UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

CORSO DI LAUREA MAGISTRALE IN ENTREPENEURSHIP AND INNOVATION

TESI DI LAUREA

"PREVENTING CRIMINAL ACTIVITY WITH CRYPTOCURRENCY"

RELATORE: PROF. MARCO GHITTI

LAUREANDO: STEFAN KLJAJIĆ

MATRICOLA N. 2081214

ANNO ACCADEMICO 2023 – 2024

Abstract

Cryptocurrencies have transformed finance, enabling decentralized, anonymous transactions without banks. While reducing transaction costs and enhancing accessibility, they have also been misused for criminal purposes. This thesis examines blockchain's key features—decentralization and anonymity—and cryptocurrency's evolution from niche digital assets to mainstream tools, alongside regional regulations and financial crime involvement.

Focusing on cryptocurrency's role in crime, this research explores how the secrecy of coins like Bitcoin and Monero supports money laundering, terrorism financing, fraud, drug trafficking, and ransomware. High-profile case studies reveal challenges in tracking transactions and linking addresses to identities. International policies, national approaches, and collaborations are reviewed, highlighting regulatory inconsistencies and law enforcement's role in prosecuting cryptocurrency crimes.

The thesis also explores technological solutions, including blockchain-based Know Your Customer (KYC), Anti-Money Laundering (AML) measures, and machine learning to detect suspicious activities. It addresses the tension between preventing crime and maintaining privacy within cryptocurrency. Finally, future trends, such as Central Bank Digital Currencies (CBDCs) and blockchain innovations, are examined for their potential role in crime prevention and regulatory support. This research emphasizes the need for effective policies to balance cryptocurrency's promise with crime prevention efforts.

Acknowledgements

I would like to express my deepest gratitude to everyone who has been part of my life over the past two years. You have made this journey unforgettable, and I am profoundly thankful.

Special thanks go to my professors at the University of Padua, especially Professor Marco Ghitti, for suggesting the idea for this paper and for offering invaluable guidance throughout the process. You have turned cryptocurrencies into more than just a hobby, and I truly appreciate that.

Finally, my deepest gratitude goes to my mother, Vesna, my brother, Jovan, and my late father, Ratko. Mom, your unwavering love and support have made everything possible. Jovan, you have been by my side in my toughest moments, and I am lucky to have you as my brother. To my dad, Ratko, although you are no longer with us physically, your spirit and presence are felt in every moment of our lives. This is dedicated to you.

APPENDICE

Dichiarazione di autenticità [da inserire, dopo il frontespizio, nella prima pagina della Tesi di laurea o di laurea magistrale]

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) .....

Table of Contents

Table of Figures

Chapter 1: Introduction

1.1. Background and Context

Cryptocurrency is a digital currency that uses cryptography to secure, regulate, and verify transactions. Bitcoin is the primary and most well-known cryptocurrency, fully decentralized and peer-to-peer, requiring no mediation from banks or financial intermediaries. Transactions happen directly between the e-wallets. Decentralization has fueled cryptocurrency's rise by increasing efficiency and transparency, thus encouraging widespread adoption. These characteristics have, however, made them an attractive target for misuse. Bitcoin's rising market value has paralleled a surge in criminal activity involving its use (Walker, 2024).

While it can be used to facilitate crime, cryptocurrency also possesses many positive attributes and holds much potential for legitimate users. Properly utilized, digital currencies have the potential to overshadow the criminal activities associated with them. One of the distinguishing features of the virtual currency marketplace is its accessibility, characterized by low barriers to entry. This enables individuals experiencing constraints in national markets or platforms to pursue options and actively engage in this sphere. Unlike PayPal and Revolut, centralized platforms that place limits based on where one lives, exchanges like Binance require only a debit card and identification verification to join in. These systems will also provide true peer-to-peer money transfer with no middlemen, giving global citizens the ability to preserve the value of their assets whenever markets might drop or during governmental unrest.

Bitcoin has been the main cryptocurrency used for performing illicit activities. However, multiple privacy coins have emerged as the "successors" of Bitcoin. Among privacy coins, Monero stands out for its strong encryption, while Zcash allows users to choose whether their transactions are transparent (Almaqbleh et al., 2023). That is exactly why these coins exist – to hide the identity of those who do not wish to be seen or tracked.

As privacy coins gain popularity, countries around the world are trying out various approaches to prevent illicit activities. On the other side, to protect themselves from hyperinflation, citizens of Argentina and Venezuela have rapidly adopted cryptocurrencies, while also struggling to combat money laundering because of weak regulatory frameworks.

Regulating the cryptocurrency market remains a challenge as long as these currencies exist. To be able to regulate them, a perfect balance between anonymity and security needs to be found, as well as international cooperation and well-enforced systems by government bodies and agencies. Over-regulation and extensive surveillance could hinder the innovation on the blockchain, while the lack of it will just ensure that the criminal activities are conducted without much hassle.

This paper examines the ethical dilemma of whether privacy should be sacrificed to prevent illicit activities, questions the role of privacy coins, and explores the future of cryptocurrency. It will give an overview of the already existing literature on these topics and try to give an answer to these questions.

1.2. Research Problem

The primary challenge facing the cryptocurrency market is its dual nature. As mentioned previously, the features like anonymity and directness that cryptocurrencies offer can also be exploited to perform criminal activities. A key issue is balancing regulation with the fundamental features of cryptocurrency—anonymity and security—which risk being compromised. Finding a balance between privacy and transparency is essential for the cryptocurrency market to reach its potential without stifling innovation. Traditional Know Your Customer (KYC) and Anti-Money Laundering (AML) measures are challenging to implement in decentralized systems, highlighting the need for new technologies and regulatory approaches. If there is not a set structure in place, illicit actors will always be able to exploit the existing system.

Inconsistent global cryptocurrency regulations remain a major issue. While some countries like the United States and EU members have AML and KYC regulations in place, there is a ban in China on cryptocurrencies and government bodies of Argentina and Venezuela have no regulatory systems in place. These conditions enable criminals to 'get lost in the system,' bypassing weak control barriers to conduct illicit activities.

Cryptocurrency market keeps growing every year, and along with it the attention of regulatory bodies and government agencies towards it. However, significant gaps remain in understanding how to combat these activities without stifling innovation and losing features that make cryptocurrency attractive in the first place. Most existing literature focuses on Western markets, particularly the European Union and the United States, with limited attention on regions with

weaker regulatory systems. There is little or no mention of Asian, African and Australian markets. The lack of research in these regions creates a blind spot in creating a big picture, where weak or non-existent regulators can be taken advantage of by criminals, allowing them to operate in relative impunity. There is also limited research on the potential roles of emerging technologies, such as Artificial Intelligence and Blockchain forensics, in combating cryptocurrency-related crime.

As the market grows, the rate of criminal activity on the market will also grow exponentially with it. This research provides a comprehensive analysis of regulatory frameworks and explores potential solutions for combating cryptocurrency misuse.

1.3. Objectives of the Study

This study aims to examine the history of criminal activity in cryptocurrency markets and to explore regulatory approaches that prevent crime while preserving the features that make cryptocurrencies unique and beneficial to legitimate users. The goal is to balance blockchain innovation with crime prevention, addressing offenses ranging from small-scale tax evasion to large-scale terrorism financing.

The objectives that this study aims to achieve are as follows:

- To examine existing literature on the effectiveness of government regulations, including AML and KYC measures, in preventing illicit activities within cryptocurrency markets.
- To uncover how cryptocurrencies facilitate criminal activities such as tax evasion, money laundering, ransomware, drug trafficking, darknet transactions, phishing, and terrorism financing. This also includes the overview of case studies such as the CHAT coin pump-and-dump, Sri Lanka Easter Bombing and the Pawn Storm attack.
- To analyze the role of privacy coins (Monero, Dash, Zcash) in illicit activities, assess regulatory approaches, and evaluate their potential future in the market.
- To investigate emerging technologies, particularly AI, machine learning, and blockchain forensics, in detecting criminal activity while safeguarding user privacy.
- To explore global regulatory gaps, demonstrating how criminals bypass and exploit weaknesses in existing systems.

- To propose solutions grounded in existing literature.

Each objective aims to clarify the challenges surrounding cryptocurrency. This study will examine case studies and data from existing literature, exploring practical technological, ethical, and regulatory solutions presented in reputable journals to deter criminal misuse and promote the intended, legitimate use of cryptocurrencies Achieving these goals is crucial for a future where the cryptocurrency market balances innovation, regulation, and privacy, rather than serving as a haven for criminal actors.

1.4. Research Questions

This study poses key questions addressing identified gaps and challenges, aiming to explore cryptocurrency's role in crime, the effectiveness of current regulations, and potential solutions.

Questions:

- How effective are current regulatory systems in preventing the use of cryptocurrencies for criminal activities?
- Why are cryptocurrencies, particularly privacy coins, attractive for illicit activities, and how do their features facilitate crime?
- How can emerging technologies like AI, ML, and blockchain forensics be regulated to balance crime prevention and user privacy?

These questions target the critical intersections between cryptocurrency crime and regulatory systems. Together, the answers aim to form practical solutions to reduce criminal activity in the cryptocurrency market and encourage legitimate usage.

1.5. Significance of the Study

With the rapid rise of cryptocurrencies over the past decade and their widespread adoption as value holders, criminal activity and misuse have naturally followed. This study will build on existing

literature by addressing gaps in areas where KYC and AML are implemented, as well as in regions lacking established laws and regulations. Additionally, it will examine privacy coins' role in criminal activity, explore proper uses, and consider regulatory alternatives to banning them. Proper use includes employing AI and ML technologies to identify criminal actors without compromising the data of legitimate users.

The practical implications are also significant. The study aims to serve as a comprehensive overview of criminal activity in cryptocurrency markets, drawing on papers from highly regarded journals. This paper will hold valuable information on tracking and preventing crime for regulatory bodies while also looking at how individual privacy rights should be upheld. On a broader level, this study aims to guide authorities in identifying criminal methods and balancing regulations to enhance cryptocurrency security across borders. This would help prevent exploitation of borders and systems to perform illicit activities without consequences. The long-term societal benefits lie in a system that is secure, well-regulated, and advantageous for both individuals and governments.

1.6. Structure of the Thesis

The following chapters systematically address the research problem, review existing literature, and propose solutions for the criminal misuse of cryptocurrencies and potential regulatory changes. Each of the chapters follows the overall objective of the study and breaks down the most important concepts in the area it explores.

Chapter 1: Introduction

This chapter introduces the research problem, outlines the study objectives, and discusses its significance. It establishes the study’s purpose, identifies challenges and gaps, and highlights potential solutions for issues in the cryptocurrency market.

Chapter 2: Understanding Cryptocurrency

This chapter introduces cryptocurrency, covering popular coins, key features, uses, misuses, and their history. It will also take a brief look at their legal status, regulations and laws in different regions to better understand what about these virtual currencies enables criminal activity

Chapter 3: Cryptocurrency and Criminal Activity

This chapter examines how cryptocurrencies are exploited for financial gain and illicit activities, including ransomware, money laundering, tax evasion, and terrorism funding. It will also explore case studies, specifically Silk Road shutdown and Sri Lanka Easter Bombing, to show patterns in cryptocurrency use to conduct small- and large-scale criminal activities.

