Andrew Poelstra

I am a mathematician and work for Blockstream where I analyze, design, and contribute to the development and implementation of protocols for zero-knowledge proof and decentralized consensus; identify and solve mathematical sub-problems that arise in the design implementation, and operations of distributed and/or cryptographic systems; review and understand state-of-the art literature in relevant fields (e.g. number-theory, cryptography, crypto-currencies, computer security) and support developers building and optimizing implementations; write peer-reviewed technical publications describing new algorithms and protocols.

Grew up in Cloverdale, BC. Attended Simon Fraser University, received a BSc with Honours and (co) authored several papers. Moved to the University of Texas at Austin, where I completed a MA in mathematics while working on open-source cryptography projects in my spare time. Left school to pursue my outside interests, since applied cryptography was more immediately practical than my academic research.

I had an early interest in mathematics, in particular cryptography, from learning about recent efforts to decode ENIGMA-ciphered messages from World War Two. I did a bachelor's degree in math in which I explored many fields. Near the end of this I encountered the cypherpunk movement, a group of activists and developers using applied cryptography for social good. At the time, the cryptocurrency Bitcoin had recently been invented, and there were a lot of accessible research questions surrounding it. My informal work on this was strongly complemented by my formal training in mathematics, and I felt it was an excellent use of my skillset. I now work full-time doing applied cryptography.