Decentralization vs. Security: The Ethical Dilemma of Cryptocurrency

A Research Paper submitted to the Department of Engineering and Society

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

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Daniel Farmer

Spring 2025

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

Advisor

Pedro A. P. Francisco, Department of Engineering and Society

Introduction

Cryptocurrency has emerged as an alternative to traditional currencies, offering decentralized, peer-to-peer transactions that promise independence from third parties such as banks or governments. Advocates of the cypherpunk movement, which promotes digital anonymity, have praised cryptocurrencies for their ability to sidestep government and bank overreach (Anderson 2024). However, the same anonymity that empowers these cypherpunks has also been exploited for illegal activities. In 2024 alone, at least $40.9 billion was received by illicit crypto addresses linked to cybercrime, including hacking, extortion, human trafficking, and financial scams (Team 2024). As a result, ongoing debates about cryptocurrency regulation have gained traction as consumers debate whether ethical responsibilities to deter crypto-related crime exist.

Governments worldwide are grappling with how to regulate cryptocurrencies. A major goal is to curb cybercrime without compromising the core principles of decentralization and anonymity. Some countries, such as Switzerland, have implemented regulatory frameworks that attempt to deter crypto-related crime by increasing financial security (Gesley 2024). The goal of these regulations is to accomplish this without stripping users of their privacy. Meanwhile, developers and blockchain communities face a similar ethical dilemma: Should they introduce proposals to blockchain technology that could limit illegal use, or would this undermine the very principles cryptocurrency was founded on?

This research focuses on two main questions: Do governments and consumers have an ethical obligation to limit crypto's ability to facilitate criminal activity? If so, is it even possible to implement these changes without changing crypto into something inconsistent with decentralization and anonymity? By analyzing global regulatory frameworks, blockchain traceability, and the ethical principles of the cypherpunk movement, this study will explore how privacy and security can coexist in the world of cryptocurrency.

Background and significance

The rise of cryptocurrency has disrupted the nature of traditional finance, which has sparked both concern and excitement among the public. Advocates emphasize the financial autonomy it offers, arguing that it acts as a tool to limit institutional control (Anderson, 2024). On the other hand, critics often point to the risks of anonymous crime made possible by cryptocurrency, as transactions are peer-to-peer and without the oversight of traditional institutions (Greenberg, 2024). This debate is not just about policy but a fundamental question about the future of digital finance and whether ethical responsibilities exist for those who develop and regulate it.

One of the biggest challenges to cryptocurrency's long-term stability is regulatory uncertainty. Financial markets remain vulnerable to fraud and illicit transactions because of a lack of clear and enforceable policy. As Marizah Minhat (2024) explains, "Governance challenges in the cryptocurrency space persist due to the lack of a unified regulatory framework, leading to increased risks of market manipulation and financial crime." Some governments around the world have attempted to implement regulations that improve security without

hindering the innovation of these currencies. However, not all countries have taken these steps, opening the door to arbitrage opportunities in weaker jurisdictions (Hollebrandse, 2022). This effectively limits the ability of regulation to deter cybercrime due to criminals simply moving to weaker jurisdictions.

Despite these concerns, the broader significance behind the adoption of new regulation lies in its potential to infringe upon the fundamental values cryptocurrency has worked to champion: financial privacy and financial sovereignty. Traditional financial institutions operate within strict anti-money-laundering (AML) and know-your-customer (KYC) laws, something cryptocurrencies have challenged by offering anonymous, decentralized transactions (Chowdhury, 2020). This raises a crucial question: Should financial privacy be considered an unalienable right, or does the need for crime prevention outweigh these freedoms? According to a report by Homeland Security (2022), "The rise of decentralized financial technologies has created new avenues for illicit activity, necessitating increased collaboration between governments and private entities to mitigate risks."