Chapter 4: Methodology

This chapter will provide a detailed explanation of the methods used to approach, collect and analyze the data. Additionally, it will provide an in-depth explanation of the research design.

Chapter 5: Legal and Regulatory Frameworks

This chapter explores various regulatory approaches to cryptocurrency across different countries and regions. It will evaluate the efficiency and effectiveness of existing regulatory systems and challenges faced by policymakers.

Chapter 6: Preventing Criminal Activity Using Cryptocurrency

This chapter discusses the role of AI, ML, and blockchain forensics in regulating cryptocurrency markets, particularly in preventing crime while safeguarding user privacy.

Chapter 7: Central Bank Digital Currency (CBDC)

This part of the research will specifically focus on CBDCs and what role they play in the future of cryptocurrency regulations and crime prevention.

Chapter 8: Conclusion

This final chapter summarizes key findings and presents suggestions and potential solutions from the existing literature for law enforcement.

Chapter 2: Understanding cryptocurrency

2.1. Overview of Cryptocurrency

Cryptocurrency is a digital currency secured through cryptography, allowing ownership and transfers without the need for banks or other intermediaries. Introduced in 2008, Bitcoin was the first cryptocurrency and remains the market leader by capitalization. Since Bitcoin's introduction, the cryptocurrency market has expanded to include other digital currencies like Ethereum, Litecoin, Ripple, and Cardano. Each of these currencies serves distinct functions in the digital economy and relies on blockchain technology, a decentralized ledger of transactions verified by a network of users (Giudici, Milne, and Vinogradov, 2020).

Blockchain functions as an immutable chain of records. Cryptocurrencies use cryptography to confirm ownership through cryptographic keys. This enables blockchain to function without central authority, relying on a proven mechanism to validate and secure transactions, making it tamper-resistant and ensuring transparency and security (Giudici, Milne, and Vinogradov, 2020).

Recent empirical investigations into cryptocurrency markets have garnered significant academic interest, particularly due to the substantial amounts of money involved in these markets. Bitcoin (BTC), Ethereum (ETH), and Ripple (XRP) consistently rank among the top cryptocurrencies by market capitalization (Sapkota and Grobys, 2021).

2.2. Key Features and Evolution

Foley et al. (2019) noted that cryptocurrencies, particularly Bitcoin, have experienced rapid growth in public adoption, leading to increased prices and popularity. By December 2019, over 4,900 cryptocurrencies existed with a total market capitalization exceeding $197 billion, with Bitcoin alone accounting for $131 billion, or 67% of the market (as cited in Sapkota and Grobys, 2021). Easley et al. (2019) estimated that approximately 35 million crypto wallets exist globally, and about 100,000 companies accept Bitcoin as payment (as cited in Sapkota and Grobys, 2021). Hileman and Rausch (2017) found that over 10 million people hold Bitcoin as an investment asset (as cited

in Sapkota and Grobys, 2021). Blockchain technology has evolved significantly since Bitcoin's inception in 2008, with new features, updated regulations, and improved traceability (Koksal, 2019, as cited in Sapkota and Grobys, 2021).

According to Sapkota and Grobys (2021), privacy coins make it harder to track transactions and identify wallet owners, a feature absent in public blockchains like Bitcoin, Ethereum, and Ripple. This is a feature absent in public blockchains like Bitcoin, Ethereum, and Ripple. Despite initial privacy measures, Androulaki et al. (2013, as cited in Sapkota and Grobys, 2021) indicate that with current blockchain technology, every Bitcoin user can be identified to some extent. Goldfeder et al. (2018, as cited in Sapkota and Grobys, 2021) note that third-party web trackers can trace transactions and de-anonymize users.

Privacy coins use advanced cryptography to mask sender and receiver identities and conceal transaction amounts, unlike Bitcoin and other non-privacy coins. This transparency deters institutional and private investors from using Bitcoin as a primary exchange medium, leading many institutions to hesitate in adopting it for transactions (Sapkota and Grobys, 2021).

Baur, Hong, and Lee (2018, as cited in Sapkota and Grobys, 2021) found that Bitcoin is primarily used as an investment, reinforcing that transparency limitations restrict its broader use.

2.3. Legal Status

The regulation of crypto exchanges varies significantly depending on the country. For instance, unregulated exchanges are more liable to be a place for illicit activities because of their lack of Know Your Customer and Anti-Money Laundering protocols. KYC (Know Your Customer) procedures verify customer identities, while AML (Anti-Money Laundering) protocols prevent money laundering through advanced transaction monitoring. As noted previously, exchanges with weak regulations are more likely to allow illegal activities.

Unregulated exchanges often attract users through deceptive methods, offering full anonymity and security during transactions (Aloosh and Li, 2021; Amiram et al., 2021; Cong et al., 2021, as cited in Amiram et al., 2022). Regulators think that manipulation with these methods should be a reason to restrict the growth of cryptocurrency markets and cryptocurrency-linked products. For example, the U.S. Securities and Exchange Commission (SEC) has rejected Bitcoin Exchange-Traded Fund (ETF) applications over concerns about market manipulation. While there is potential to expand

oversight through improved detection methods and regulatory frameworks, standardizing regulations often entails significant costs. In addition, poorly designed or too stringent regulations may discourage innovation processes that are associated with significant welfare losses as well (Amiram et al., 2022).

National strategies vary widely, with some nations implementing favorable regulations to attract cryptocurrency enterprises, while others enforce strict regulations or total prohibitions. Nations such as the United States, Japan, and Germany acknowledge cryptocurrencies as legitimate forms of payment or financial assets, yet concurrently prioritize consumer protection and enforce regulations designed to deter criminal activities. However, some countries, like China, have banned cryptocurrencies for financial transactions and introduced their own central bank digital currency (CBDC). After China banned cryptocurrency due to money laundering concerns, in a year the engagement with cryptocurrencies increased by 231% (Akartuna et al., 2022). International collaborations, like those led by the Financial Action Task Force (FATF), have issued guidelines on cryptocurrency regulation to prevent money laundering and terrorist financing (Amiram et al., 2022).

The European Union, since the outbreak of the war between Russia and Ukraine, put in place regulations to ban large cryptocurrency transactions to Russia. Within the US, regulators started making initial moves to plug the loopholes in the sanctions regime related to digital currencies. The EU's fifth package of sanctions, published on April 8, 2022, prohibits providing accessible crypto-asset wallets, accounts, or custody services to persons, residents, or entities in Russia when the total value exceeds €10,000. The eighth legislative package, which was implemented on October 6, 2022, eliminates the €10,000 threshold, thus enforcing the prohibition irrespective of the monetary value (Alexakis et al., 2024).

Due to strict cryptocurrency policies in Russia, many exchanges relocated to Estonia, which has relatively lenient crypto regulations. That made Estonia one of the popular destinations for virtual asset services that were displaced from Russia. Chatex crypto exchange later came under U.S. sanctions for its involvement with money laundering and darknet marketplaces after the transfer to Estonia. In response, an internationally coordinated regulatory approach was recommended to ensure consistency, reducing the likelihood of criminals exploiting loopholes in less regulated regions (Akartuna et al., 2022).

Chapter 3: Methodology

3.1. Research Design

This is a qualitative study that offers a thorough literature review and specific case studies to analyze the linkage between cryptocurrency and various criminal activities. It examines already published academic materials to determine how cryptocurrencies are being used to facilitate illegal activities, particularly terrorist financing with main focus on the case study of Easter bombing in Sri Lanka.

3.2. Data Sources

The main data source for this study was academic journals rated 4*, 4, or 3* in the 2021 ABS Journal Ranking. Articles were sourced via the Scopus database, setting filters to capture only high-quality academic output relevant to the purpose of this paper about the illicit use of cryptocurrencies.

Particular keywords utilized during the search will be mentioned in the annex of this document. By focusing on these key terms, the research was able to include diverse literature related to the illicit use of cryptocurrencies, hence ensuring that a thorough review of existing knowledge on the subject was covered.

3.3. Case Study Selection

Case studies were selected based on their relevance to academic debate and their relation to cryptocurrency and criminality. Particular focus was placed on high-profile cases, such as the Easter bombing in Sri Lanka, as a means of examining the role that cryptocurrency plays in terrorist financing. These particular case studies have been chosen for their illustrative qualities, offering real examples of how cryptocurrencies are used in nefarious activities, especially in the facilitation of large-scale terrorist activities.

3.4. Central Theme

This study focuses on a broad range of crimes related to cryptocurrency, with a particular emphasis on:

- Terrorist financing
- Money laundering
- Pump-and-dump schemes
- Ransomware
- Tax evasion

The thematic analysis was organized to comprehensively address each of these subjects by drawing on existing literature to investigate the mechanisms through which these offenses are enabled by the pseudo-anonymity and decentralized characteristics of cryptocurrency. Terrorism-related use cases, in particular those related to the funding of the Easter bombing in Sri Lanka, are analyzed in-depth to illustrate in detail the wider ramifications of cryptocurrency on global security. 5. Data Analysis Content analysis was the primary approach to studying the literature collected. Subject matter organized the study, including relevant publications on each type of criminal activity into its corresponding category. This provided a systematic assessment of findings in regard to various types of crimes associated with cryptocurrency. Each article was analyzed to extract implications and trends that explain how cryptocurrencies are used for illegal actions, and the data were thematically coded. The case studies were utilized to contextualize the content analysis and highlight specific examples of cryptocurrencies' use during real criminal incidents. There is also a particular focus on the Easter bombing in Sri Lanka because, being a larger attack, it provides a clearer example of how terrorist organizations can use the anonymity of cryptocurrencies to their advantage in financing.

3.5. Bibliometric Information

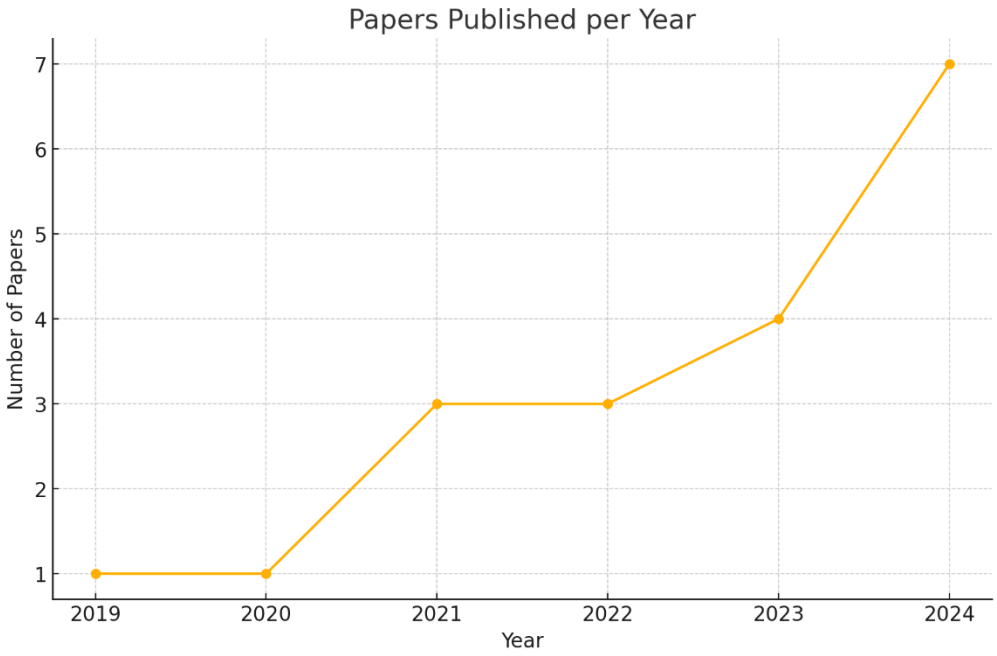


Figure 1—Number of cited papers published in each year

Figure 1 shows the trends in the number of published academic papers relating to cryptocurrency and its involvement in criminal activities between 2019 and 2024. That trend of data clearly shows the steady rise in research output over the years, indicating an increased academic and regulatory interest in the field.

