

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

Director of the Digital Currency Initiative at the MIT Media Lab. Leading a team of 13 including research scientists, Bitcoin Core developers, and other staff. Activities include research, writing software, teaching classes, advising undergraduates and masters students, and fundraising (2020 FY budget of \$2.9M).

Central bank digital currency. We engage in technology research to understand how to safely design central bank digital currency and solve challenges including enabling offline access and preserving privacy. In addition to this work, we are engaged in a sponsored research collaboration with the Federal Reserve Bank of Boston to design, implement, and test a hypothetical digital currency.

Economic security of proof-of-work. Billions of dollars rest on the security of proof-of-work to prevent double spending in cryptocurrency. Though it is thought that proof-of-work is unsecure without very high miner rewards, we show that due to possible strategies like counter-attacking and soft-forking, proof-of-work is cheaper to economically secure than was previously believed. We also implement monitoring tools to detect illicit miner activity. Understanding the true security we achieve using proof-of-work is critical to creating and fairly comparing to alternative protocols. This led us to design a new, less energy-intensive consensus protocol with provable guarantees about adversarial models inspired by proof-of-work-based protocols.

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

Research Assistant in Parallel and Distributed Operating Systems

Cambridge, MA

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.

BFlow. BFlow is a browser extension and server-side component which tracks confidential data as it flows within the browser. BFlow allows users to run untrusted JavaScript which can compute with, render, and store confidential data without being able to leak it. I contributed to BFlow's design, implementation, and evaluation.

INDUSTRY
EXPERIENCE

News.me/Digg
Data Scientist

New York, NY

June 2012 – August 2012

Member of the five-person engineering team which launched the new Digg.com in six weeks.

Designed and implemented a system for analyzing shared content on Twitter and Facebook, and using these and other signals generated trending, new, and breaking news. Currently used on Digg.com.

Google, Inc.
Senior Software Engineer

Mountain View, CA

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.

Led the verification of the transition of Google's entire billing system to a new vendor.

Developed the first system integration test bed for the ads backend serving system.

PUBLICATIONS

Su, L., Liu, Q.C. and **Narula, N.** *The Power of Random Symmetry-Breaking in Nakamoto Consensus*. In 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.

Böhme, R., Ekey, 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 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 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 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 Chorzempa, M. *Digital Currencies: Risk or Promise?*. Cato Journal, 2021.

Casey, M., Crane, J., Gensler, G., Johnson, S. and **N. Narula**. *The Impact of Blockchain Technol-*

ogy on Finance: *A Catalyst for Change*. ICMB, International Center for Monetary and Banking Studies, 2018.

POSTS,
ABSTRACTS, AND
REPORTS

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

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

Cline, D., Dryja, T. and **Narula, N.** *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

Co-chair, ACM Advances in Fintech Technology	2022
Program Committee, OSDI	2022
Program Committee, ACM Advances in Fintech Technology	2021
Program Committee, Financial Cryptography	2020-2021
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-present
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

Shwetark Patel, MEng CS, MIT	2021-present
James Lovejoy, MEng CS, MIT (now an engineer at the Boston Fed)	2019-2020
Henry Aspegren, MEng CS, MIT (now a Product Manager at Google)	2017-2018

