Cryptocurrency Regulation and Security Enhancements

Ethics and Privacy in the Cypherpunk Movement

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Daniel Farmer

November 8, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Prof. Pedro Augusto P. Francisco, Department of Engineering and Society

Mark Floryan, Computer Science

Introduction

Cryptocurrencies represent a new era in international finance by enabling decentralized, peer-to-peer transactions that are seemingly anonymous, a novelty that is not without risk. Since their inception, many cryptocurrencies have cited anonymity as a fundamental value; however, this has quickly made them popular as a means of funding illicit activities such as money laundering, tax evasion, and ransomware payments (Greenberg, 2022). Due to these risks, the development of legal strategy and secure systems is imperative to guarantee that these technologies can advance and prosper while disentangling themselves from the criminal underworld.

In this prospectus, I will address the technical aspects of enhancing cryptocurrency through innovative regulatory and technological solutions while ensuring that privacy principles are respected. Based on case studies of blockchain's traceability (Chowdhury, 2022) and Switzerland's regulatory frameworks (Gesley, 2022), the technical project will attempt to strike a balance between traceability and the promise of anonymity and decentralization that are essential to the crypto community.

Simultaneously, my STS research explores the morality of the cypherpunk movement, which opposes corporate and governmental overreach by promoting the use of cryptography and privacy-enhancing tools (Anderson, 2023). The ethical ramifications of digital privacy will be discussed, especially as they relate to regulatory initiatives meant to stop illegal activity funded by anonymous cryptocurrency. The STS research focuses on the moral and ethical issues in defending private rights while combating cybercrime, whereas the technical project stresses regulatory frameworks.

Together, these research directions provide an exploration of how privacy and security can coexist in cryptocurrency technologies, ultimately contributing to a safer, ethically grounded digital market.

Enhancing Cryptocurrency Regulation and Security

The novelty of cryptocurrencies lies in their peer-to-peer, decentralized architecture, which permits financial transactions to take place only between people and without the supervision of a conventional bank or middleman. It is these novelties that are actually cited in the whitepapers of many different coins, making them a founding principle of crypto as a whole. These advantages are offset, though, by their own principles, an inherent anonymity that makes cryptocurrencies extremely vulnerable to abuse. Cryptocurrencies are common in illegal markets due to the lack of a standardized regulatory environment and difficulty to trace, especially in areas with uneven enforcement. Canada and Switzerland, for example, have created legislative frameworks that try to strike a compromise between security and individual freedom (Gesley, 2022). Motivated by these instances, my study suggests a thorough strategy for improving bitcoin security via blockchain research and governmental oversight.

One central issue is the traceability of transactions on the blockchain. Blockchain technology was first thought to provide true anonymity, but as Greenberg (2022) shows, it can still enable law enforcement to monitor illegal transactions with advanced analysis tools. Greenberg offers case studies in Tracers in the Dark, where law enforcement agencies utilized blockchain research to find criminal networks such as the Silk Road. This suggests that although transactions can be linked to specific individuals, finding the person responsible eventually requires sophisticated and efficient tools. In order to improve the transparency of financial transactions, this project will investigate cutting-edge blockchain analytics that may facilitate adherence to Know Your Customer and anti-money laundering regulations.

Furthermore, I will look into regulatory frameworks that allow blockchain tracing in the case of harmful use without impeding innovation or violating people's rights to decentralized transactions. For instance, FINMA's rules and Switzerland's Distributed Ledger Technology (DLT) Act encourage bitcoin development while ensuring safety. According to these rules, cryptocurrency brokers must track transaction thresholds and identify participants engaged (Gesley, 2022). These frameworks will be the basis for the suggested regulatory actions in this project, which permit transparency without compromising user freedom. This study will assess how uniform global regulatory regulations might foster a more secure cryptocurrency ecosystem by examining various regulatory strategies.

Finally, there is the problem of fixing blockchain splits and forks. Gray's (2023) research on addressing these technical problems sheds light on how stable bitcoin systems will be after a fork. Gray illustrates how features like Ethereum's "uncle blocks" help create a more robust blockchain by looking at a number of cryptocurrencies, including Ethereum and Bitcoin (Gray, 2023). In order to ensure that security improvements do not jeopardize decentralization, this study will take Gray's results into account and provide methods for preserving system integrity during blockchain splits.