Early studies laid the foundation by exploring the relationship between cryptocurrencies and illicit activities; more recent publications have diversified in focus, covering topics such as regulatory effectiveness and technological advancements to case studies of cryptocurrency use in terrorism financing and money laundering. The peak in 2024 reflects increased interest by researchers in addressing the dynamic challenges presented by cryptocurrencies, now more so under the influence of global geopolitical tension and financial instability that impacts the usage of cryptocurrencies in illegal transactions.

This trend highlights the increasing recognition of cryptocurrency as a financial innovation tool and a potential vector for criminality, thus provoking an extensive examination by scholars coming from multiple disciplines: finance, law, technology, among others. Such analysis of publication

trends puts into perspective the need to address both the regulatory gaps and technological advancements necessary to manage the dual nature of the impact of cryptocurrency on society.

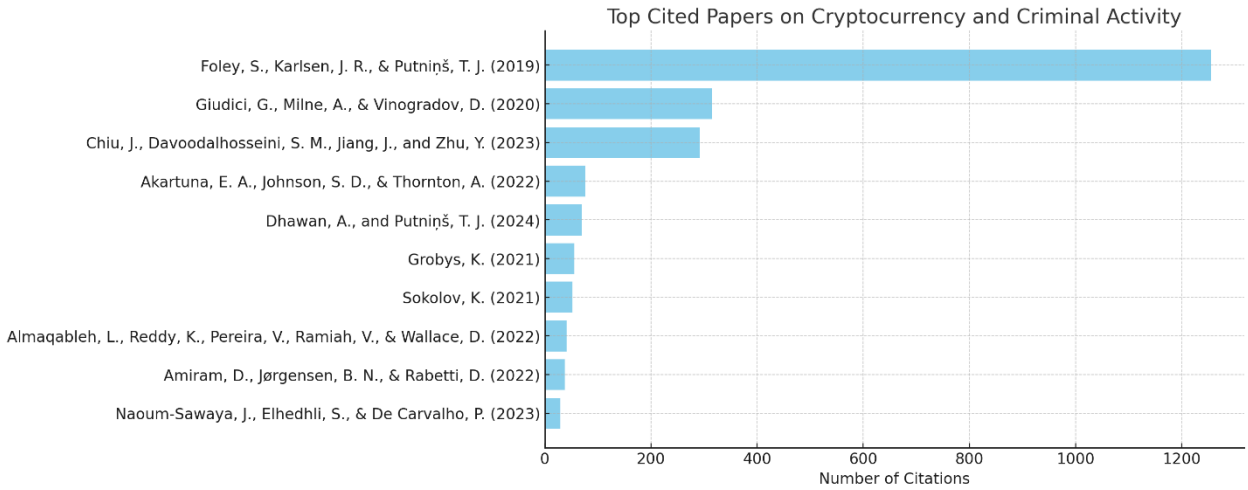


Figure 2—Top Cited Papers on Cryptocurrency and Criminal Activity

Figure 2 shows the ten most-cited papers among the references used in this research. Foley, Karlsen, and Putniņš's (2019) work, with 1253 citations, is the most influential, exploring the extent of illegal activities financed through cryptocurrencies. Following it, Giudici, Milne, and Vinogradov (2020) and Chiu et al. (2023) also have high citation counts, indicating significant contributions to the understanding of cryptocurrency markets and regulatory implications. These highly cited works underscore the foundational role of these studies in shaping the academic discourse on cryptocurrency-related crime and regulation. This analysis shows pivotal studies

providing valuable insights and theoretical frameworks that inform ongoing research in cryptocurrency and its intersection with criminal activities.

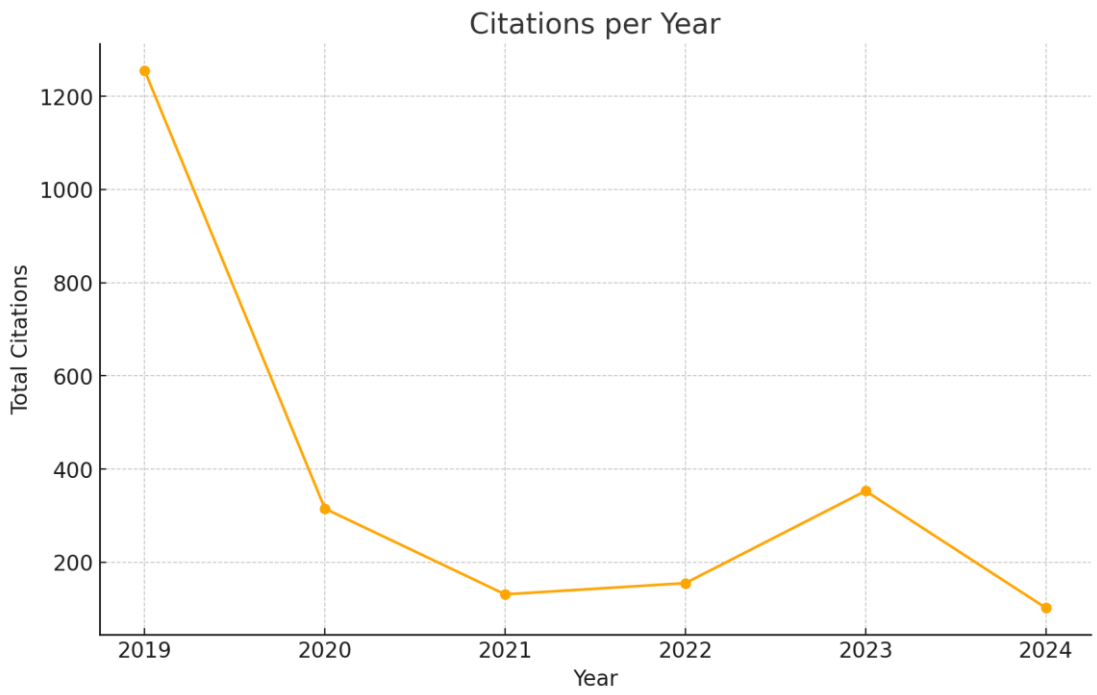


Figure 3—Citations per year

Figure 3 presents the total number of citations per year for research papers referenced in this paper, focusing on cryptocurrency and criminal activity. The sharp peak in 2019 is primarily due to Foley et al.'s highly influential study. The following years show a decline in total citations, with smaller peaks in 2020 and 2023, indicating periodic increases in academic interest as new issues and global events arise.

It's important to note that many of the studies referenced are recent, particularly those from 2022 to 2024. As these studies gain visibility and impact, they are likely to accumulate more citations in the coming years. This pattern suggests a continuing and dynamic interest in understanding and addressing the risks associated with cryptocurrencies in criminal activity, as scholars explore emerging areas like central bank digital currencies (CBDCs), privacy coins, and advancements in regulatory technology. The variability in citation counts underscores the evolving nature of this research field and its relevance in addressing new challenges over time.

Chapter 4: Cryptocurrency and Crime

4.1. Money Laundering and Tax Evasions

Tax evasion associated with cryptocurrency use has raised concerns among governmental bodies, as it reduces overall tax revenue and undermines tax system efficacy. Noteworthy tax deficits attributable to the unregulated characteristics of cryptocurrency markets have been highlighted by the IMF and other relevant organizations. Additionally, the research seeks to examine the effects of cryptocurrencies on tax revenue and to analyze the connection between digital currencies and the capacity of the government to effectively collect taxes (Goel and Mazhar, 2024).

Their hypothesis suggests that increased cryptocurrency use correlates with lower tax collections, as digital transactions are often untraceable and enable more informal, untaxed transactions. Such revenues, in turns, affect the long-term implications of government policy as informal transactions become far more prevalent, and a state is thus less able to collect taxes efficiently (Goel and Mazhar, 2024).

On the other hand, digital payment systems have the potential to reduce tax evasion; this is supported by studies finding a positive impact of better payment systems on fiscal affairs. This paper explores the direct and indirect impacts of cryptocurrency on tax revenues, examining possible channels of influence. The authors consider a panel of over 50 countries to study the impact of cryptocurrencies on tax revenue; they focus on two main questions (Goel and Mazhar, 2024):

- Do cryptocurrencies negatively affect tax collections?
- What are the specific channels through which cryptocurrencies impact tax collections?

The sample showed wide variation in cryptocurrency usage, from over 20% in countries like Nigeria, Vietnam, and Thailand to under 6% in countries like Japan and Sweden. The mediation analysis examined both the direct and indirect effects of cryptocurrency utilization on tax revenue, particularly its relationship with the informal economy and corruption. For instance, cryptocurrencies may have a direct influence on tax revenue by decreasing the traceability of transactions, while also exerting an indirect influence by facilitating corruption or encouraging the

growth of the informal economy. The study is timely, relevant, and responds to the public policy challenge of regulating cryptocurrencies in view of slow growth, high inflation, and aftereffects caused by the COVID-19 pandemic (Goel and Mazhar, 2024).

Goel and Mazhar do the research by considering numerous elements in order not to miss any unforeseen variable that may cause an error in interpreting the effect of cryptocurrencies on revenues collected from taxes.

Larger governments generally generate more tax revenue due to increased expenditure and activity. Fragility, however, inhibits the processes of revenue collection and here refers to instability within either the economic system or the government itself. Economies which are more fragile have low levels of revenues which emanate from the general uncertainty and lack of confidence in the institution. Another measure of the use of cryptocurrencies is indicative of similar results, which would tend to imply that revenues suffer with the use of cryptocurrencies. The relationship is statistically weaker in some of the models evaluating overall revenues that Goel and Mazhar (2024) applied.

Mediation analysis reveals both direct and indirect effects of cryptocurrency use on tax revenue (Goel and Mazhar, 2024):

- Their direct effects are uniformly negative, suggesting that greater use of cryptocurrencies results in lower tax revenues.
- Indirect effects can occasionally be beneficial. For instance, a nation's economic expansion and inflation may serve to enhance tax revenues indirectly; however, an increased adoption rate of cryptocurrencies counteracts this effect.

The research underscores significant policy issues, as cryptocurrencies pose major challenges to effective tax revenue collection. The worldwide and predominantly anonymous characteristics of cryptocurrency hinder the capacity of tax authorities to monitor transactions effectively, resulting in correspondingly low revenue from this sector (Goel and Mazhar, 2024).

The beginning of digital currencies has caused many challenges for tax administrations worldwide and has shaped their methods of collecting revenue and regulatory environment. This research utilizes an extensive global panel dataset to investigate the relationship between cryptocurrency

adoption and tax revenue generation, asserting that a heightened use of digital currency negatively impacts tax collection revenue (Goel and Mazhar, 2024).

