Thesis Project Portfolio

Cryptography: How to Build an Intuitive Cryptographic Library without Sacrificing Power

(Technical Report)

Decentralization vs. Security: The Ethical Dilemma of Cryptocurrency

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Daniel Evan Farmer

Spring, 2025

Department of Computer Science

Table of Contents

Executive Summary

Computer science is a rapidly evolving field, with new technologies emerging every day. However, rapid innovation has been met with cyber criminals constantly looking for ways to exploit new technologies, justifying the importance of cryptography in protecting personal data. Cryptocurrency, for example, has amassed controversy as this technology has served as a vehicle for anonymous online crime. My technical report details the development of an intuitive yet powerful cryptographic library for the C programming language, made to address the steep learning curve seen in many of today's cryptographic toolkits. My STS Research focuses on whether an ethical obligation exists for regulatory bodies and cryptocurrency developers to implement changes that will mitigate cybercrime. This question is important as cryptocurrency's fundamental values – anonymity and decentralization – have been co-opted for illicit activity. Improving cryptographic tools and strengthening the cryptocurrency ecosystem are not just technical challenges, they're matters of personal privacy in an era where such technologies are becoming a part of everyday life.

Cryptography is essential for developers looking to safeguard data and is primarily implemented through specialized libraries. However, in the C-programming language, these libraries are either powerful or easy to use, never both. My project aims to bridge this gap by developing a library that combines functionality with a low barrier to entry, enabling the user to accomplish essential cryptographic functions on the fly. To achieve this, I built my library on top of Libgcrypt, a powerful cryptographic library, so I could leverage its well tested algorithms. To promote usability, I modeled the library's semantics after Libsodium, which is known for its simplicity but lacks the depth of more advanced tools. This approach allows developers to access strong cryptographic functions through an approachable interface.

The result of this project was an intuitive powerful library that allows the user to accomplish essential and advanced cryptographic operations using a wide range of algorithms. To ensure correctness and reliability, the library was tested by substituting it into existing projects that use mainstream cryptographic toolkits. It was also rigorously analyzed with Valgrind to detect any memory leaks, ensuring memory safety for robust performance.

If cryptocurrency's promise of anonymity has made it the currency of choice for online crime, do developers have an ethical obligation to curb its misuse? Likewise, do regulatory bodies and governments have a moral obligation to put forth legislation aimed at preventing such abuse? By examining legislation in foreign countries, reports from government agencies, and the cypherpunk movement, amongst other sources, I aimed to find an answer to these questions.

This research made it clear that regulatory changes are necessary to deter this cybercrime. However, even if such changes were to take place in countries like the United States, for example, criminals often exploit arbitrage opportunities in other countries by moving to weaker jurisdictions. Compounding the issue, any changes to the blockchain itself need a majority consensus, which is very challenging in large, decentralized communities. Ultimately, effective cryptocurrency regulation requires an ongoing dialogue about how to balance privacy and security, as well as strong collaboration between developers and regulatory bodies.