



# 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

- 2022-Present **Principal Research Scientist**, *Heliix.dev*.  
I research advanced protocols for tracking and maintaining integrity in cross-domain applications. I work with mathematicians and engineers to open new doors for product development, and ensure products provide strong, well-defined guarantees for customers.
- 2019-2022 **PostDoc**, *Max Plank Institute for Software Systems*, Saarbrücken, Germany.  
I worked 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 **Summer Undergraduate Research Fellow**, *Caltech & JPL*.
- 2009-2011 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 Progress

- Work In Progress **Cross-Domain Integrity With Controller Tags and Attestation.**  
*Isaac Sheff, Murdoch "Jamie" Gabbay*  
We design rules and procedures for a multi-controller ecosystem, featuring mutable digital objects that move between controllers. Each object carries a tag, with which users can judge whether the object's history is serializable, based on their own trust assumptions. These generalize token wrapping for arbitrary computation objects.

Work In Progress **Consistent histories: enforcing linearity and excluding double-spending amongst collaborating controllers.**

*Murdoch "Jamie" Gabbay, Isaac Sheff*

We develop a mathematical formalization of controllers, and a new primitive called *attestation*, in which one controller checks another. With this framework, we tag resources that move between controllers, so users can know if some collection of resources violate linearity (contain the results of both sides of a double-spend).

In Submission **Heterogeneous trust in reliable broadcast via modal logic and history structures, *Information and Computation*.**

*Murdoch "Jamie" Gabbay, Isaac Sheff*

We develop a novel modal logic and semantics for specifying and proving properties of distributed full-information-transfer protocols, and use this to design and prove correctness of novel generalisations of Bracha's 'reliable broadcast' algorithm to a heterogeneous trust setting. The maths has been mechanically formalised and checked.

In Submission **ProofLoc: Robust Location Proofs in Hindsight, *UbiComp*.**

*Roberta De Viti, Pierfrancesco Ingo, Isaac Sheff, Peter Druschel, Deepak Garg*

ProofLoc infers a bounded area within which a device must have been at a given time, with no deployed infrastructure. It uses uploaded movement trajectories, short-range radio (BLE) contacts with nearby devices, and transportation-network constraints, and defends against attacks using a TrustRank variant on the device-encounter graph.

---

## Peer-Reviewed Publications

2025 **CoVault: Secure, Scalable Analytics of Personal Data, *USENIX Security*.**

*Roberta De Viti, Isaac Sheff, Noemi Glaeser, Baltasar Dinis, Rodrigo Rodrigues, Bobby Bhattacharjee, Anwar Hithnawi, Deepak Garg, Peter Druschel*

CoVault uses different trusted execution environment implementations (e.g. Intel TDX and AMD SEV) as the parties for secure multi-party computation, ensuring confidentiality and integrity even when one of the TEE types (and all of the host computers) are compromised. The platform can perform epidemic analytics for a country of 80 million people on a continuous basis.

2023 **Charlotte: Reformulating Blockchains into a Web of Composable Attested Data Structures for Cross-Domain Applications, *ACM Transactions on Computer Systems*.**

*Isaac Sheff, Xinwen Wang, Kushal Babel, Haobin Ni, Robbert van Renesse, Andrew C. Myers*

Charlotte is a framework for composable, Authenticated Distributed Data Structures (ADDSSs), like blockchains, git, bittorrent, etc.

2020 **Heterogeneous Paxos, *Conference on Principles of Distributed Systems (OPODIS)*.**

*Isaac Sheff, Xinwen Wang, Robbert van Renesse, Andrew C. Myers*

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 have a formally verified safety proof in TLAPS, and are working on a liveness proof.

2016 **Safe Serializable Secure Scheduling, *ACM 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.

---

## Technical Reports

2024 **Anoma State Architecture.**

*Isaac Sheff*

I designed a state layout for the Anoma virtual machine, to maximize concurrency for serializable transactions. It facilitates both transparent and shielded updates using general-purpose anoma resource machine resources, and is intended for use with the proposed Typhon replicated state machine system.

2024 **Heterogeneous Narwhal and Paxos.**

*Tobias Heindel, Aleksandr Karbyshev, Isaac Sheff*

We explore generalizing the Narwhal Mempool for a heterogeneous setting using a learner graph, and achieve total ordering using Heterogeneous Paxos.

2018 **A Web of Blocks, *Cornell*.**

An earlier iteration of our Charlotte paper, and prototype implementation.

- 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.
- 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.
- 2013 **Webcomic Author 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.
- 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.
- 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.
- 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.

## Presentations

- December 2025 **Controller Tags for Cross-Chain Integrity**, *Anoma Day*.  
*Isaac Sheff* (slides & video at isaacsheff.com)  
A work-in-progress talk for our controller tags research.
- March 2025 **Store, Order, Execute**, *Anoma Research Day*.  
*Isaac Sheff* (slides & video at isaacsheff.com)  
A proposed next-generation architecture for blockchains with high throughput and unlimited concurrency, supporting serializability for (mostly) arbitrary state machines.
- 2023 **Chimera Chains: Cross-Domain Atomic Commits Using Heterogeneous Paxos**, *Workshop on Heterogeneous Trust in Distributed Systems*.  
*Isaac Sheff* (slides & video at isaacsheff.com)  
Chimera Chains are a technique for cross-domain atomic transactions making use of Heterogeneous Consensus, using overlapping trust assumptions to commit directly to multiple state machines simultaneously without the liveness blocks or multi-round requirements of multi-phase commits.
- July 2022 **Typhon, Chimera Chains, and Multi-Chain Atomic Transactions**, *Nebular Summit*, Paris.  
*Isaac Sheff* (slides & video at isaacsheff.com)  
A work-in-progress talk laying out the vision for our Typhon ordering and execution stack, and how chimera chains can enable cross-chain atomic transactions between chains using Typhon.
- December 2020 **Heterogeneous Paxos**, *OPODIS*, online.  
*Isaac Sheff, Xinwen Wang, Robbert van Renesse, Andrew C. Myers* (slides & video at isaacsheff.com)  
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.
- May 2018 **Multi-Chain Transactions (with Demo)**, *IC3 Fall Retreat*, Cornell Tech, New York City.  
*Isaac Sheff, Andrew C. Myers, Robbert van Renesse* (slides & video at isaacsheff.com)  
With Charlotte, we can append one block onto multiple blockchains, solving the atomic commit problem. This demo uses our Heterogeneous Consensus algorithm.
- 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* (slides at isaacsheff.com)  
A work in progress talk about Scalability, Confidentiality, Availability, and Integrity for Block-Webs with the Charlotte Framework.
- July 2017 **Heterogeneous Consensus**, *IC3-Ethereum Crypto Boot Camp*, Cornell, Ithaca, NY.  
*Isaac Sheff, Andrew C. Myers, Robbert van Renesse* (slides at isaacsheff.com)  
A work-in-progress talk about our Heterogeneous Consensus algorithm.

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

- 2016–2019 **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