At the heart of this question lies the dilemma of ethical responsibility. Governments and developers must decide if it is their duty to curb cryptocurrency's misuse. On top of that, they must decide what lengths they are willing to go to to accomplish this and if they are willing to infringe on any rights in the process. Cryptocurrency traditionalists and cypherpunks will claim that regulation threatens the fundamental essence of decentralization (Anderson, 2024), while others will claim regulation is necessary due to high levels of crime (Team, 2024). This research is significant because it examines both the technical challenges of regulation and the ethical challenges these regulations cause. Understanding this balance is crucial as policymakers and the crypto community look to change the future of digital finance (Haynes & Yeoh, 2020).

Methodology

For this research, I used a qualitative approach that examined ideas from law, ethics, political science, and technology. Cryptocurrency is a very complex issue, so I had to look at it from multiple angles, considering everything from privacy and security to regulation and criminal activity. The goal was to better understand how stakeholders such as governments, developers, law enforcement, or even cypherpunk activists might view these issues surrounding crypto. This allowed me to see if it's possible to balance security and privacy without completely hindering the core principles of decentralization that cryptocurrencies were founded on.

This study had three main parts. First, I looked at cryptocurrency regulations across different countries. Some places, like Switzerland, Japan, and the EU, have attempted to enact changes that balance privacy and financial security. According to Gesley (2019), Switzerland has developed a progressive regulatory framework that integrates cryptocurrencies into existing financial laws while maintaining an environment that promotes innovation. By comparing these regulations, I was able to see if they successfully lowered crypto-related crime rates without detracting from a user's privacy and anonymity.

Second, I examined blockchain traceability, which refers to the tracing of crypto transactions back to the identity of those involved. Law enforcement agencies and companies

like Chainalysis use analysis tools to follow illegal crypto activity through the blockchain (Team, 2024). But these tools also raise concerns about privacy and government overreach. As Greenberg (2024) documents in "Tracers in the Dark," authorities have successfully used blockchain analysis to dismantle illicit online markets and criminal enterprises, demonstrating its effectiveness. I analyzed how effective they are at stopping crimes while avoiding too much surveillance.

Third, I investigated the ethical aspects of cryptocurrency through the lens of the cypherpunk movement, which strongly influenced Bitcoin's founding principles. Cypherpunks advocate for financial privacy through cryptographic technologies while promoting transparency in governance (Anderson, 2024). This raises an important question: Can these values coexist with crime prevention measures? By analyzing cypherpunk writings and historical examples of privacy activism, I explored whether it is possible to uphold these ideals while addressing cryptocurrency-related crimes.

I used the Social Construction of Technology (SCOT) framework to guide my analysis. SCOT focuses on how societal actions and values influence technology rather than technology existing as an independent force. In the case of cryptocurrency, its development and regulation are influenced by various stakeholders, including developers and users. By using SCOT, I examined how different groups define and negotiate the meaning of cryptocurrency and what attributes they value most.

To gather information, I used a mix of sources, including academic papers, government reports, books on cryptocurrency, blockchain forensics, and cypherpunk ethics. Reports from organizations like Chainalysis (Team, 2024) and the Department of Homeland Security (2022) helped me understand how governments and law enforcement are dealing with crypto-related crime. I also looked at legal documents from countries with cryptocurrency regulations to see how different jurisdictions approach the issue. For example, Switzerland has a regulatory framework that aims to balance privacy and security, integrating AML and KYC measures while still allowing for innovation (Gesley, 2019), serving as a case study in balancing regulation with financial privacy.

Additionally, I examined the role of forks in cryptocurrency development. Forks, which occur when a blockchain splits into two separate chains due to disagreements among the community, are a key concept in implementing new changes in a cryptocurrency. Hard forks, such as Bitcoin Cash’s split from Bitcoin, can reflect serious divisive issues, while soft forks introduce gradual changes (Chowdhury, 2020). By studying notable forks and their impact, I analyzed how the crypto community negotiates ideological arguments. This aspect of the research helped me dive into how cryptocurrencies evolve in response to regulatory pressures and internal debates, providing insights into how cryptocurrencies are continually reshaped by their community's values.