The findings strongly support the hypothesis that increased cryptocurrency use decreases tax revenues, with statistical significance across all models. The findings suggest that a 10% rise in the utilization of cryptocurrency leads to:

- A 10% reduction in VAT revenues.
- A 12% reduction in GST revenues.
- A 7% reduction in overall tax revenues.

The results obtained are consistent across various assessments, indicating that the utilization of cryptocurrency presents considerable difficulties for tax authorities and systems of revenue collection. An essential policy implication is that to mitigate the tax revenue losses attributed to cryptocurrencies, it is imperative for governments to adopt a holistic strategy that addresses both direct and indirect influences (Goel and Mazhar, 2024).

Policymakers must monitor trends in cryptocurrency and other digital assets, as these innovations will increasingly impact tax systems in the foreseeable future. Additionally, further research at both national and organizational levels will be required toward the formulation of better policies that are more precise and contextually relevant. One constraint of the research pertains to the possibility of confounding variables, and it is advised that subsequent investigations employing different methodologies be conducted to enhance the causal comprehension of the association between cryptocurrency utilization and tax revenue (Goel and Mazhar, 2024).

Buckley et al. (2024) examine how Criminal Multinational Enterprises (CMNEs) use cryptocurrencies for money laundering. CMNEs have rapidly adapted to new technologies, such as cryptocurrency and blockchain, to conduct illegal transactions and launder money, outpacing regulatory authorities. Blockchain and cryptocurrency provide CMNEs with anonymity and lower transaction costs, allowing them to evade detection, particularly with privacy-focused coins like Monero. In 2020, illicit entities received $4.9 billion in cryptocurrency (Buckley et al., 2024).

Money laundering activity often spikes in the days leading up to major terrorist attacks. In the study conducted by Amiram et al., the wallet activities of the flagged users showed abnormal behavior in the days leading up to the bombing, using money laundering techniques. This further reinforces

the link between money laundering and terrorist financing using Bitcoin. This rise in CAV before the event underlines furthered efforts of money laundering to meet the financial needs of terrorist organizations (Amiram et al., 2022).

A notable criminogenic risk arises from the utilization of decentralized platforms, including cryptocurrency exchanges, by criminals for purposes such as money laundering and financing terrorism (Akartuna et al., 2022). These platforms often lack the rigid regulations characteristic of more conventional financial systems and, as such, allow users to move illegal funds with comparative ease. In 2015, Europol reported that 40% of illegal transactions in Europe involved Bitcoin, highlighting its growing role in financial crime (Akartuna et al., 2022).

Innovations in mobile POS payment solutions and virtual assets promote faster and more hidden transactions, improving the opportunities for money laundering (Akartuna et al., 2022) Cryptocurrencies also increase the geographic dislocation of crimes. After the ban in China on Bitcoin was issued due to concerns over money laundering, cryptocurrency transactions rose 231% (Akartuna et al., 2022).

Anti-money laundering systems, such as those by the Financial Action Task Force, rely heavily on regulatory supervision and 'Know Your Customer' policies. However, these traditional frameworks cannot keep pace with the rapid growth in decentralized technologies and digital currencies, where users are allowed to remain anonymous and obscure the origin of illegal funds (Akartuna et al., 2022).

Establishing Anti-Money Laundering (AML) systems is costly, especially for developing companies, and some argue these systems are ineffective in detecting large volumes of illegal proceeds. Rough estimates suggest that current AML systems detect only 0.1% of global criminal financial activity (Akartuna et al., 2022). This hence brings the need for new approaches like artificial intelligence and machine learning in transaction monitoring. The effect related to AML regulations because of their social and economic impact is nevertheless still debated, as some experts consider that overregulation may impede innovation, especially in the FinTech industry, according to Akartuna et al. (2022).

4.2. Terrorism Financing

Many cryptocurrencies, particularly Bitcoin, are used for terrorist financing due to their pseudo-anonymous nature and global accessibility. This trend poses significant challenges for law enforcement and regulatory bodies attempting to track and trace funds used to finance terrorist operations. The inherent transparency in blockchain technologies offers insights into these operations for the privileged few with the necessary knowledge, thus affording researchers and analysts insights into irregular transaction behaviors that often precede the financing of widespread terrorist activities (Amiram et al., 2022).

The financing of terrorist operations through cryptocurrencies covers the range from weapon and equipment purchases to logistics needs. Money laundering typically involves 'reshuffling' funds across multiple wallets to conceal the origin of the cryptocurrency and reduce traceability. The above-mentioned approaches are notably effective in view of the non-centralized character of cryptocurrencies, devoid of the strict regulations that would normally oversee conventional financial systems.

Unusual transaction volumes, especially around major terrorist events, are key indicators of potential money laundering. Multiple studies have found that extraordinary increases in CAV can be a leading indicator of a pending attack. Examples include cryptocurrency mixers and exchanges with weak requirements regarding Know Your Customer and Anti-Money Laundering regulations to hide their activities. Mixers and exchanges help terrorists launder cryptocurrencies gained illicitly into usable money or obscure the trail before and after an attack. Investigations show that around major terrorist events, suspicious transaction volumes spike, particularly on unregulated exchanges and mixers. This is an environment that is easier to manipulate since it doesn't follow the AML technologies (Amiram et al., 2022).

Money laundering processes are complex, often involving extensive redistribution of cryptocurrency across multiple transactions. Such restructuring increases the apparent level of transactions and diminishes the capability to identify the legitimate transfers from those designed for funding terrorism. For example, in the lead up to most attacks, there is often a spike in transactional activity, which mirrors the need of terrorists to move funds into accessible channels or to transform these funds into usable assets to buy weapons or to pay operatives. Following the event, this size usually shrinks over time because the funds are either entirely laundered or not in active circulation anymore (Amiram et al., 2022).

Terrorists commonly use unregulated cryptocurrency exchanges due to their minimal regulatory oversight. Such exchanges are usually found in those countries which have less rigid financial regulatory mechanisms and, therefore, are not strictly regulated like their regulated counterparts operating in the United States, the United Kingdom, or Japan. It is this lack of regulation that enables terrorists to move a high volume of cryptocurrency through such exchanges with limited fear of detection.

In contrast, regulated exchanges follow KYC and AML regulations, making them less appealing for those seeking to conceal their funding sources. Amiram et al., 2022. The disparity in regulatory frameworks among exchanges is pronounced, with unregulated platforms accounting for a significant proportion of the unusual cryptocurrency activities noted prior to terrorist incidents. Of particular significance is the observation that the demand for money laundering services, notably mixing services, sees a considerable increase prior to attacks, suggesting the expanding involvement of cryptocurrency in these operations (Amiram et al., 2022). Whereas cryptocurrencies make every transaction readable, pinpointing which users are associated with them is very difficult due to the anonymity properties typical in many blockchain models. Advances in blockchain forensics, including co-spend analysis, now enable wallet address mapping and correlation to specific users or entities.

The mapping process allows researchers to trace the flow of money through multiple wallets and services despite users' efforts to remain anonymous. As promising as this sounds, the method is far from ideal, and the overall usage of cryptocurrency is making finding particular activities connected to terrorism more difficult than previously imagined by Amiram et al. (2022).

Amiram et al. (2022) suggest that cumulative abnormal volume (CAV) could serve as an early warning system for detecting terrorist financing. The monitoring of bitcoin transactions shall be done through the identification of sudden spikes in volume, probably showing an impending attack. The research indicated that, ahead of such events as bombings or mass shootings, transaction volume through exchanges and mixers increases significantly in the days preceding, to hint at the notion that terrorists are possibly laundering money or preparing funds to be utilized in the attack. These atypical surges in trading activity are frequently succeeded by a reduction in trading volume subsequent to the event, suggesting that the financial transactions were explicitly associated with the attack (Amiram et al., 2022).

In some cases, money laundering continues after attacks, especially to support operatives' families or sustain ongoing operations. These continuous efforts can help law enforcement agencies track

financial funding flows and perhaps block future attacks. Despite these tools, finding the terrorists who finance terrorism using cryptocurrency is complex and resource-intensive problem to solve, Amiram et al., (2022) add. While focused principally on the predictive power of unusual volumes of transactions, the study covers a growing reliance on unregulated exchanges and mixers and hence contributes to the critical gap in global anti-money laundering efforts. The lack of consistent regulations across jurisdictions allows terrorists and other criminals to exploit the cryptocurrency market. (Amiram et al., 2022).

The main factors underlying the use of cryptocurrencies as a terrorist financing vehicle pertain to their decentralized nature, which enables individuals to perform significant cross-border financial transactions with anonymity. However, such features are exploited by terrorist groups in their efforts to bypass the checks imposed through the traditional financial sector institutions, such as banks, where there is stringent implementation of AML and CTF regimes. On the contrary, cryptocurrencies operate outside centralized regulatory mechanisms and thus cannot easily trace monetary transfers between sponsors and recipients when such transactions involve multiple wallets and are interwoven with transactions that are legal (Almaqableh et al., 2022).

Terrorist organizations exploit unique blockchain features, particularly the decentralized and anonymous nature of certain cryptocurrencies, to obscure transactions. The touted transparency of blockchain-the recordation of transactions on a public ledger is often cited as the deterrent to illicit activities. However, terrorists bypass this transparency by using cryptocurrencies that offer enhanced anonymity, such as Monero and Zcash, concealing transaction details and the identity of parties. This level of privacy makes it difficult for any authority to trace this flow of funds, even using advanced blockchain forensic technologies (Almaqableh et al., 2022).

Methods of cryptocurrency use for funding terrorism vary, but donations from supporters and direct monetary transfers between operatives are the most dominant. Some terrorist groups set up cryptocurrency wallets to receive anonymous donations from supporters worldwide. Such donations are often solicited through social media platforms or encrypted messaging apps, where donors are requested to supply cryptocurrency rather than depend on traditional financial infrastructure, which is vulnerable to monitoring by national and international authorities (Almaqableh et al. 2022). The donations are then used to purchase weapons, fund training programs, or provide other forms of logistical support to terrorist activities.

Others convert cryptocurrencies to fiat currency through various exchanges or ATMs, further obscuring the money trail. Conversion of cryptocurrency into cash will enable terrorist groups to

utilize the funds towards the operational expenses since acceptance of crypto is not easy in that region. Their ability to quickly convert digital assets into local currencies without raising suspicions allows them to operate under the radar and, in most cases, until after an attack has been executed. The problem is further compounded by their increasingly widespread access to cryptocurrency ATMs, which are an easy way to convert Bitcoin and other virtual currencies into physical cash anonymously (Almaqableh et al., 2022). While regulators have been trying to introduce AML and CTF policies into the world of cryptocurrencies, the consistency of enforcement remains poor, and the decentralized nature of cryptocurrencies makes thorough oversight all but impossible. The reasons are that, quite often, there is literally no one entity in a position of centralized control responsible for reporting or even monitoring suspicious activities, which puts law enforcement agencies on a very difficult task of tracking terrorist financing.

Terrorist organizations exploit the instability and speculative nature of cryptocurrency markets for financial gain. In this way, by employing price manipulation techniques such as pump-and-dump, fraudsters can inflate the value of their targeted cryptocurrencies for their benefit, sell their holdings, and thus make a profit from their activities using these proceeds, in which they have invested. Noise trading, speculative efforts, and organized market manipulations are some of the explanations usually faulted for the observed price volatility, which has been related to a variety of illegitimate activities, including financing terrorism. The capacity to move markets with modest capital investments gives terrorist organizations a financial advantage in being able to raise money far more effectively than by traditional means of Almaqableh et al. (2022).

