Isaac Sheff

Curriculum Vitae

*"Incantations in a language no human being has ever spoken . . .
a world imagined within the pattern on the stone" - W D Hillis*

Research Interests

The future is distributed, cross-domain, full of complex trust and failure tolerance, and that's where I want to be. I design distributed protocols and algorithms with strong guarantees, real implementations, and broad applications from medical privacy to blockchains.

Education

2012-2019 **Ph.D. in Computer Science**, *Cornell*, Programming Languages & Systems.
Advisor: Andrew Myers — Systems Minor Advisor: Robbert van Renesse
Dissertation: *Serializability and Heterogeneous Trust from Two Phase Commit to Blockchains*

2016 **Master of Science**, *Cornell*, Computer Science, Programming Languages & Systems.

2008–2012 **Bachelor of Science**, *The California Institute of Technology*, CS Major, *GPA: 3.4*.

Employment

2019–Present **PostDoc**, *Max Plank Institute for Software Systems*, Saarbrücken, Germany.
I work with Peter Druschel on distributed systems with rich trust models, including high integrity & confidentiality databases with 2 party computation inside of trusted hardware.

2012-2019 **Ph.D. Candidate**, *Research Assistant / Teaching Assistant*, Cornell.
While most of my time as a Ph.D. Student is devoted to research, I have also participated in teaching both undergraduate and masters students.

2016-2017 **Research Intern**, *Oracle Labs East*, Burlington, Massachusetts.
I worked with Mark Moir, Harold Carr, Maurice Herlihy, and others on experimental sharded blockchains using Haskell and the Tangaroa byzantine consensus algorithm. (full-time summer, part-time remote for a year)

2012 **Software Engineering Intern**, *Google*, Los Angeles.
I worked with Eric Wood and the Google Ads team to keep Google-supported ads off policy-violating sites, gaining experience with MapReduce, Internet-Scale Datasets, C++ and large codebases. (see research)

Summer 2009-2011 **Summer Undergraduate Research Fellow**, *Caltech & JPL*.
I was awarded a $6,000 research fellowship three years running, and conducted research at Caltech and JPL in Physics and Computer Science. (see research)

Publications

In Preparation **CoVault: A Secure Framework for Epidemic Analytics**, *SOSP 2021*.
Roberta De Viti, Baltasar Dinis, Isaac Sheff, Noemi Glaeser, Deepak Garg, Peter Druschel
An epidemic-analytics framework that relies on state-of-the-art trusted execution environments and secure multi-party computation to ensure confidentiality, privacy, integrity, and transparency under a strong threat model that includes TEE compromise and side channels.

In Submission **ProLoc: Trustworthy Mobile Device Trajectories**, *MobiSys 2021*.
Roberta De Viti, Pierfrancesco Ingo, Isaac Sheff, Deepak Garg, Peter Druschel
We propose algorithms and techniques for inferring high-integrity location data using GPS and bluetooth encounters from phones in an open system, even in the presence of faulty GPS and malicious adversaries.

In Preparation **Charlotte: Composable Authenticated Distributed Data Structures**, .
Isaac Sheff, Xinwen Wang, Haobin Ni, Robbert van Renesse, Andrew C. Myers (more info at isaacsheff.com)
Charlotte is a framework for composable, Authenticated Distributed Data Structures, such as blockchains, torrents, and version control systems. We implement several example Charlotte applications.

2020 **Heterogeneous Paxos**, *Conference on Principles of Distributed Systems (OPODIS)*.
Isaac Sheff, Xinwen Wang, Robbert van Renesse, Andrew C. Myers (more info at isaacsheff.com)
Generalizing Lamport's *Byzantized Paxos*, we present the first consensus algorithm with heterogeneous failures, heterogeneous acceptors, and heterogeneous learners: everyone decides for themselves with whom they must agree, under which failure conditions. We demonstrate our implementation using Charlotte blockchains.

2016 **Safe Serializable Secure Scheduling**, *Conference on Computer and Communications Security*.
Isaac Sheff, Tom Magrino, Jed Liu, Andrew C. Myers, Robbert van Renesse (available at isaacsheff.com)
We explore atomic transactions featuring data in multiple trust domains, and uncover a fundamental trade-off between security and consistency.