In the end, the goal surrounding this research was to figure out how to balance the founding principles of cryptocurrency, like anonymity and decentralization, with the need to address its propensity for illegal activity. By understanding the trade-offs involved, I was able to

look at how regulations and current blockchain technology could be improved without undermining the core values of crypto. This study provides useful insights into how governments and the crypto community can work together to make the digital financial system safer while still respecting a user's privacy.

Literature Review

Both scholars and policymakers have taken turns analyzing the challenges posed by cryptocurrencies in terms of crime prevention, ethical considerations, and their notorious volatility. This literature review aims to provide an overview of existing takes on these ideas.

Marizah Minhat (2024) discusses the lack of regulatory oversight that has made crypto a target for criminals looking to participate in money laundering, fraud, or other illicit activities. This study discusses the idea of arbitrage and how criminals exploit inconsistencies between countries' policies. Marizah Minhat states that this has led to an ineffective global landscape and highlights how one country's efforts to ramp up regulation might be ineffective in the grand scheme of things.

In contrast, we see the perspective of the cypherpunk movement, which emphasizes the ethical importance of digital privacy and personal protection in online spaces. Anderson (2024) argues that crypto serves as a safeguard against tyrannical government overreach. They argue that these currencies facilitate financial independence and institutional transparency. However, Greenberg (2024) points out that the very tools that ensure anonymity are also being leveraged by government agencies trying to track down criminals. His research demonstrates that blockchain forensics can still be used to trace illicit activities using advanced tracking technologies.

International approaches to crypto regulation can also vary significantly. Switzerland, for example, has implemented innovative frameworks that aim to prevent crime while not inhibiting crypto development (Gesley 2019). Along those same lines, we have seen Japan, and the EU adopt similar regulatory measures such as the Payment Services Act and the Anti-Money Laundering Directives (Hayes & Yeoh, 2020). These efforts, though, have not necessarily been successful. Individuals and businesses will typically just migrate to areas with more relaxed laws to avoid these new regulations.

We also see studies indicate that economic instability has been a driving influence in cryptocurrency adoption. Hollebrandse (2022) discusses that nations with volatile economies like Venezuela and Nigeria have seen an increase in crypto adoption due to the unreliability of the national currency and a rise in inflation. This raises ethical concerns, as increased adoption of these currencies will often coincide with higher rates of financial crimes like tax evasion.

Lastly, David Gray (2022) examines blockchain governance and protocols, particularly forks and their impact on how blockchains would adapt to new regulations. His work proposes the idea that crypto can be made safer through new governance mechanisms but acknowledges how difficult it is to implement these changes in a decentralized system that requires consensus among stakeholders.

Overall, these studies indicate the growing tension between maintaining privacy, ensuring financial security, and creating and then enforcing regulations. This research aims to build upon these studies to assess whether ethical obligations exist to curb illicit crypto activities. Additionally, this research aims to discuss whether regulatory measures can even be implemented without undermining the fundamental values of cryptocurrency, like decentralization and anonymity.

Results and Discussion

This research sought to answer two key questions: Do governments and cryptocurrency users have an ethical obligation to limit crypto's role in criminal activity? If so, can such measures be implemented without undermining the core values of decentralization and anonymity? The findings indicate that though these obligations do exist, the feasibility of implementing regulations without compromising core cryptocurrency principles is highly challenging and contested. By analyzing global regulatory frameworks, blockchain traceability, and ethical considerations, several key insights have emerged.

First, studies of international regulations reveal that stronger oversight can deter cryptocurrency-related crime or limit the use of cryptocurrency to fuel illicit transactions. Switzerland's model provides a balanced approach that doesn't stop blockchain-based businesses from thriving.

Another finding is that blockchain traceability tools are instrumental in law enforcement's efforts to combat cybercrime, which should make their development a priority for regulatory bodies. As Greenberg (2024) demonstrates, forensic techniques can be used on the blockchain to track transactions that are linked to illegal activity. However, this surveillance can raise ethical concerns regarding individual privacy and potential government overreach.

