# Neha Narula

20 Ames St E15-351
Cambridge, MA 02142

narula@mit.edu
http://nehanarula.org


**Interests** Distributed systems, security, cryptocurrencies, and digital money

**Education**

**Massachusetts Institute of Technology** — Cambridge, MA
Ph.D. in Computer Science — June 2015
Advisors: Robert T. Morris and Eddie Kohler
Thesis: *Parallel Execution for Conflicting Transactions*

**Massachusetts Institute of Technology** — Cambridge, MA
S.M. in Computer Science — September 2010
Advisor: Robert T. Morris.
Thesis: *Distributed Query Execution on a Replicated and Partitioned Database*

**Dartmouth College** — Hanover, NH
A.B. in Computer Science and A.B. in Mathematics — June 2003
Advisor: Prasad Jayanti
Thesis: *Eliminating Complex Synchronization Instructions in the Contention-Free Case for Mutual Exclusion Algorithms*

**Research Experience**

**MIT Media Lab** — Cambridge, MA
*Director, Digital Currency Initiative* — May 2016 – present

Director of the Digital Currency Initiative at the MIT Media Lab. Leading a team of 10 including research scientists, Bitcoin Core developers, and other staff. Activities include research, writing software, teaching classes, advising undergraduates and masters students, and fundraising.

**Stablecoins.** We research and investigate financial and technology risks and opportunities for stablecoins.

**Central bank digital currency.** We do technology research to understand how to safely design central bank digital currency and solve challenges including scalability, enabling offline access, and preserving privacy. We engaged in sponsored research collaborations with the Bill and Melinda Gates Foundation, Federal Reserve Bank of Boston, Bundesbank, Bank of Canada, Bank of England, World Bank, and Bank for International Settlements.

**Economic security of proof-of-work**. Trillions of dollars rest on the security of proof-of-work to prevent double spending in cryptocurrency. Our work expands the space of strategies to secure proof-of-work and implements monitoring tools to detect illicit miner activity.

**Cryptocurrency security**. We found a vulnerability in the Curl-P hash function used in the cryptocurrency IOTA. I wrote the code to efficiently find collisions and generate conflicting attack transactions. Based on this and another vulnerability a DCI developer found in Bitcoin Cash, we established a cryptocurrency security initiative to explore the question of whether decentralized networks can be secure at scale and disseminate best practices on cryptocurrency security and vulnerability disclosure.

**zkLedger**. zkLedger is a distributed ledger which provides transaction privacy and provably-correct, third-party auditing. zkLedger hides the participants and amounts in transactions, but

the transactions can still be publicly verified to show that financial invariants are maintained. By using non-interactive zero-knowledge proofs, zkLedger allows a third party to query the participants to analyze the contents of the ledger, without revealing individual transactions. We designed, implemented, evaluated, and released zkLedger as an open source project.

**Supervised work**. Other work at the DCI includes Utreexo, a design for shrinking Bitcoin's 4 GB (and growing) unspent coins database to less than a kilobyte, and developing and maintaining Bitcoin Core, the primary software used in the Bitcoin network.

**MIT CSAIL** Cambridge, MA
*Research Assistant in Parallel and Distributed Operating Systems* January 2008 – May 2015

**Doppel**. I created Doppel, an in-memory multi-core transactional database designed to improve performance on workloads with many conflicting transactions. We developed a new technique called phase reconciliation; we take advantage of commutativity and executing transactions in explicit phases in order to increase concurrency. Doppel provides a dramatic performance improvement over existing concurrency control algorithms (3-30×) on highly conflicting workloads.

**Dixie**. I wrote Dixie, a SQL query planner, optimizer, and executor which issues SQL queries written for one database over a database sharded and replicated over multiple servers. Dixie focuses on increasing inter-query parallel speedup and throughput by using table replicas to involve fewer servers in each query, and simplifies the process of moving an application from a single database to a sharded database.

## Industry Experience

**Block**
*Member, Board of Directors* July 2023 – present

Also serve on the Audit and Risk Committee and the Nominating and Corporate Governance Committee.

**Federal Reserve Bank of New York**
*Member, Innovation Advisory Council* March 2022 – present

**Paypal**
*Member, Blockchain and Digital Currencies Advisory Council* February 2022 – April 2023

**Google, Inc.** Mountain View, CA
*Senior Software Engineer* July 2003 – January 2011

Designed and developed a Linux security sandbox for untrusted code running in the Native Client framework. Helped launch the research prototype of Native Client.

Designed and developed a highly available, distributed storage and serving system for large binary objects with five other engineers. Launched and maintained the system while supporting several production applications and serving gigabits of traffic per second.

Launched Froogle, Google's shopping website, into Germany and France.