Ethics and Privacy in the Cypherpunk Movement

Digital ethics have been greatly impacted by the cypherpunk movement, an ideology that promotes digital anonymity, especially in areas like cryptocurrencies. This STS study will investigate how the cypherpunk movement might prevent cryptocurrency abuses without compromising its privacy ideals. As monitoring capabilities increase, protecting privacy has become increasingly important. In Cypherpunk Ethics, Anderson (2023) makes the case that cryptographic methods can protect individual liberties against governmental monitoring, a problem that is becoming more urgent as financial institutions implement digital surveillance techniques.

This study aims to investigate two primary ethical dilemmas: how to balance privacy and transparency, and how additional regulation might impact individual freedoms. According to Anderson (2023), cypherpunk ethics encourages institutional openness for the powerful while endorsing the use of cryptographic techniques to thwart surveillance. According to this theory, people should still have the right to privacy, but institutions should be held to a higher standard. The study will look at how this kind of thinking might be used in regulatory frameworks that protect people's rights while preventing cryptocurrency abuse.

The historical and philosophical analysis of regulatory processes will be a crucial component of this study. According to Haynes and Yeoh (2024), various regulatory strategies across nations leave holes that bad actors take advantage of, thus permitting regulatory arbitrage. The project will examine how cypherpunk ideas could influence regulatory frameworks that strike a compromise between privacy and supervision, protecting the core liberties of cryptocurrencies.

Case studies on regulatory procedures and historical instances from the cypherpunk movement will serve as evidence for this examination. In order to investigate how privacy and transparency principles are handled in various regulatory contexts, I will gather information on current international frameworks, such as the EU's Anti-Money Laundering Directives and Japan's

Payment Services Act (Gesley, 2022). In order to suggest rules that respect cypherpunk ideals, this study will also analyze data from regulatory policies that affect user privacy.

Conclusion

Enhancing bitcoin security while upholding privacy rights is a challenge that both the technical and STS research components seek to address. The technology project will enable decentralized architecture and provide methods to monitor and reduce unlawful transactions. The STS analysis will support a privacy-respecting regulatory strategy by offering an ethical framework based on cypherpunk ideas. When combined, these initiatives will improve the technological and moral integrity of the bitcoin industry while also fostering a safe and equitable environment.

References:

- Marizah Minhat. (2024). *Cryptocurrency risk and governance challenges*. Routledge.
- ANDERSON, P. D. (2024). *Cypherpunk Ethics: Radical ethics for the Digital age*. ROUTLEDGE.
- Greenberg, A. (2024). *Tracers in the dark: The global hunt for the Crime Lords of Cryptocurrency*. Vintage Books, a division of Penguin Random House LLC.

- Chowdhury, N. (2020). *Inside blockchain, Bitcoin, and cryptocurrencies*. CRC Press, Taylor & Francis Group.
- Hollebrandse, J. (2022). Crime Is the Driving Factor of Cryptocurrency Adoption. Charlottesville, VA: University of Virginia, School of Engineering and Applied Science, BS (Bachelor of Science), 2022. Retrieved from https://doi.org/10.18130/za7z-ap60

- Gray, D. (2022). CRYPTOCURRENCY: RESOLVING SPLITS and FORKS on the BLOCKCHAIN;CAN WE MAKE CRYPTOCURRENCY SAFER WITHOUT HURTING IT?. Charlottesville, VA: University of Virginia, School of Engineering and Applied Science, BS (Bachelor of Science), 2022. Retrieved from https://doi.org/10.18130/9w05-4x16
- Gesley, J. (2019). Switzerland: Cryptocurrency Regulation Updates. Washington, D.C.: The Law Library of Congress, Global Legal Research Directorate.
- Haynes, A., & Yeoh, P. S. (2020). Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues. Abingdon, Oxon: Informa Law from Routledge.
- Team, C. (2024, February 29). *2024 crypto crime trends from chainalysis*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
- Homeland Security, U. D. of. (2022). Combatting illicit activity utilizing financial technologies ... https://www.dhs.gov/sites/default/files/2022-09/Combatting Illicit Activity .pdf