Neha Narula

1 Broadway, 14th floor
Cambridge, MA 02142

narula@gmail.com
http://nehanarula.org

Interests

Cryptocurrencies and distributed systems.

Education

Massachusetts Institute of Technology Cambridge, MA
Ph.D. in Computer Science September 2010 – June 2015

Advisors: Robert T. Morris and Eddie Kohler
Thesis: *Parallel Execution for Conflicting Transactions*

Massachusetts Institute of Technology Cambridge, MA
M.S. in Computer Science January 2008 – September 2010

Advisor: Robert T. Morris.
Thesis: *Distributed Query Execution on a Replicated and Partitioned Database*

Dartmouth College Hanover, NH
B.A. in Computer Science and B.A. in Mathematics September 1999 – 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. Responsible for a team doing research, writing software, and teaching classes. Includes advising undergraduates and masters students.

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.

b_verify. b_verify is a system for efficiently preventing an untrusted server from equivocating on the contents of multiple logs. A single b_verify server can provide non-equivocation for millions of applications and handle thousands of new log statements per second. It accomplishes this by efficiently recording many statements anchored on Bitcoin. Users maintain small proofs which require downloading kilobytes of data per day. We implement b_verify and show that users can easily run b_verify clients on mobile phones.

MIT CSAIL Cambridge, MA
Research Assistant in PDOS January 2008 – May 2015

Doppel. Doppel is 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.

Pequod. Pequod is an in-memory distributed caching layer which can automatically materialize and update the results of simple joins. It simplifies programs which manually perform incremental updates to cached objects, like Twitter timelines, while beating the performance of in-memory key-value caches like Redis and memcached.

Dixie. Dixie is 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.

Professional Experience

News.me/Digg New York, NY
Data Scientist 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. 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 two new countries.

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.

Peer-reviewed Publications

Narula, N., Vasquez, W. and Virza, M. *zkLedger: Privacy-Preserving Auditing for Distributed Ledgers.* In NSDI. Renton, WA, 2018.

Narula, N., Cutler, C., Kohler, E. and R. Morris. *Phase Reconciliation for Contended In-memory Transactions.* In OSDI. Broomfield, Colorado, 2014.

Kate, B., Kohler, E., Kester, M., **Narula, N.**, Mao, Y., and R. Morris. *Easy Freshness with Pequod Cache Joins.* In NSDI. Seattle, Washington, 2014.

Narula, N. and R. Morris. *Executing Web Application Queries on a Partitioned Database.* In USENIX Webapps. Boston, Massachusetts, 2012.

Chandra, R., Kim, T., Shah, M., **Narula, N.** and N. Zeldovich. *Intrusion Recovery for Database-*

backed Web Applications. In 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 IEEE Symposium on Security and Privacy. Oakland, California, 2010. **Best Paper Award**

Yip, A., **Narula, N.**, Krohn, M. and R.T. Morris. *Privacy-Preserving Browser-Side Scripting with BFlow.* In 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, Berlin, 2005.

Posters, Abstracts, and Reports

Casey, M., Crane, J., Gensler, G., Johnson, S. and **Narula, N.**. *The Impact of Blockchain Technology on Finance: A Catalyst for Change.* In Geneva Reports, Geneva, 2018.

Heilman, E., **Narula, N.**, Dryja, T. and Virza, M. *IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency.* Report, 2017.

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

Narula, N. *A Multi-core Database is not a Distributed System.* In CIDR. Asilomar, California, 2015.

Narula, N. and R. Morris. *Designing a Toolkit for Distributed Storage in Web Applications.* Poster at SOSP. Big Sky, Montana, 2009.

Talks

A Tangled Curl: How We Forged Signatures in IOTA

Blackhat, Las Vegas, NV.	August 2018

zkLedger: Privacy-Preserving Auditing for Distributed Ledgers

MIT Bitcoin Expo, Cambridge, MA.	March 2018
Microsoft Research, Redmond, WA.	April 2018
NSDI, Renton, WA.	April 2018
PODC Blockchain Workshop, Egham, UK.	July 2018

The Future of Money

TED@BCG, Paris, France.	May 2016
Banco Central de Chile, Santiago, Chile.	December 2017
EmTech China, Beijing, China.	January 2018
SXSW, Austin, TX.	March 2018

The End of Data Silos: Interoperability via Cryptocurrencies

CRAFT, Budapest, Hungary.	April 2016
Bits and Blockchain Series, Fidelity, Cambridge, MA.	April 2016
Mahindra Group visit, Cambridge, MA.	May 2016

Trading Simplicity for Performance When Designing Distributed Systems

MesosCon (keynote), Seattle, WA.	August 2015
Mesosphere, San Francisco, CA.	October 2015

Splitting and Replicating Data for Fast Transactions: Don't Give Up on Serializability Just Yet

CRAFT, Budapest, Hungary.	April 2015
GOTO Chicago, Chicago, IL.	April 2015
OREDEV, Malmo, Sweden.	November 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

Service

Program Committee Member, Eurosys	2019
Program Committee Member, Scaling Bitcoin Milan	October 2016
Program Chair, Scaling Bitcoin Hong Kong	December 2015
Resident at Hacker School	April 2015
MIT EECS Faculty Search Student Subcommittee	Spring 2015
Leading MIT's distributed systems reading group	2014-2015
Member of the Google Mentoring Committee	2006-2008
Member of the Google Foundation Steering Committee	2003

Students

Henry Aspegren, MEng CS, MIT	2017-2018
Willy R. Vasquez, MEng CS, MIT	2016-2017

Teaching

Cryptocurrency Engineering and Design (MAS.S62)

Co-lecturer with Tadge Dryja	Spring 2018

Shared Public Ledgers: Cryptocurrencies, Blockchains, and Other Marvels (6.892)

Co-lecturer with Silvio Micali	Spring 2017

Distributed Systems (6.824)

Teaching Assistant — Spring 2013
Guest lecturer

Computer Systems Engineering (6.033)
Teaching Assistant — Spring 2011

Press

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*
WBUR.org. *Enough With The Lawsuits: Berklee, MIT Lead Effort To Create Ownership Rights Database For Music Industry*
BostonInno.com. *2015: The Year Women Take Back Tech*
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

Thinkers50 Radar list	2018
Fortune's The Ledger 40 under 40 list	2018
Eben Tisdale Fellowship (declined)	2009
NSF Graduate Research Fellowship	2007
High Honors in Computer Science	2003
Inducted into Sigma Xi	2003

References

Joi Ito
Director, Media Lab
Massachusetts Institute of Technology
joi@media.mit.edu

Robert T. Morris
Professor, Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
rtm@csail.mit.edu

Eddie Kohler
Associate Professor, School of Engineering and Applied Sciences
Harvard University
kohler@seas.harvard.edu

Barbara Liskov
Institute Professor, Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
liskov@piano.csail.mit.edu