## Publications

Lovejoy, J., Virza, M., Fields, C., Karwaski, K., Brownworth, A. and **Narula, N.** *Hamilton: A High Performance Transaction Processor for Central Bank Digital Currencies*. In Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI). Boston, MA, 2023.

Su, L., Liu, Q.C. and **Narula, N.** *The Power of Random Symmetry-Breaking in Nakamoto Consensus*. In Proceedings of the 35th International Symposium on Distributed Computing, 2021.

Park, S., Specter, M., **Narula, N.** and Rivest, R.L. *Going from bad to worse: from internet voting to blockchain voting*. In Journal of Cybersecurity, 2021.

Heilman, E., **Narula, N.**, Tanzer, G., Lovejoy, J., Colavita, M., Virza, M. and Dryja, T. *Cryptanalysis of curl-p and other attacks on the IOTA cryptocurrency*. In IACR Transactions on Symmetric Cryptology, 2020. Invited to present at Blackhat and Real World Crypto.

Böehme, R., Eckey, L., Moore, T., **Narula, N.**, Ruffing, T. and A. Zohar. *Responsible Vulnerability Disclosure in Cryptocurrencies*. In Communications of the ACM. 2020.

**Narula, N.**, Vasquez, W. and M. Virza. *zkLedger: Privacy-Preserving Auditing for Distributed Ledgers*. In Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI). Renton, WA, 2018.

**Narula, N.**, Cutler, C., Kohler, E. and R. Morris. *Phase Reconciliation for Contended In-memory Transactions*. In Proceedings of the 11th USENIX Symposium on Operating Systems Design and Implementation (OSDI). Broomfield, Colorado, 2014.

Kate, B., Kohler, E., Kester, M., **Narula, N.**, Mao, Y. and R. Morris. *Easy Freshness with Pequod Cache Joins*. In Proceedings of the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI). Seattle, Washington, 2014.

**Narula, N.** and R. Morris. *Executing Web Application Queries on a Partitioned Database*. In Proceedings of the USENIX Conference on Web Application Development (USENIX WebApps). Boston, Massachusetts, 2012.

Chandra, R., Kim, T., Shah, M., **Narula, N.** and N. Zeldovich. *Intrusion Recovery for Database-backed Web Applications*. In Proceedings of the ACM Symposium on Operating Systems Principles (SOSP). Cascais, Portugal, 2011.

Yee, B., Sehr, D., Dardyk, G., Chen, J.B., Muth, R., Ormandy, T., Oksaka, S., **Narula, N.** and N. Fullagar. *Native Client: A Sandbox for Portable, Untrusted x86 Native Code*. In the IEEE Symposium on Security and Privacy (Oakland). Oakland, California, 2010. **Best Paper Award, Test of Time Award**

Yip, A., **Narula, N.**, Krohn, M. and R.T. Morris. *Privacy-Preserving Browser-Side Scripting with BFlow*. In Proceedings of the ACM European Conference on Computer Systems (EuroSys). Nuremberg, Germany, 2009.

Jayanti, P., Petrovic, S. and **N. Narula**. *Read/Write Based Fast-Path Transformation for FCFS Mutual Exclusion*. International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM). Berlin, 2005.

## Invited Publications

Hensarling, J., Gramm, P., Taylor, J.B., Adrian, T., Mancini-Griffoli, T., Narula, N., White, L.H., Prasad, E.S., Carlson, J., Gladstein, A. and M. Chorzempa. *Digital Currencies: Risk or Promise?*. Cato Journal, 2021.

Casey, M., Crane, J., Gensler, G., Johnson, S. and **N. Narula**. *The Impact of Blockchain Technology on Finance: A Catalyst for Change*. ICMB, International Center for Monetary and Banking Studies, 2018.

## Posts, Abstracts, and Reports

Toh, W. K., Maurer, M., Landriault, E., Samuel, A., Wang, L. and **N. Narula**. *Designing Payment Tokens For Safety, Integrity, Interoperability, and Usability*. May 2025.

Lovejoy, J., Brownworth, A., Virza, M. and **N. Narula**. *PARSEC: Executing Smart Contracts in Parallel*. October 2023.

George, N., Dryja, T. and **N. Narula**. *A Framework for Programmability in Digital Currency*. August 1, 2023.

**Narula, N.**, Swartz, L. and Frizzo-Barker, J. *CBDC: Expanding Financial Inclusion or Deepening the Divide? Exploring Design Choices that Could Make a Difference*. January 12, 2023.

Auer, R., Frost, J., Lee, M., Martin, A., and **N. Narula**. *Why Central Bank Digital Currencies?* NY Fed Liberty Street Economics blog, December 1, 2021.

