Derek Sorensen

Curriculum Vitae

Education

2019 - 2022 **PhD Candidate (Mathematical Logic)**, *University of Cambridge*.

2016–2017 **MSc in Mathematics and Foundations of Computer Science**, *University of Oxford*.

2013–2016 **BSc in Mathematics**, *Brigham Young University*, Provo, UT, USA.

Employment

Oct 2019 - Present **Senior Formal Verification Engineer**, *Clearmatics*, London, United Kingdom.
- Design, formally specify, and formally verify cryptocurrency systems.
- Develop the software development life cycle to formally verify Ethereum smart contracts.

Jul 2019 - Sep 2019 **Cryptocurrency Consultant**, *Digital Asset*, New York, NY.
- Designed and built a functional cryptocurrency that supports legal compliance and privacy.
- Specified privacy model, fee structure, minting structure, and incentive systems.

Mar 2018- Jun 2019 **Research Mathematician**, *Pyrofex Corporation*, Provo, UT.
- Research in the fundamental algorithms supporting cryptocurrencies.
- Developed cryptocurrency that can process transactions at the rate of Visa.
- Built the formal semantics for Rholang in K-Framework for the RChain Coop.

2017-2019 **Adjunct Faculty (Mathematics)**, *Utah Valley University*, Orem, UT.
- Wrote lecture notes, homework, quizzes, exams.
- Marked and give feedback to all written work.

Mathematical Interests

I specialize in mathematical logic and its applications to the design and security of blockchains and cryptocurrencies. I am currently focused on algorithm design and security within cryptocurrencies, including economic and incentive structures. Within pure maths, I'm interested in synthetic homotopy theory, specifically formalizing results from analytic homotopy theory regarding loop spaces, moduli spaces, spectral sequences, and stable homotopy theory.

Preprints

2019 Maric, O., Lochbihler, A., Sorensen, D. CantonCoin: Gaining Horizontal Scalability and Privacy with Distributed Commits Instead of Global Consensus. (2019) (Awaiting response from Cryptoeconomic Systems 2020.)

Flat 31, Auckland Ct, Auckland Rd – Cambridge, UK CB5 8DS
✉ *derekhsorensen@gmail.com* • *derekhsorensen.com*

2018 Butt, K., Sorensen, D., Stay, M. Casanova. (2018) https://arxiv.org/abs/1812.02232
(Awaiting response from IEEE.)

Publications

2019 Butt, K., Sorensen, D. *Streamlining Classical Consensus*.
(To appear in IJBC.)

2019 Sorensen, D. *Establishing Standards for Consensus on Blockchains*.
(To appear in the 2019 International Conference on Blockchain.)

2017 A. Francis, D. Smith, D. Sorensen and B. Webb, *Extensions and applications of equitable decompositions for graphs with symmetries*. Linear Algebra and its Applications **532** (2017), 432-462.

Scholarships and Awards

2016 Robert K Thomas Honors Scholarship

2015 AMS Math in Moscow Travel Grant

2015 Marc Burton Scholarship

2015 Best of session at the 2015 BYU Spring Research Conference

2014 & 2015 Award for Excellence in Undergraduate Research

2014 & 2015 Award for Academic Excellence in Mathematics

Teaching

Lent 2021 Groups, Rings, and Modules (University of Cambridge)

Mich. 2020 Economics, Law, and Ethics (University of Cambridge)

Mich. 2020 Analysis & Topology (University of Cambridge)

Lent 2020 Groups, Rings, and Modules (University of Cambridge)

Spring 2019 Stat 1040 - Introduction to Statistics (Utah Valley University)

Spring 2018 Stat 1040 - Introduction to Statistics (Utah Valley University)

Spring 2018 Stat 2040 - Introduction to Statistics (Utah Valley University)

Spring 2018 Math 1050 - College Algebra (Utah Valley University)

Presentations

2018 Rholang Semantics and the K-Framework, **RCon3**, *Berlin, Germany*

2018 Formal Verification Panel, **RCon3**, *Berlin, Germany*

2015 Presentation at the 2015 BYU Spring Research Conference
- Voted best of session

2014 Presentation at the 2014 BYU Spring Research Conference

Summer Schools

2019 Interenational Conference and Summer School of Homotopy Type Theory

2017 CMI-LMS Research School Algebraic Topology of Manifolds

Computer skills

Basic C++, Haskell

Competent Formal verification in Agda, TLA+, and K
DAML

Languages

Native English

Fluent Spanish

Intermediate Russian

Basic French

Flat 31, Auckland Ct, Auckland Rd – Cambridge, UK CB5 8DS
derekhsorensen@gmail.com • *derekhsorensen.com*