Third, the cypherpunk movement continues to push back against regulations that might infringe upon financial privacy. Anderson (2024) argues cryptocurrency plays a crucial role in countering institutional corruption and ensuring personal financial freedom. The ethical debate thus comes down to whether privacy rights should be prioritized over new regulations, which many in the community believe that decentralization and anonymity must remain at the forefront of cryptocurrency.

Some major challenges in the battle to push forth new regulations are forks and consensus among stakeholders. As Gray (2022) argues, implementing security-enhancing measures would require a broad consensus among stakeholders which is very difficult to achieve in a massive decentralized system. This ongoing struggle between security and anonymity emphasizes the ongoing division in the crypto community and the massive challenge new regulations represent.

Overall, ethical obligations exist for governments and developers to prevent crime, but practical solutions are riddled with technological and ideological challenges. Governments, blockchain developers, and regulatory bodies must work collaboratively to find middle-ground

solutions that will enhance security and deter crime without eroding the fundamental values of cryptocurrency.

Conclusion

The intersection of privacy and regulation in the cryptocurrency space represents a complex ethical and technical issue. This research highlights that while there is certainly a need to address cryptocurrency-related and cryptocurrency-funded crimes, finding regulatory solutions that don't undermine the core values of these currencies is an unsolved problem.

Studies suggest that while regulatory frameworks can combat illegal activity, enforcement remains a hurdle due to arbitrage opportunities in differing jurisdictions. Blockchain forensic technology has shown promise in tracking activity, but these tools raise concerns as some worry they will lead to governments infringing on one's personal privacy. The cypherpunk movement continues to advocate for the use and adoption of cryptocurrencies, reinforcing the ideological divide between those who advocate for privacy and regulatory agencies.

Ultimately, the balance between privacy and security in crypto regulation requires both ongoing dialogue and technological innovation in the blockchain forensics space. Future research should explore how blockchain governance models can effectively deter crime without dismantling the core ideas of decentralization. Policymakers and the crypto community must collaborate to ensure that regulatory approaches evolve in a manner respecting both financial security and personal freedoms.

References

Anderson, P. D. (2024). *Cypherpunk ethics: Radical ethics for the digital age*. Routledge.

Berentsen, A., & Schär, F. (2019). Stablecoins: The quest for a low-volatility cryptocurrency. In *The economics of fintech and digital currencies* (pp. 65–75).

Bijker, W. E. (2007). American and Dutch coastal engineering: Differences in risk conception and differences in technological culture. *Social Studies of Science, 37*(1), 143–151.

Buchholz, K., & Richter, F. (2021, March 17). How common is crypto? *Statista Infographics*. https://www.statista.com/chart/18345/crypto-currency-adoption/

Chowdhury, N. (2020). *Inside blockchain, Bitcoin, and cryptocurrencies*. CRC Press.
Dat, T. (2020, March 11). Inflation rate rides on outbreak eventualities. *Vietnam Investment Review*. https://vir.com.vn/2020-inflationrate-rides-on-outbreak-eventualities-74558.html

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a

complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control*.

Gesley, J. (2019). *Switzerland: Cryptocurrency regulation updates*. The Law Library of Congress, Global Legal Research Directorate.

Greenberg, A. (2024). *Tracers in the dark: The global hunt for the crime lords of cryptocurrency*. Vintage Books.

Haynes, A., & Yeoh, P. S. (2020). *Cryptocurrencies and cryptoassets: Regulatory and legal issues*. Informa Law from Routledge.

Hollebrandse, J. (2022). *Crime is the driving factor of cryptocurrency adoption* (Bachelor's thesis, University of Virginia). https://doi.org/10.18130/za7z-ap60

Minhat, M. (2024). *Cryptocurrency risk and governance challenges*. Routledge.

Team, C. (2024, February 29). *2024 crypto crime trends from Chainalysis*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

U.S. Department of Homeland Security. (2022). *Combatting illicit activity utilizing financial technologies*. https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity.pdf