Liu, Q., Dryja, T. and **N. Narula**. *A Lower Bound for Byzantine Agreement and Consensus with Adaptive Adversaries using VDFs*.

Cline, D., Dryja, T. and **N. Narula**. *Clockwork: An Exchange Protocol for Proofs of Non Front-Running*.

Moroz, D., Aronoff, D., Lovejoy, J., **Narula, N.** and D. Parkes. *Double-Spend Counter-Attacks: Threat of Retaliation in Proof-of-Work Systems*.

**Narula, N.** and C. Fields. *Reducing the Risk of Catastrophic Cryptocurrency Bugs*. Medium post, August 9, 2018.

Aspegren, H., Glasbergen, G., Weber, M. and **N. Narula**. *b_verify: Scalable Non-Equivocation for Managing Public Data*.

Barabas, C., **Narula, N.** and E. Zuckerman. *Back to the Future: The Decentralized Web*. Report, 2017.

**N. Narula**. *A Multi-core Database is not a Distributed System*. In the Conference on Innovative Data Systems Research (CIDR). Asilomar, California, 2015.

**Narula, N.** and R. Morris. *Designing a Toolkit for Distributed Storage in Web Applications*. Poster at the Symposium on Operating Systems Principles (SOSP). Big Sky, Montana, 2009.

## Service

| | |
|---|---|
| Program Committee, Financial Cryptography | 2025 |
| Program Committee, Advances in Fintech Technology | 2024 |
| Program Committee, NSDI | 2023 |
| Invited academic expert, World Economic Forum Annual Meeting | 2023 |
| Co-chair, ACM Advances in Fintech Technology | 2022 |
| Program Committee, OSDI | 2022 |
| Program Committee, Financial Cryptography | 2021 |
| Program Committee, ACM Advances in Fintech Technology | 2021 |
| Program Committee, Financial Cryptography | 2020 |
| Invited academic expert, World Economic Forum Annual Meeting | 2020 |
| Program Committee, IEEE Security and Privacy | 2020 |
| Program Committee, Stanford Blockchain Conference | 2020 |
| Program Committee, ACM Symposium on Cloud Computing | 2019 |
| Program Committee, EuroSys | 2019 |
| External Reviewer, PODC | 2019 |

| | | |
|---|---|---|
| | Member, World Economic Forum's Global Blockchain Council | 2019-2020 |
| | Co-editor-in-chief and cofounder, Journal of Cryptoeconomic Systems (MIT Press) | 2019 |
| | Program Committee, Scaling Bitcoin | 2016 |
| | Program Chair, Scaling Bitcoin | 2015 |
| | Resident at Hacker School (now the Recurse Center) | 2015 |
| | MIT EECS Faculty Search Student Subcommittee | 2015 |
| | Leading MIT's distributed systems reading group | 2014-2015 |
| | Google Mentoring Committee | 2006-2008 |
| | Google Foundation Steering Committee | 2003 |

| | | |
|---|---|---|
| Students Advised | Ayesha Ali, MEng CS, MIT (Instabase) | 2023-2024 |
| | Claire Bao, MEng CS, MIT (Jump Trading) | 2023-2024 |
| | Shwetark Patel, MEng CS, MIT (startup) | 2021-2022 |
| | James Lovejoy, MEng CS, MIT (Director of Engineering at the Boston Fed) | 2019-2020 |
| | Henry Aspegren, MEng CS, MIT (PM Google, Meta, OpenAI) | 2017-2018 |
| | Willy R. Vasquez, MEng CS, MIT (PhD UT Austin, Apple) | 2016-2017 |

| | | |
|---|---|---|
| Teaching | **Cryptocurrency Design and Engineering (MIT MAS.S62)** | Fall 2025 |
| | **MIT/GetSmarter online cryptocurrency course** | |
| | Co-lead with Gary Gensler | Fall 2019 |
| | **Blockchain Lab (MIT 15.S68, 15.217)** | |
| | Co-lecturer with Michael Casey, Gary Gensler, and Simon Johnson | Spring 2019, 2020 |
| | Co-lecturer with Simon Johnson, Gary Gensler, and Luis Barros | Spring 2021 |
| | **Cryptocurrency Engineering and Design (MIT MAS.S62)** | |
| | Co-lecturer with Tadge Dryja. Available on MIT Open Courseware. | Spring 2018 |
| | **Shared Public Ledgers: Cryptocurrencies, Blockchains, and Other Marvels (MIT 6.892)** | |
| | Co-lecturer with Silvio Micali | Spring 2017 |
| | **Distributed Systems (MIT 6.824)** | |
| | Teaching Assistant | Spring 2013 |
| | Guest lecturer | |
| | **Computer Systems Engineering (MIT 6.033)** | |
| | Teaching Assistant | Spring 2011 |