Empirical evidence has shown that terrorist activities are financed through the use of cryptocurrencies, but specific examples of these activities will not be touched on in this manuscript, since they will be handled in their own separate section. Events like the financing of ISIL through cryptocurrencies, however, show a growing role of digital currencies in terrorist activities. These examples underscore the urgent need for enhanced regulatory frameworks and advanced technological measures to reduce cryptocurrency misuse in terrorism (Almaqableh et al., 2022).

4.2.1. Case Study — Sri Lanka Easter Bombing

The Sri Lanka Easter bombing on April 21, 2019, serves as a critical case in Amiram et al. (2022) to demonstrate the importance of blockchain analytics in identifying unusual financial behaviors. Substantial Bitcoin transactions that seemed to fit the characteristics of money laundering or terrorist financing were closely followed upon this platform. Using the rolling three-sigma rule, Amiram et al. (2022) identified irregular transfers where transaction values exceeded three standard deviations from a user's historical average. This methodology signaled potentially dubious behavior, assisting in the identification of possible funding sources for the attack.

Amiram et al. (2022) flagged 48 users with at least one anomalous transfer near the time of the bombing. Of those, six were flagged for suspicious behavior that mainly transacted between services, exchanges, and dark markets. The behavior represented the methods practiced by the financiers of terrorism, where large chunks of Bitcoin would be mixed among many wallets so their origin could not be traced. Many of these flagged users had significant balance fluctuations around the time of the bombing, showing likely laundering activity leading up to financing the attack. A significant finding in the study was the activity of a popular cryptocurrency payment gateway. This wallet received an unusually large number of incoming Bitcoin transactions on the day before the bombing that was subsequently followed by an unusually large drop in its balance on the day of the attack (Amiram et al., 2022).

This cryptocurrency wallet had been involved in over a million transactions and had moved some 1.9 million BTC in value. Signs of its usage in criminal activity were very evident since the funds went through this wallet quickly, raising extraordinarily strong suspicions of its use as a means to funnel funds into terrorist activities and potentially marking an important stage in the financing cycle ahead of the planning of an attack. In that period, a significant virtual currency exchange also based in the US participated in the transfers of substantial sums of Bitcoin. Though some of the transactions were related to market activities, many transfers were suspicious given their suspicious timing and connections to mixers and anonymous wallets, according to Amiram et al., 2022. Mixers played a significant role by reorganizing large amounts of Bitcoin to enhance anonymity and obscure the funds' origin.

The study of Amiram et al. in 2022 noted clear evidence of money laundering on the identified wallets and transactions, which is a widely used tactic to camouflage the transfer of funds by terrorist groups.Mixers were identified as a primary tool for terrorists to mask large quantities of

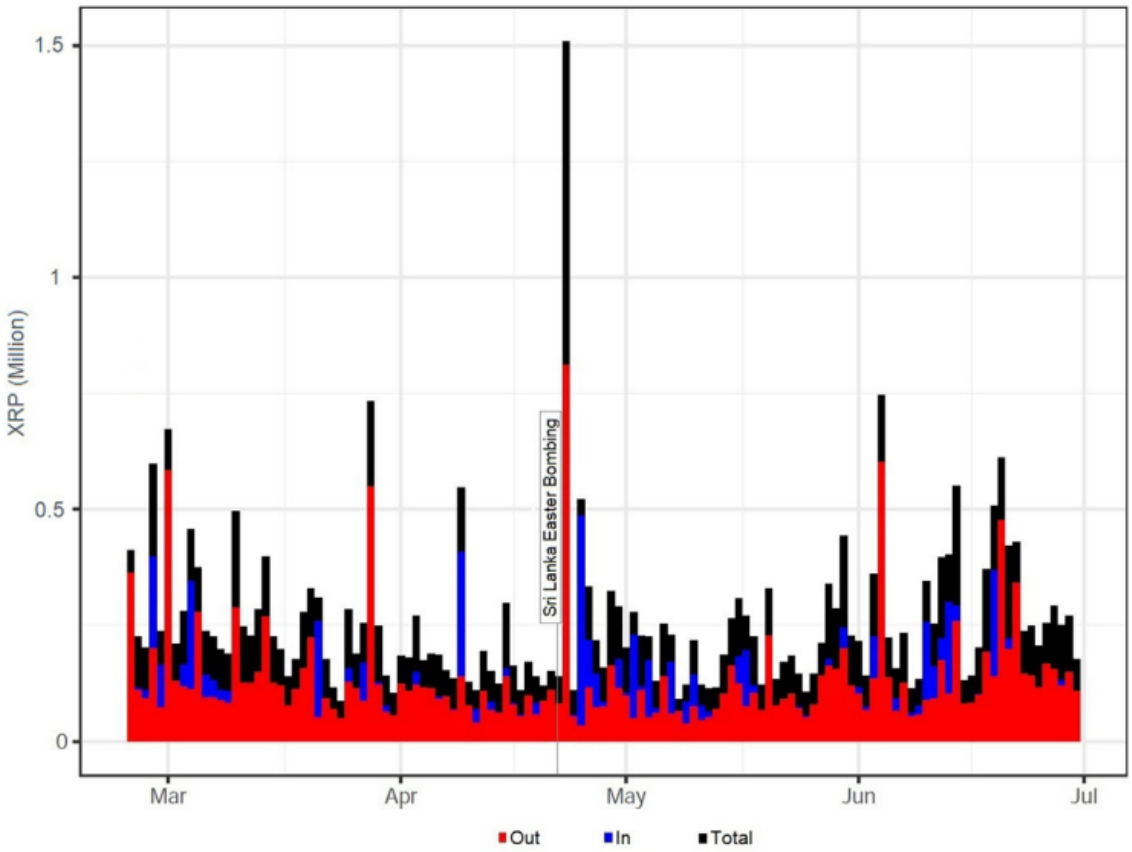
Bitcoin, subsequently distributing it among multiple anonymous wallets. The reshuffling of funds through mixers not only disguised the origin of the money but also allowed smaller transactions, which could avoid raising suspicion more easily.

Among them, the role of cryptocurrency payment gateway was very vital. As Amiram et al. (2022) explain, this wallet allowed several online retailers to receive cryptocurrency payments and immediately converted them into fiat currency while reaping the commissions from each transaction. This wallet's balance spiked with a 400 BTC ($2.8 million) transfer on the day before the bombing. Further forensic analysis linked this wallet to other heinous crimes, such as kidnappings and the financing of jihadist groups in Syria; thus, bolstering the assertion that the wallet was entangled in larger terrorist financing schemes.

Blockchain analytics enabled Amiram et al. (2022) to trace these funds across exchanges and wallets potentially linked to the Sri Lanka bombing. The wallets that were frequently associated with non-regulated exchanges that have little or no Know Your Customer requirements and Anti-Money Laundering programs have been a significant focus of attention upon analysis. It is postulated that these unregulated exchanges are likely participants in allowing such illicit deals, enabling terrorists to eliminate the conventional financial systems and efficiently move large volumes of money safely. The outliers in the three-sigma rule applied in the analysis were picked out by measuring deviations from normal transaction patterns. Amiram et al. (2022) explain that dark market wallets tend to have more frequent anomalies because these wallets typically collect payments before transferring them into fiat currencies. Out of the 48 users that this flagged, many were indeed using the platform for their dark market operations, while a large portion of the remaining users were mixers and exchanges.

Suspicious transactions from various services and exchanges, especially those with large volumes in the days leading up to the bombing, provided additional evidence that such wallets were used to enable terrorist financing. Similarly, the study conducted by Amiram et al. (2022) disclosed that more than 1 million transactions containing about 1.9 million BTC were involved in suspicious activities linked to the Easter bombing in Sri Lanka.

In addition to Bitcoin, Amiram et al. (2022) investigated Ripple (XRP) transactions associated with the Sri Lanka Easter bombing, revealing suspicious XRP wallet activities. One Ripple wallet was identified, in particular, for unusual behavior due to the size and timing of its transactions in the weeks leading up to the attack. This wallet is intricately linked to a cryptocurrency payment gateway that earlier was identified for involvement in suspicious Bitcoin transactions.



Amiram et al. (2022), Figure 4 — Aggregated daily inbound (blue), outbound (red) and total (black) transfers on the Ripple network at the Gateway Ripple wallet (GRW) in 2019. XRP transfers are measured in units. There is one anomalously high transfer of 0.7 million XRP) occurred in the early morning one day after the Sri Lanka Easter bombing.

Between January and April of 2019, the XRP wallet under scrutiny had an average of 133,000 and 153,000 XRP in daily inbound and outbound transactions, respectively (Amiram et al., 2022). On April 23, 2019, an unusually large transfer of 660,000 XRP (about $212,000) was recorded, two days after the Sri Lanka bombing. The huge transaction deviated from the usual volumes of transactions associated with the payment gateway's framework operations and consequently raised concerns about whether it might be financing the attack. Amiram et al. (2022) demonstrated that the transaction activity of the wallet in question had a similar structure to that of a mixer involved in money laundering. Additionally, the timing of this large transfer, together with suspicious Bitcoin transactions from the same exchange, gave further confirmation to the hypothesis of their involvement in financing the bombing. These transfers, like their Bitcoin counterparts, were likely

intended to conceal the source of the funds, thereby complicating any attempt to definitively link them with acts of terrorism.

Further analysis identified three additional XRP wallets linked to money laundering (Amiram et al., 2022). The first wallet acted as a mixer, transferring millions in cryptocurrency. These restructured funds were forwarded to unidentified wallets using the secondary wallet, breaking the transaction sequence and enhancing the anonymity of the beneficiaries. The tertiary wallet acted as a deposit institution with more than $200 million reserves and might have served as a depository for money gained through illegal means. The work by Amiram et al. (2022) on XRP is just an example of how versatile the individuals funding terrorism are in leveraging various cryptocurrencies apart from Bitcoin. Ripple's fast transaction processing and low fees make it an attractive option for discreet, large transfers. This case study highlights the challenges of monitoring illegal activities across various cryptocurrencies in efforts to combat terrorist financing.

4.3. Drug Trafficking

Foley et al. (2019) investigate how cryptocurrencies, particularly Bitcoin, facilitate illicit activities on darknet marketplaces. Their contribution points primarily to how the nature and structure of cryptocurrencies like Bitcoin have changed the nature of illicit drug trafficking worldwide to facilitate traffickers in making anonymous transactions and evading law enforcement agencies.

According to Foley et al. (2019), Bitcoin seems to be the cryptocurrency of choice for illicit use, settling almost 98% of the flows created in darknet markets. These markets resemble legitimate e-commerce platforms like eBay, where vendors sell drugs, and buyers rate purchases to establish trust and quality within an otherwise anonymous and unregulated setting. The authors note that this proliferation of these digital drug markets has brought about an unparalleled increase in international drug trafficking networks.

