

Education

- **University of Texas at Austin** Austin, TX, USA
M.A., Mathematics Sept. 2013 – Jan. 2015
 - Completed preliminary coursework one year ahead of schedule
 - Focus on applied cryptography
- **Simon Fraser University** Burnaby, BC, CA
B.Sc., Mathematics; CGPA: 3.6 Sept. 2008 – May 2013
 - Minor: physics
 - Waived/challenged computing science requirements through second year

Professional Experience

- **Blockstream** remote, Austin, TX
Mathematician August 2014 – present
 - Invented, proved secure and implemented several cryptosystems
 - Created autonomous financial systems which work in adversarial environments
 - Published papers, gave talks, communicated with press and public about my work
- **Delta Controls** Surrey, BC
Software Development Jan. 2010 – Sept. 2010
 - Wrote boot-loader recovery code to solve field issues overseas; saved hundreds of thousands of dollars by prevented RMA's
 - Assessed hardware designs for future products
 - Software development: wrote software to automate assembly-line circuit board configuration
 - Software QA: developed, maintained and executed test cases; documented and helped fix in-house software bugs

Open Source

- **libsecp256k1** Sept. 2013 – Present
<https://www.github.com/bitcoin/secp256k1>
 - High-performance cryptographic library
 - Algebraically verified correct operation; identified and corrected errors
 - Analyzed proposed improvements, including original mathematical research
 - Implemented ECDH secret sharing
 - Implemented high-performance modular inversion and Jacobi symbol calculation
- **pcb** Summer 2011
<http://sourceforge.net/projects/pcb/>
 - Printed circuit board editor
 - Overhauled internal measurement tracking; significant code quality improvements
 - Replaced several UI elements
- Contributed code to: Bitcoin, Rust, rust-crypto, creator of RamseyScript and several Bitcoin-related Rust packages
- Published several popular and academic papers about these projects.

Skills

Languages: C, Rust, Lisp, Python; have 20 years experience programming, 12 years in C

Projects: pcb; Stereo bicycle battery-powered, shock and weather resistant amplifier; Finex online money management; Bitcoin cryptocurrency development and research;