Technical Reports

2020 **Heterogeneous Paxos**, *Cornell*.
Generalizing Lamport's *Byzantized Paxos*, Xinwen Wang, Robbert van Renesse, Andrew C. Myers and I present the first consensus algorithm with heterogeneous failures, heterogeneous acceptors, and heterogeneous learners. We demonstrate our implementation using Charlotte blockchains. (report at `isaacsheff.com`)

2019 **Charlotte: Composable Authenticated Distributed Data Structures**, *Cornell*.
Charlotte is a framework for composable, Authenticated Distributed Data Structures, such as blockchains, torrents, and version control systems. (report at `isaacsheff.com`)

2018 **A Web of Blocks**, *Cornell*.
An earlier iteration of our Charlotte paper, and prototype implementation. (report at `isaacsheff.com`)

2014 **Distributed Protocols and Heterogeneous Trust**, *Cornell*.
Myself, Andrew Myers, and Robbert van Renesse use the Decentralized Label Model to show how distributed algorithms, like Bosco and Nysiad, can be generalized with more complex trust. (report at `isaacsheff.com`)

2013 **Stable Paxos**, *Cornell*.
Working with Ken Birman, I investigated some potential slowdown cases of the classic multi-Paxos algorithm, and developed some new variants to avoid them. (report at `isaacsheff.com`)

2013 **Automated Artist Identification**, *Cornell*.
With novel, carefully tuned features, neural nets, and SVMs, Daniel Schroeder and I were able to determine the author of samples from a group of ten webcomic artists with 94% accuracy. (report at `isaacsheff.com`)

2011 **Branching Messaging for Anonymous Communication**, *Caltech*.
As a Summer Undergraduate Research Fellow, I worked with Professor Tracey Ho to develop an algorithm for anonymous communication in the presence of an observer with knowledge of all traffic on the network graph, as well as compromised nodes. Through theoretical analysis and simulation, we found that strong statistical anonymity with logarithmic latency, and minimal overhead traffic is possible. (report at `isaacsheff.com`)

2010 **NuSIM**, *Caltech*.
As a Summer Undergraduate Research Fellow, I worked with Fiona Harrison, Kristin Madsen, and the rest of the NuSIM team to test and improve a simulation of the NuSTAR space telescope prior to launch. The purpose of NuSIM is to verify and validate as many of NuSTAR's mission capabilities as possible before launch. As part of this project, I worked with other coders and astrophysicists on the codebase of NuSIM, as well as building utilities and running simulated tests and analysis. (report at `isaacsheff.com`)

2009 **Lunar Web Registry Service Under OpenGIS Specifications**, *JPL*.
As a Summer Undergraduate Research Fellow, I worked with Dr. Lucian Plesea at the Jet Propulsion Laboratory on a Geospatial Coordinate System Registry for the moon, similar to the EPSG registry for the earth. During this project I explored different web service architectures, ISO standards, and the complex systems used by software to manage Geospatial Coordinate Systems. (report at `isaacsheff.com`)

Presentations

December 2020 **Heterogeneous Paxos**, *OPODIS*, online.
Isaac Sheff, Xinwen Wang, Robbert van Renesse, Andrew C. Myers
Generalizing Lamport's *Byzantized Paxos*, we present the first consensus algorithm with heterogeneous failures, heterogeneous acceptors, and heterogeneous learners: everyone decides for themselves with whom they must agree, under which failure conditions. (slides and video at isaacsheff.com)

May 2018 **Multi-Chain Transactions (with Demo)**, *IC3 Fall Retreat*, Cornell Tech, New York City.
Isaac Sheff, Andrew C. Myers, Robbert van Renesse
With Charlotte, we can append one block onto multiple blockchains, solving the atomic commit problem. This demo uses our Heterogeneous Consensus algorithm. (slides at isaacsheff.com)

December 2017 **S.C.A.I.f. Block-Webs with Charlotte**, *Tsinghua Winter School on Blockchain*, Shenzhen.
Isaac Sheff, Andrew C. Myers, Robbert van Renesse
A work in progress talk about Scalability, Confidentiality, Availability, and Integrity for Block-Webs with the Charlotte Framework. (slides & transcript at isaacsheff.com)

July 2017 **Heterogeneous Consensus**, *IC3-Ethereum Crypto Boot Camp*, Cornell, Ithaca, NY.
Isaac Sheff, Andrew C. Myers, Robbert van Renesse
A work-in-progress talk about our Heterogeneous Consensus algorithm. (slides & transcript at isaacsheff.com)

October 2016 **Safe Serializable Secure Scheduling**, *Conference on Computer and Communications Security*.
Isaac Sheff, Tom Magrino, Jed Liu, Andrew C. Myers, Robbert van Renesse
We explore atomic transactions featuring data in multiple trust domains, and uncover a fundamental trade-off between security and consistency. (youtu.be/ZO_6UAwDAQg)

September 2016 **Abort Channels**, *Programming Languages Retreat*, Cornell.
Isaac Sheff, Tom Magrino, Jed Liu, Andrew C. Myers, Robbert van Renesse
We present a successfully implemented attack on traditional atomic commit methods across trust domains, and explain what is necessary to secure this new information channel.