Unlike traditional trafficking, relying on direct exchanges with the considerable risk of violence, the use of cryptocurrencies has allowed drug traffickers to tap into a broader market while limiting their physical exposure, thus decreasing the overall risk of their business. Foley et al. (2019) highlight Silk Road as a pioneering darknet marketplace where Bitcoin was extensively used for drug trafficking. During the operation of closing SilkRoad, the FBI seized more than $4 million worth of Bitcoin; nevertheless, Foley et al. (2019) claim that with the takedown of Silk Road, a

few of its alternative darknet-based markets were only expanded, without causing any disruption to the trade of illicit drugs. The robustness of illicit drug markets is additionally evident in the authors' finding that illicit activities related to Bitcoin reached their zenith from 2012 to 2016, which coincided with the emergence of these marketplaces.

Foley et al. (2019) estimate that, in April 2017, around 46% of all Bitcoin transactions were illegal and that a significant fraction were related to drug use. Bitcoin use in narcotics markets not only facilitates drug trading but also helps traffickers evade law enforcement. Narcotics traffickers use techniques like “tumbling” or “mixing”, where transaction origins are obscured by pooling funds with others and cycling them through multiple addresses.

These methodologies have increasingly made it impossible for law enforcement agencies to track the flow of money and link it to specific unlawful activities. The study also looks into the response of police to this growing challenge. Operations like “Operation Onymous”, a joint effort by U.S. and European authorities, have identified illegal darknet sites, resulting in numerous seizures and arrests. However, Foley et al. (2019) express that such efforts, albeit great in stature, do no more than temporarily hamper the expansive illicit drug networks operating on such sites. They indicated that following the takedown of key markets, such as Silk Road and AlphaBay, other places quickly emerge to fill in the void left behind to keep the cycle of illicit drugs within the darknet going.

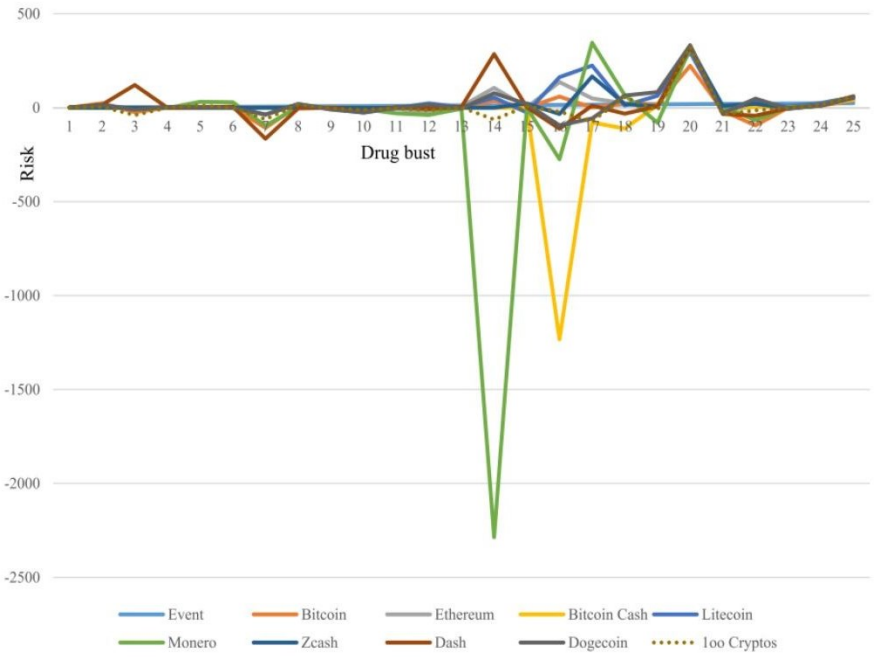
Speaking to the issue of assessing the impact of cryptocurrencies on drug trafficking, Foley et al. (2019) provide some dramatic statistics. Foley et al. (2019) estimate that by 2017, about 27 million Bitcoin users engaged in illegal activities, with 37 million transactions valued at $76 billion, much of it tied to drug trafficking. This statistic illustrates how serious an issue this is and the significant role that cryptocurrencies play in perpetuating international drug trafficking operations. Foley et al. (2019) note, however, that even with law enforcement's best efforts, the cumulative sum of illegal Bitcoin transactions, including those related to drugs, has remained at, or near, all-time highs. The persistence of such illegal conduct, now into a period of relative mainstream acceptance of Bitcoin, demonstrates the resilience of such networks and the challenges regulators face in effective countermeasures against drug trafficking via cryptocurrencies.

Almaqableh et al. (2022) argue that cryptocurrencies have evolved from speculative instruments to essential mechanisms for both legal and illegal exchanges since Bitcoin’s introduction in 2009. Among all the illegal activities, drug trafficking has taken up one of the leading positions due to, among other factors, the partial anonymity given by cryptocurrencies, especially in dark-net marketplaces. Through anonymizing technologies and decentralized frameworks, these online

platforms offer the ability for drug traffickers to be at a lower level of detection when transactions occur. Along with this system, the effective encryption derived by cryptocurrencies such as Monero, Dash, and Zcash makes cryptomarkets an integral part of the global setting when it comes to drug trafficking.

Such a link between drug trafficking and cryptocurrency is also rooted in the ease they provide in transferring illegal funds across borders at minimal cost, while avoiding the scrutiny of conventional financial institutions. According to Almaqableh et al. (2022), the pseudonymity of transactions facilitates a way for criminals to exploit these technologies, hence making cryptocurrencies a top preference for money laundering purposes originating from drug sales. This illicit use does not go without impacting the cryptocurrency market, in which speculation upon news related to drug busts contributes to significant fluctuations in risk and return. In particular, Almaqableh et al. (2022) investigate how seizure reports influence the pricing and volatility of leading cryptocurrencies, considering 24 recent drug seizures and their respective effects on the cryptocurrency market.

They found that drug seizure reports sometimes led to increased cryptocurrency prices due to reduced illegal drug supply. The reduction increased the prices of such drugs, which, in turn, inflated demand for the cryptocurrencies used in buying the drugs. This confirmed hypothesis H1, especially for the more anonymous cryptocurrencies like Monero, Dash, and Zcash. Conversely, the study also captured events where the announcement of drug seizures produced opposite outcomes. Hypothesis H2 explored whether high-profile drug busts could dampen drug demand and reduce cryptocurrency usage in these markets. Evidence supporting this hypothesis was considerably stronger and exhibited significant negative CAR over the 30-, 60-, and 90-day windows following announcements of drug busts. Certain busts, especially those identified as numbers 2, 19, and 20 in this series, revealed stark drops in cryptocurrencies, indicating that law enforcement operations can successfully impede the illicit market and reduce the demand for drug trafficking facilitated by cryptocurrencies.



Almaqableh et al. (2022), Figure 5—Impact of Each Drug Bust on Short-Term Systematic Risk

Further, as we can see in Figure 2, the study examined how news about drug busts affects the systematic risk-as measured by beta-of virtual currencies. Hypothesis H3 proposed that drug bust news reduces virtual currency risk by signaling a decrease in criminal activity. Evidence was then provided by Almaqableh et al. (2022), who, after noting significant declines in most cryptocurrencies' beta values, such as Litecoin, would indicate that police efforts against the drug trade lower perceived market risk. The absence of risk would, therefore, mean the market adjusts its expectations upon knowledge of a reduced crime rate; the responses, however, vary among cryptocurrencies. The study demonstrates that while law enforcement actions against drug trafficking can disrupt illicit exchanges, their impact on cryptocurrency markets is complex. In certain instances, immediate surges in drug prices post-bust may trigger temporary increases in cryptocurrency demand, whereas in other situations, apprehension regarding enforcement measures may reduce this demand, resulting in prolonged declines in prices.

4.4. Ransomware

Ransomware has emerged as a major threat in cyberspace, particularly through its integration with blockchain-based cryptocurrency systems. According to Sokolov (2021), the connection between ransomware and Bitcoin is gradually increasing due to the anonymity and reliability of cryptocurrency. Ransomware attackers exploit vulnerabilities of widely used software, which encrypts vital files on a user's system, rendering them inaccessible until the targeted user pays a ransom in Bitcoin. The need for anonymity has placed blockchain technologies, especially Bitcoin, at the center of ransomware activities.

Ransomware's reliance on Bitcoin is evident in the use of ad hoc Bitcoin addresses created specifically to facilitate ransom payments. Sokolov (2021) categorizes Bitcoin addresses into two types: standard addresses and ad hoc addresses, where only ad hoc addresses have a direct relationship with ransomware.

During ransomware surges, ad hoc addresses see transaction volumes increase by about 3.6%, while regular addresses, typically used for legitimate purposes, decrease their activity by 1.2% to 2.7%. This shift in behavior arises primarily because blockchain congestion is an influential driving factor. Ransomware incidents often develop into increased demand for Bitcoin transactions, thus creating blockchain congestion. During periods of ransomware proliferation, such as that experienced in the 2015 Pawn Storm attack, which exploited a weakness in Adobe Flash Player, regular users reduce their demand for settlement. This shift allows opportunistic users, such as those involved in ransomware activities, to increase their contribution, as seen by Sokolov, 2021. The shift does little to ease the overall congestion, though, which increases between 15% and 27% during the proliferation of ransomware activities. A significant element that intensifies this congestion is the rivalry among users to impose elevated fees on their transactions. With blockchain capacity constrained, especially by Bitcoin's 1 MB block size, users offer higher fees to ensure expedited processing. Individuals affected by ransomware, who typically encounter pressing time constraints to access their encrypted data, are compelled to offer higher bids than competing users, resulting in significant escalations in transaction fees—averaging 2.1% during periods of congestion, with some extreme instances witnessing fee surges of up to 28% (Sokolov, 2021).

While congestion is often seen as friction within the blockchain network, it plays a crucial role in incentivizing miners. Miners receive compensation for the execution of transactions via transaction fees, with increased congestion resulting in elevated fees, which in turn incentivizes miners to

enhance their infrastructure. Nonetheless, as noted by Sokolov (2021), this framework is not without its constraints. Ordinary users, dissuaded by escalating fees, may diminish their engagement with the blockchain, thereby jeopardizing the mining rewards that are largely dependent on fees driven by congestion. While mining rewards in the form of new Bitcoin tokens decrease over time, transaction fees are expected to become the main reward for miners. At the same time, congestion-induced fees alone might not incentivize miners enough, assuming regular users continue to leave the blockchain when fees are high.

A key finding in Sokolov's (2021) research is a strong positive correlation between ransomware incidents and software vulnerability disclosures. Public disclosures of critical vulnerabilities often provoke ransomware attacks as malicious actors incorporate these vulnerabilities into the exploit frameworks. The National Vulnerability Database (NVD), responsible for tracking publicly known cybersecurity threats, provides substantial support in this regard. Once severe vulnerabilities have been disclosed, almost immediate opportunities can arise for cybercriminals to launch ransomware attacks, thus increasing demand for Bitcoin transactions (Sokolov, 2021). The 2015 Pawn Storm attack exemplifies this, where a vulnerability in Adobe Flash Player led to a sharp increase in Bitcoin transactions, followed by a drastic drop once Adobe released an urgent patch.

