

Derek Sorensen

d@dhsorens.com | derekhsorensen.com

EDUCATION

University of Cambridge

PhD in Theoretical Computer Science

Cambridge, UK

2019 – 2023

University of Oxford

MSc in Mathematics and Foundations of Computer Science

Oxford, UK

2016 – 2017

EXPERIENCE

Formal Verification Wizard

Certora

Jan 2024 – April 2025

Remote (UK)

- Audited code for top-tier EVM-based DeFi protocols, including Silo and Safe.
- Thoroughly read, formally specified, and formally verified all audited code, providing a detailed written report.
- Managed client relationships and projects and developed new DeFi security products.

Software Engineer

Protocol Labs

Oct 2022 – Feb 2023

Remote (UK)

- Contributor to Lurk, a Turing complete dialect of LISP for zero-knowledge proofs.
- Used formal verification expertise to build a shell for manipulating ZK proofs as first-class objects.

R&D (Sustainability and Carbon Offsets)

Trilitech

May 2021 – Aug 2022

London, UK

- Audited, formally specified, and formally verified DeFi contracts for the Tezos blockchain.
- Lead business development for sustainability on the Tezos blockchain, including tokenized carbon offsets, regenerative finance (ReFi), and sustainability-oriented art marketplaces.
- Member of the Technical Advisory Committee, the funding body for the Tezos Foundation

Senior Software Engineer (Formal Verification)

Clearmatics

Oct 2019 – Nov 2020

London, UK

- Advised the company's formal verification agenda for Ethereum smart contracts.
- Wrote seminar series to train a team of ten engineers in mathematics.

Blockchain Consultant

Digital Asset

Jul 2019 – Sep 2019

New York, New York

- Designed and built a functional cryptocurrency in DAML on the Canton Network.
- Wrote a paper with two teammates outlining the industry-leading privacy features of the novel cryptocurrency.
- Held regular meetings with company executives and gave a live tutorial of the novel cryptocurrency.

Research Mathematician

Pyroflex Corporation

Mar 2018 – Jun 2019

Provo, Utah, USA

- Created a cryptocurrency that is 7,000 times faster than Bitcoin, and processes 50% more transactions than Visa.
- Coauthored, presented, and promoted three peer-reviewed, disruptive papers on blockchain scalability.
- Consulted as chief mathematician on two major industry projects involving cryptocurrency.

PROGRAMMING LANGUAGES

Lean, Coq, CameLIGO, Solidity, CVL, K Framework, Python

ADDITIONAL SKILLS

Spoken Languages: English (native), Spanish (fluent), Russian (intermediate), French (beginner)

Additional Interests: Alpine skiing, English choral music, bouldering, classical voice, Homotopy Type Theory (HoTT)