovation*. Panel Discussion at 2023 MIT Research and Development Conference. Link.

Aronoff, D. (Sept. 2021b). *Rethinking Currency with Daniel Aronoff*. Invited Lecture: Rethinking Economics NL. Link.

Slide Presentations

Aronoff, D. (Oct. 2024c). SCBX Cryptography Use Cases: Credit Score Avereging with Differential Privacy and FHE. Presentation to SCB^x R&D Department. Link.

— (2021a). A Causal Infrence Algorithm for Heterogeneous Treatment Efects. Presentation to MIT Econometrics Lunch. Link.

Blog Posts

Aronoff, D., A. Brownworth, J. Jin, A. Samuel, and N. Narula (July 2025). *Stablecoins and the Limits of Existing Analogies*. MIT Media Lab Digital Currency Initiative. Link.

Aronoff, D., A. Brownworth, A. Samuel, and N. Narula (July 2025). *The GENIUS Act is Now Law. What's Missing?* MIT Media Lab Digital Currency Initiative. Link.

Aronoff, D., A. Samuel, and N. Narula (July 2025a). *1:1 Redemptions for Some, Not All*. MIT Media Lab Digital Currency Initiative. Link.

— (July 2025b). *Will Stablecoins Impact the US Treasury Market?* MIT Media Lab Digital Currency Initiative. Link.

Project Sites

Aronoff, D. (July 2025c). *Targeted Nakamoto: Project site*. MIT Media Lab Digital Currency Initiative. Link.

Aronoff, D. and I. Ardis (July 2025). *ADESS: Project site*. MIT Media Lab Digital Currency Initiative. Link.

Professional Service

Committees 2022: **Advances in Financial Technologies (AFT2022)**
Program Committee

Refereeing 2020 - 2023: *Cryptoeconomic Systems*.

Academic Boards 2003 - 2008: **Grand Valley State University** Grand Rapids, MI.
Board of Trustees.
2006 – 2008: Vice-Chair.
2007 - 2010: **Roeper School** Bloomfield Hills, MI.
Board of Trustees

Consulting

2024– Client: SCB^X. Project: An AI-Driven Post-Quantum Cryptographically Secure Workflow for Collaborative Credit Scoring.

References

Available upon request.