Furthermore, the study highlights how Bitcoin is indeed vulnerable to disruptions in darknet markets and other illicit activities related to money laundering, contraband trafficking, and even gambling. Anonymizing services like Bitcoin Laundry and Anonymix further obscure ransom payments by routing funds through temporary addresses to mask their origin. A part of the success of ransomware comes from the time constraints that ransomware puts its victims under. Sokolov (2021) notes that ransomware often imposes a payment deadline, after which the ransom may increase, or the files could become permanently inaccessible. This urgency compels victims to act quickly, often during peak congestion, which exacerbates rising transaction costs. Victims often create new Bitcoin addresses to facilitate ransom payments, increasing the overall number of blockchain transactions. Sokolov's (2021) research culminates in an exploration of the wider ramifications of ransomware operations within the blockchain context. While blockchain's decentralization offers anonymity, it also incurs societal costs by enabling unlawful activities. The study underscores the need for a nuanced approach to blockchain regulation, balancing the benefits of anonymity and decentralization with the rising threats posed by cybercrime, especially ransomware.

4.4.1. Case Study — The Pawn Storm attack

According to Sokolov (2021), the Pawn Storm attack exemplifies ransomware activities exploiting vulnerabilities in Adobe Flash Player. The cyber espionage group Pawn Storm launched this attack back in 2015. The effects of the ransomware activities increased after this attack and were reflected in the increased demand for Bitcoin transactions. Soon after the discovery, the vulnerability joined the toolkits of various cybercriminals involved in ransomware campaigns to take advantage of the widespread deployment of Adobe Flash Player in varied systems.

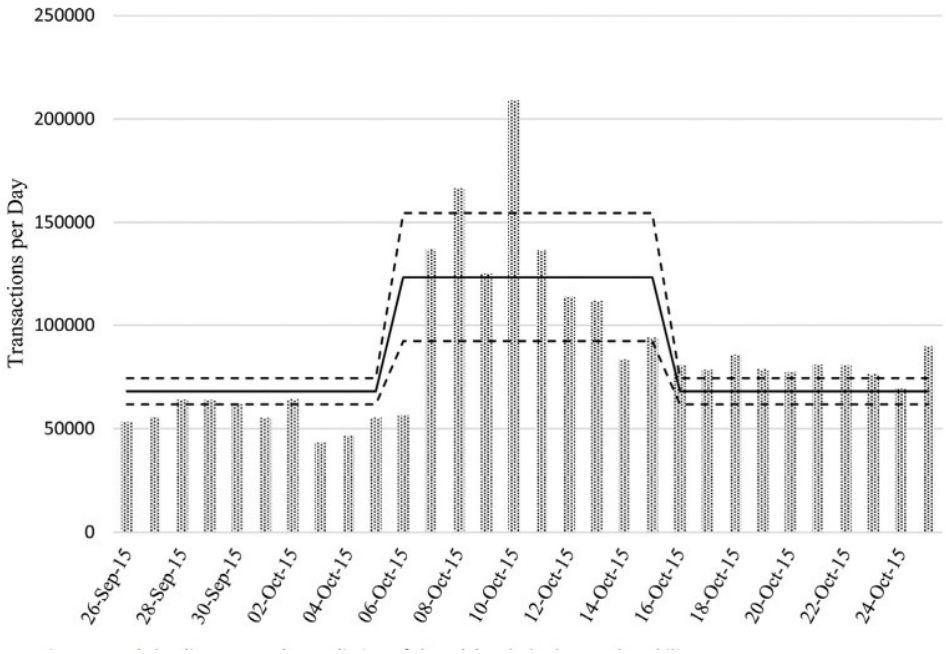
The attack exploited a critical vulnerability in Adobe Flash Player, which scored high on the CVSS scale according to the NVD, indicating potential for severe system compromise (Sokolov, 2021). The aim here was to use this bug to get unauthorized access to systems, encrypt crucial files, and lay ransom demands in Bitcoins. The ransomware used in this attack effectively encrypted victims' data without affecting the system's bootability, giving end users only two options: either pay the ransom or lose all their files.

As the Pawn Storm attack gained momentum, ransomware activities surged, driving a significant increase in Bitcoin transactions as attackers demanded ransom payments in Bitcoin.

During this period, Sokolov (2021) observed a notable increase in transactions linked to ad hoc Bitcoin addresses used to facilitate ransom payments. Specifically, transactions per ad hoc address surged by 3.6 percent, a development that is linked to the need to manage the ransom payments accrued from the large number of victims affected by the incident. Concurrently, standard Bitcoin addresses, which were not explicitly engaged in ransomware transactions, demonstrated a significant decrease in transactional activity. Standard addresses saw transaction volumes decline by 1.2% to 2.7%, as typical users postponed or avoided blockchain use due to rising fees (Sokolov, 2021). This behavior is in line with theoretical predictions made by Easley et al. (2019) that high-frequency users will leave the blockchain when transaction costs rise during high-demand periods.

he Pawn Storm attack intensified Bitcoin blockchain congestion as users competed to prioritize their transactions. Individuals affected by ransomware, confronted with the urgent demands to remit payment and retrieve their data, found themselves compelled to impose increased fees on their transactions to guarantee prompt processing (Sokolov, 2021). Consequently, this situation resulted in a notable escalation in the average transaction fees, with an ordinary ransomware spike during this timeframe corresponding to a 2.1% rise in fees, while particularly severe instances experienced fee increases reaching as high as 28%. The Pawn Storm attack highlighted the

vulnerability of the Bitcoin blockchain to network congestion. According to Sokolov (2021), congestion occurs when unprocessed transaction volume exceeds network throughput. In this case, it was reportedly because of a limit in block size of 1 MB on the Bitcoin blockchain, which only allowed a little more than 1,000 transactions per block.



Sokolov (2021), Figure 6— Bitcoin transactions around the discovery and recovery of the Adobe Flash Player vulnerability

Despite the higher transaction fees paid by users bidding for priority positions in transaction settlement, this did not improve the blockchain's capacity to process more transactions. Rather, it only intensified competition among users, thereby aggravating congestion costs.

The miners, however, benefited from this congestion. TThe surge in transaction fees led to higher mining rewards, as miners received increased compensation for processing transactions during the attack (Sokolov, 2021). This dynamic incentivized miners to invest in their infrastructure, since increased congestion meant greater profitability from the processing of Bitcoin transactions during

an incident of ransomware. The increased mining rewards in this period underlined the blockchain's reliance on fee-based models, wherein congestion acts as a catalyst to incentivize miners to increase the blockchain and ensure reliable settlement.

Subsequent to the identification of the vulnerability in Adobe Flash Player, Adobe promptly released a critical update aimed at alleviating the associated security threat. Following the update, ransomware operations tied to Pawn Storm declined, and Bitcoin transaction demand returned to pre-attack levels (Sokolov, 2021). The fact that transaction volume reduced rapidly following the resolution of the vulnerability further attested that blockchain congestion was a result of ransomware activities, not from other phenomena such as speculative demand or theft of coins.

The event study by Sokolov (2021), conducted for the Pawn Storm attack, supported, on a larger scale, the conclusions of the above analysis on increases in ransomware attacks and congestion within the Bitcoin blockchain. In this attack, ad hoc Bitcoin addresses used solely for the purpose of processing ransom experienced much higher activity while regular addresses unrelated to ransomware reduced their demand for blockchain settlement. This resulted in short but intensive congestion in the Bitcoin network: transaction fees strongly increased and miners benefited from congestion-induced fee competition. This goes to show, according to Sokolov (2021), that the exploitation of software vulnerabilities by cybercriminals can result in blockchain congestion and high surges in transaction fees. This incident highlights the vulnerability of decentralized blockchain systems, such as Bitcoin, to demand surges driven by illicit activities like ransomware. These findings underscore the urgent need for prompt vulnerability patching by software developers, as delays can lead to widespread ransomware attacks and spikes in blockchain transaction demand.

4.5. Pump-and-dump schemes

Pump-and-dump schemes in cryptocurrency markets are highly organized and frequent, differing significantly from traditional stock market manipulations. Dhawan and Putnins (2023) provide a deep insight into how these schemes are carried out, their rampant prevalence, and what motivates participation from a psychological perspective. Unlike the traditional form of a pump-and-dump scheme, relying on information asymmetry and spreading false information to manipulate stock prices, many cryptocurrency pump-and-dumps are performed openly, with manipulators declaring their intent to participants via social media platforms like Telegram.

In a pump-and-dump, 'pump group administrators' choose a low-liquidity cryptocurrency and issue a pump signal to artificially inflate its price. These schemes target relatively illiquid coins to make price manipulation easier, though the coin must still have enough liquidity to make the manipulation worthwhile. Dhawan and Putnins 2023 identified 355 cases of pump-and-dump schemes over a six-month period involving 197 distinct cryptocurrencies. This accounts for about 15% of the total coins traded on the two cryptocurrency exchanges analyzed: Binance and Yobit. That works out at an average of two pumps per day with such schemes raking in about $350 million in trading volume, and manipulators siphoning off about $6 million in profits from participants.

A typical pump-and-dump scheme begins with preparatory steps, wherein the manipulators amass positions in the particular cryptocurrency before advertising the upcoming pump. The organizers give a “pump signal” at some predetermined time, indicating what cryptocurrency will be pumped. This was usually given as a message in the Telegram or Discord group. This would serve as a call for action for members to start buying the coin in bulk, leading to its price increase. A typical example cited by Dhawan and Putnins (2023) is ChatCoin (CHAT). It was the target of a popular Telegram group named Big Pump Signal (BPS), with over 63,000 members. In this case, the pump signal was at 20:00:23 GMT on June 10, 2018. Given the announcement, the price sharply surged by 55% in a rather short period of 17 seconds. The trading volume increased from $17,313 to $2.69 million within half an hour after the pump signal.

This is not all: the pace of these plans is amazing, too. A pumped coin typically reaches its peak price within eight minutes, after which the price drops sharply as manipulators and quick actors cash out. The price often falls back to pre-pump levels within a day, or sometimes in mere hours. Dhawan and Putnins 2023 show that price distortions during such pump events are significant, leading to an average return of 65% in a few minutes, which is roughly four standard deviation returns of daily cryptocurrency returns. Moreover, on pump days, the trading volume is as large as 13.5 times the usual volume. It enables manipulators to take full advantage of the volatility to unwind their positions with large gains. A notable difference between cryptocurrency pump-and-dump schemes and traditional stock market schemes is the lack of pretense. The promoters of cryptocurrency markets do not require a fictional story of intrinsic value and/or persuading investors that there is private information of undervaluation. Instead, they explicitly invite others to join the pump and get them to benefit from the price increase thereafter. The participants also fully understand that the price rise is artificial; yet they must purchase now and sell during or at the peak or ahead of time when the price may fall. In contrast, Dhawan and Putnins, 2023 argue that

these mechanisms are inherently zero-sum game in nature: it is only the fastest or best player gains while remaining players collectively face financial loss.

Two primary behavioral drivers are overconfidence and gambling. These overconfident participants believe that they can sell at the peak of the market frenzy. However, in reality, most participants become losers because of rapid reversals in prices after the fact. Dhawan and Putnins (2023) provide evidence of empirical data on overconfidence due to past successes in pump schemes where participants attribute favorable outcomes to their expertise and not due to chance. This self-attribution bias encourages individuals to further continue the activity under the impression that they expect poor returns.