	Willy R. Vasquez, MEng CS, MIT (now a PhD student at UT Austin)	2016-2017
TEACHING	<p>MIT/GetSmarter online cryptocurrency course Co-lead with Gary Gensler</p> <p>Blockchain Lab MIT 15.S68, 15.217 Co-lecturer with Michael Casey, Gary Gensler, and Simon Johnson Co-lecturer with Simon Johnson, Gary Gensler, and Luis Barros</p> <p>Cryptocurrency Engineering and Design (MIT MAS.S62) Co-lecturer with Tadge Dryja. Available on MIT Open Courseware.</p> <p>Shared Public Ledgers: Cryptocurrencies, Blockchains, and Other Marvels (MIT 6.892) Co-lecturer with Silvio Micali</p> <p>Distributed Systems (MIT 6.824) Teaching Assistant Guest lecturer</p> <p>Computer Systems Engineering (MIT 6.033) Teaching Assistant</p>	<p>Fall 2019</p> <p>Spring 2019, 2020 Spring 2021</p> <p>Spring 2018</p> <p>Spring 2017</p> <p>Spring 2013</p> <p>Spring 2011</p>
SELECT MEDIA	<p>CBS 60 minutes. <i>Bitcoin's Wild Ride</i></p> <p>Wall Street Journal. <i>Does the U.S. Need a National Digital Currency?</i></p> <p>The New Yorker Live. <i>How Memes Become Money</i></p> <p>Amanpour & Co. <i>Currency Futurist Neha Narula Debunks Cryptocurrency</i></p> <p>Wired.com. <i>The Blockchain: Boon for Bankers or Tool for Tyrants?</i></p> <p>Techcrunch.com. <i>Cryptocurrency Insecurity: IOTA, BCash and Too Many More</i></p> <p>Motherboard.com. <i>A \$5 Billion Cryptocurrency Has Enraged Cryptographers</i></p> <p>CNBC. <i>Digital Currency Could Change How We Deal with Money</i></p> <p>PBS Newshour. <i>The How and Why of Buying Bitcoin</i></p> <p>Wired.com. <i>Decentralized Social Networks Sound Great. Too Bad They'll Never Work</i></p> <p>Harvard Business Review. <i>The Blockchain Will Do to the Financial System What the Internet Did to Media</i></p> <p>Wired.com. <i>MIT Computer Scientists Demonstrate the Hard Way That Gender Still Matters</i></p> <p>Reddit.com. <i>We're 3 Female Computer Scientists from MIT. Ask us anything!</i></p>	
HONORS AND AWARDS	<p>IEEE Symposium on Security and Privacy Test of Time Award</p> <p>IMSA Alumni Trailblazer Award</p> <p>WIRED 25 Leaders Shaping the Next 25 Years of Technology</p> <p>Academy of Achievement Delegate</p> <p>Thinkers50 Radar list</p> <p>Fortune's The Ledger 40 under 40 list</p> <p>IEEE Symposium on Security and Privacy Best Paper Award</p> <p>Eben Tisdale Fellowship (declined)</p> <p>NSF Graduate Research Fellowship</p> <p>High Honors in Computer Science</p> <p>Inducted into Sigma Xi</p>	<p>2021</p> <p>2021</p> <p>2019</p> <p>2019</p> <p>2018</p> <p>2018</p> <p>2010</p> <p>2009</p> <p>2007</p> <p>2003</p> <p>2003</p>
SELECT INVITED TALKS	<p>Central Bank Digital Currency: Risks and Opportunities Hoover Institute, Stanford</p>	<p>July 2021</p>

Digitizing the Dollar Congressional testimony before the House Task Force on Financial Technology	June 2021
Building A Stronger Financial System: Opportunities of a Central Bank Digital Currency 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
Economic Security of Proof-of-Work Chaincode, New York, NY.	July 2019
The Architecture of Crypto Innovation a16z Crypto Regulatory Summit	May 2019
SEC FinTech Forum Panel on Trading and Markets Considerations	April 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
SXSW, Austin, TX	March 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 (2.3M views).	May 2016
Trading Simplicity for Performance When Designing Distributed Systems Mesosphere, San Francisco, CA.	October 2015
MesosCon (keynote), Seattle, WA.	August 2015
Splitting and Replicating Data for Fast Transactions: Don't Give Up on Serializability Just Yet	

OREDEV, Malmo, Sweden.	November 2015
CRAFT, Budapest, Hungary.	April 2015
GOTO Chicago, Chicago, IL.	April 2015
Papers We Love: The Scalable Commutativity Rule	
Papers We Love, New York, NY.	April 2015
A Multi-core Database Is Not a Distributed System	
CIDR short talk, Asilomar, CA.	January 2015
Phase Reconciliation for Contended In-Memory Transactions	
RICON, Las Vegas, NV.	October 2014
OSDI, Broomfield, CO.	October 2014
MIT Industry Affiliate Program Cloud Workshop, Cambridge, MA.	September 2014
Consensus and Consistency: Why Should I Care?	
Berlin Buzzwords, Berlin, Germany.	May 2014
The Good, the Bad, and the Ugly (of Caching)	
All Your Base (keynote), Oxford, UK.	October 2013
Smarter Caching With Pequod	
RICON East, New York, NY.	May 2013
Executing Queries on a Sharded Database	
Future of Webapps, Las Vegas, NV.	October 2013
Future Insights Live, London, UK.	May 2013
Strangeloop, St. Louis, MO.	September 2012
Hacker School, New York, NY.	August 2012
USENIX Webapps, Boston, MA.	June 2012