August 2015 **Secure Distributed Transactions**, *Programming Languages Retreat*, Cornell.
Isaac Sheff, Tom Magrino, Robbert van Renesse, Andrew C. Myers
A work-in-progress talk about atomic transactions featuring data in multiple trust domains.

August 2014 **Distributed Protocols and Heterogeneous Trust**, *Programming Languages Retreat*, Cornell.
Isaac Sheff, Andrew C. Myers, Robbert van Renesse
A work-in-progress talk about two algorithms: Bosco Fast Consensus, and Nysiad Omission to Byzantine Tolerant Conversion, adapted to a Heterogeneous Trust setting using the Decentralized Label Model.

Patent

2018 **Sharded Permissioned Distributed Ledgers**, *US 2018/0341930 A1*.
Mark S. Moir, Harlold Carr, Maurice P. Herlihy, Isaac Sheff

Other Research Projects

Ongoing **New Building Blocks for Secure, Correct Distributed Systems**, *Cornell*.
I have proposed a new language, tentatively called *TinyTX*, in which to express low-level distributed algorithms with provable Information Flow based security properties. (more at `isaacsheff.com`)

2016-2017 **Sharded Permissioned Distributed Ledgers**, *Oracle Labs East*, Burlington, Massachusetts.
I worked with Mark Moir, Harold Carr, Maurice Herlihy, and others on experimental sharded blockchains using Haskell and the Tangaroa byzantine consensus algorithm.

2013–2015 **Heterogeneous Fast Consensus**, *Cornell*.
I have adapted Robbert van Renesse's *Bosco: Fast Consensus* algorithm to a world in which not everyone has the same idea of who can fail, and what "failure" means, taking advantage of the richer notion of trust provided by the Decentralized Label Model. ("Distributed Protocols" report available at `isaacsheff.com`)

2014–2015 **Heterogeneous Omission to Byzantine Conversion**, *Cornell*.
Similarly, I've adapted Robbert van Renesse's *Nysiad: Omission Tolerant to Byzantine Tolerant Conversion* algorithm in terms of Information Flow. ("Distributed Protocols" report available at `isaacsheff.com`)

2012 **Learning From Internet Link Graph Structure, and Porn**, *Google*.
I interned at Google LAX, preventing Google's ads from appearing on porn sites. This was part of a large-scale machine learning project featuring whole-internet size datasets and massively parallelized algorithms.

Academic Service

2021 – Present **Editorial Board, Distributed Consensus**, *Journal of Systems Research (JSys)*.

2019 **Technical Program Committee**, *IEEE Conference on Blockchain and Cryptocurrency*.

2017 **Artifact Evaluation Committee**, *ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming / International Symposium on Code Generation and Optimization*.

Teaching Experience

Spring 2015 & 2016 **Graduate Teaching Assistant**, *CS 4320 / 5320*, Cornell.
Introduction to Database Systems with Lucja Kot (Senior & Masters Level) — HW creation, grading, OH

Spring 2013 **Graduate Teaching Assistant**, *CS 2110*, Cornell.
Object Oriented Programming and Data Structures with Ken Birman and David Gries (Undergraduate Level) — Organizing 30-40 TAs, creating recitation curriculum for this and future years, grading, recitation, OH

Fall 2012 **Graduate Teaching Assistant**, *CS 5414*, Cornell.
Distributed Computing Principles with Fred Schneider (Masters Level) — Grading, office hours

Fellowships and Awards

2013 Outstanding Contributions as a Teaching Assistant

2009–2011 Three Distinct Summer Undergraduate Research Fellowships

Selected Coursework

2012-2015 **Cornell**.

CS 6110 Advanced Programming Languages
CS 6113 Language Based Security
CS 6117 Category Theory for Computer Scientists
CS 6410 Advanced Systems
CS 6820 Analysis of Algorithms
CS 6700 Advanced Artificial Intelligence

2008-2012 **California Institute of Technology**.

CS 141a	Distributed Computing	CS 151	Complexity Theory	CS 156ab	Learning Systems
CS 146	Advanced Networking	CS 101a	Algorithmic Game Theory	CS 101c	GPU Programming