Select Media

TED.com. *The future of money* (3M+ views)
MIT Technology Review. *The MIT researcher who helps senators understand digital currencies*
CBS 60 minutes. *Bitcoin's Wild Ride*
Wall Street Journal. *Does the U.S. Need a National Digital Currency?*
The New Yorker Live. *How Memes Become Money*
Amanpour & Co. *Currency Futurist Neha Narula Debunks Cryptocurrency*
Wired.com. *The Blockchain: Boon for Bankers or Tool for Tyrants?*
Techcrunch.com. *Cryptocurrency Insecurity: IOTA, BCash and Too Many More*
Motherboard.com. *A $5 Billion Cryptocurrency Has Enraged Cryptographers*
CNBC. *Digital Currency Could Change How We Deal with Money*
PBS Newshour. *The How and Why of Buying Bitcoin*
Wired.com. *Decentralized Social Networks Sound Great. Too Bad They'll Never Work*
Harvard Business Review. *The Blockchain Will Do to the Financial System What the Internet*

*Did to Media*
Wired.com. *MIT Computer Scientists Demonstrate the Hard Way That Gender Still Matters*
Reddit.com. *We're 3 Female Computer Scientists from MIT. Ask us anything!*

## Honors and Awards

| | |
|---|---|
| Rockefeller Foundation Bellagio Center Residency | 2025 |
| IEEE Symposium on Security and Privacy Test of Time Award | 2021 |
| IMSA Alumni Trailblazer Award | 2021 |
| WIRED 25 Leaders Shaping the Next 25 Years of Technology | 2019 |
| Academy of Achievement Delegate | 2019 |
| Thinkers50 Radar list | 2018 |
| Fortune's The Ledger 40 under 40 list | 2018 |
| IEEE Symposium on Security and Privacy Best Paper Award | 2010 |
| Eben Tisdale Fellowship (declined) | 2009 |
| NSF Graduate Research Fellowship | 2007 |
| High Honors in Computer Science | 2003 |

## Select Invited Talks

**System requirements and design choices for private, scalable digital cash**
Bank for International Settlements, Basel, Switzerland. August 2025
Advances in Fintech (keynote), Vienna, Austria. September 2024

**Can Bitcoin Self-Custody Scale to a Billion Users?**
BITCOIN 2025, Las Vegas, NV. May 2025
MIT Bitcoin Expo, Cambridge, MA. April 2025
Plan B Forum, El Salvador. January 2025

**Economic Security of Proof-of-Work**
MIT Bitcoin Expo, Cambridge, MA. April 2024
Chaincode, New York, NY. July 2019

**Central Bank Digital Currency: Risks and Opportunities**
Hoover Institute, Stanford July 2021

**Digitizing the Dollar**
US congressional testimony before the House Task Force on Financial Technology June 2021

**Building A Stronger Financial System: Opportunities of a Central Bank Digital Currency**
US congressional testimony before the Senate Economic Policy Subcommittee June 2021

**Redesigning Digital Money: What Can We Learn from a Decade of Cryptocurrencies?**
Bank of Canada, Ottawa, Canada. October 2019

**The Architecture of Crypto Innovation**
a16z Crypto Regulatory Summit May 2019

**Preventing Catastrophic Cryptocurrency Attacks**
MIT Bitcoin Expo, Cambridge, MA. March 2019
Financial Cryptography (keynote), St. Kitts. February 2019

**A Tangled Curl: How We Forged Signatures in IOTA**
Real World Crypto, San Jose, CA. January 2019
Blackhat, Las Vegas, NV. August 2018

**zkLedger: Privacy-Preserving Auditing for Distributed Ledgers**

| | |
|---|---|
| NBER Cryptocurrencies Workshop, Cambridge, MA. | May 2019 |
| Fintech@CSAIL Annual Meeting, Cambridge, MA. | September 2018 |
| PODC Blockchain Workshop, Egham, UK. | July 2018 |
| Microsoft Research, Redmond, WA. | April 2018 |
| NSDI, Renton, WA. | April 2018 |
| MIT Bitcoin Expo, Cambridge, MA. | March 2018 |
| Technion Summer School on Cyber and Security, Haifa, Israel. | September 2017 |

**21st Century Alchemy: Creating the Internet of Value**

| | |
|---|---|
| Depository Trust and Clearing Corporation, New York, NY | April 2019 |
| Goldman Sachs, New York, NY | May 2018 |

**The Future of Money**

| | |
|---|---|
| SXSW, Austin, TX. | March 2018 |
| EmTech China, Beijing, China. | January 2018 |
| Banco Central de Chile, Santiago, Chile. | December 2017 |
| TED@BCG, Paris, France (**3M views**). | May 2016 |