Dhawan and Putnins (2023) contend that the asymmetrical payoff distribution characteristic of pump schemes—where there exists a minimal probability of substantial gains—draws individuals who perceive these pumps as a variant of gambling. The phenomenon is reminiscent of the interest of people in lotteries or speculative bubble games, where the expectation of high return compensates for the risks involved. Empirical evidence supports the gambling explanation, as activities indicative of cryptocurrency gambling correlate with pump scheme participation. In both cases, individuals join these pumps notwithstanding that the probability of losing is high. The manipulators, or, in other words, the pump group administrators, gain from the Participants' naivety or overconfidence. Dhawan and Putnins (2023) found that manipulators typically earn an average return of 24.77% within minutes of issuing a pump signal, totaling roughly $6 million in profits across 355 cases. Manipulators start building their positions in the target cryptocurrency several hours before issuing the pump signal. This would enable them to sell at inflated prices once the pump occurred. Besides, the greater the participation by members, the higher the peak prices will be, which, in turn, also helps manipulators achieve higher profits.

Another spillover effect typical for cryptocurrency pump-and-dump schemes is found in other markets trading the same coins. Dhawan and Putnins (2023) discovered that trading volume and volatility rose on other exchanges where the pumped coins were listed, although these effects were typically smaller than on the primary exchange where the pump took place. Of course, arbitrage between the exchanges helps to align prices, but some price distortion remains.

The welfare implications of the cryptocurrency pump-and-dump scheme are more complex. Dhawan and Putnins (2023) assert that the flow of wealth is primarily from the less capable participants such as slower traders or gamblers to better-skilled entities including manipulators and faster participants. While gamblers might get some utility from the excitement of being part of

pumps, the overall welfare effects are probably negative as wealth will be shifted from those with higher marginal utility, namely the less sophisticated, to those with low marginal utility, namely the manipulators and faster traders. Third, there are the price distortions induced by pumps, which decrease the accuracy and informativeness of prices. According to theory, such distortions can hurt the efficiency of resource allocation. Nevertheless, these price distortions are typically ephemeral, vanishing within a matter of days; consequently, the enduring effects on resource allocation are probably minimal. A second concern is that rampant manipulation undermines confidence in cryptocurrency markets and, with it, participation and liquidity. Dhawan and Putnins (2023) observe that regulators, such as the U.S. Securities and Exchange Commission, have pointed to manipulation as grounds for rejecting applications for Bitcoin ETFs. The loss of confidence could inhibit the broader adoption of cryptocurrency and the tokenization of assets-a welfare consequence potentially much more significant than the wealth transfers associated with pump-and-dump schemes. Dhawan and Putnins (2023) also show that cryptocurrency pump-and-dump schemes are something more than speculative activities; they are actually very organized manipulations that attract people through overconfidence and gambling preferences. The consequence of such schemes is significant price distortion and volatility, although the effects are usually temporary. Despite these activities being a negative-sum game for most of those participating, the incidence of such pumps keeps rising, fed by the growing interest in cryptocurrencies and the perpetual appeal of speculative gain.

Pump-and-dump schemes in cryptocurrency markets have evolved to capitalize on the influence of personalities and crypto influencers, as extensively discussed by Meyer et al. (2024). While the previously mentioned traditional form of a pump group organizes its manipulative activities through private channels, such as Telegram, crypto influencers use more open platforms like Twitter, YouTube, and other social media outlets to generate participation in those schemes. This approach enables them to exert a more nuanced influence over the market by shaping the actions of their substantial follower networks.

Crypto influencers hold significant sway over retail investors, especially those who are inexperienced or unaware of the risks involved in cryptocurrency trading. These are the influencers who, in most cases, may promote the use of certain coins or tokens to the following people with the guise of offering investment advice or revealing new “hidden gems” in the market. This naturally leads to a collective buying spree wherein the followers are quick to buy the promoted coins, driving up the price in a typical pump phase of action. The involvement of influencers in

pump-and-dump schemes has gained incidence with the growth of the cryptocurrency sector. For example, Meyer et al. (2024) mention that some influencers profit by front-running on their own advice, meaning that they have bought the cryptocurrency in advance of its recommendation to followers. They immediately sell their holdings at considerable profit once their followers start buying and the price rises, leaving their followers to lose when the coin's value finally falls.

One of the defining characteristics of influencer-driven pump-and-dump schemes is that the transaction is shrouded in opaqueness. Often, followers are unaware that the influencer has already purchased the cryptocurrency before promoting it, leading to information asymmetry While classic pump groups are composed of any person who knowingly can act with speculation and risk, in the case of cryptocurrency influencers, their followers may be actually receiving valid investment advice, hence raising ethical concerns for such schemes. Meyer et al. (2024) give several interesting examples of promotional activities through the so-called influencer-led campaigns that have actually caused huge market disruptions. For example, an influencer publicly endorsed an unknown cryptocurrency on Twitter in 2021, and its price surged more than 80% in minutes. That surge was short-lived, however, because the price plummeted just as rapidly once the influencer and initial investors sold their holdings.

Less-experienced retail investors who had been seduced by the hype incurred significant losses when the coin's value fell back to pre-promotional levels. The exaggeration of such plans might stem from the usually decentralized and mostly unregulated nature of cryptocurrency markets, wherein it is possible for influencers to exploit follower demographics without undergoing similar regulatory scrutiny seen in more traditional financial markets. As Meyer et al. (2024) mention, that lack of regulation has enabled these influencers to practice moves that otherwise might be considered illegal or quite unethical in more traditional markets, such as front-running or releasing false information regarding the prospect of a cryptocurrency.

Another characteristic of influencer-led pumps is the manipulation of sentiment. Meyer et al. (2024) observe that influencers build positive sentiment toward a coin by using emotive language to generate excitement and FOMO among followers. This sentiment-driven behavior has proven to be extra effective in cryptocurrency markets characterized by high volatility and easily manipulated prices due to heavy buying and selling. What is more, most of the influencers time their endorsements to popular market trends or events-like new coin listings or partnerships that give credibility to their endorsements. This way, influencers can mask their pump-and-dump operations to seem just like a legitimate market opportunity and further blind their followers from

recognizing the manipulative activity. Meyer et al. (2024) suggested that this practice would not only individually affect investors but also make the vulnerability in cryptocurrency markets worse. Distortions in prices due to pump-and-dump schemes spill into other assets as well, thereby increasing volatility and damaging market confidence.

These influencers also target relatively illiquid coins, similar to more traditional pump-and-dump schemes, where large buy orders have the most pronounced price impact. Through this, driving up the price of such low-liquidity assets would allow influencers to generate significant short-term gains but also more extreme price reversions once the pump ends.

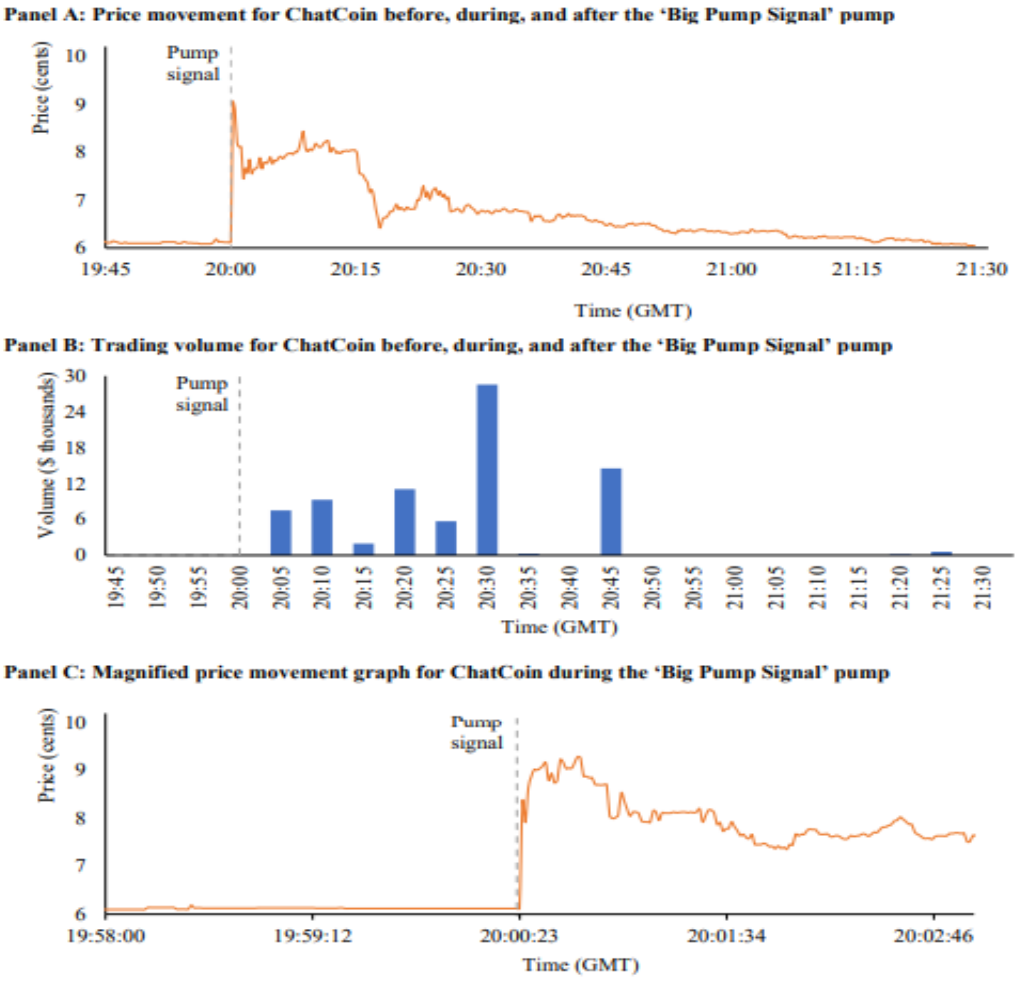
The rapid flows-especially those characterized by high inflows and outflows of capital-increase the volatility of the given cryptocurrency and pose risks to other market participants who are not a party to the scheme. Meme culture and the growth of social media communities of cryptocurrencies have amplified the effects of influencer-led price increases. Meyer et al. (2024) observe that certain influencers leverage the meme and narrative viruses coming from these communities to promote specific cryptocurrencies, often with a lack of concern for the actual features of the coin. This speculative behavior represents the enthusiasm found in traditional pump-and-dump schemes but is magnified by the speed and breadth possible through social media platforms. While some participants recognize the speculative nature of those pumps, the mere promise of a quick profit, especially amplified by the perceived credibility and social status of the influencers themselves, easily lures many retail investors. Meyer et al. (2024) emphasize that these practices raise significant red flags for regulators, as the lines between market promotion and manipulation become blurred. The research advocates for enhanced supervision and the possible establishment of regulatory structures to mitigate the influence of social media personalities in cryptocurrency markets, given that their activities can result in considerable financial detriment to unwary investors.

4.5.1. Case Study — CHAT coin

Dhawan and Putnins (2023) provide an extended, real-time analysis of a ChatCoin (CHAT) pump-and-dump scheme orchestrated by the large Telegram group Big Pump Signal (BPS). This group of roughly 63,000 members at that time coordinated the pump on the Binance exchange on June 10, 2018.

The manipulators first positioned themselves favourably by buying ChatCoin in anticipation of an imminent price increase. At exactly 20:00:23 GMT, the BPS operators sent a pump signal, notifying members that ChatCoin was the target cryptocurrency for the manipulation. The message marked the beginning of the manipulation period; participants, anticipating the message, had already begun buying ChatCoin, which quickly drove up its price.

The effects did not take long to arrive. Just 17 seconds after the pump signal, ChatCoin's price surged by an impressive 55%, driven by the collective buying from group participants. The rapid price increase was thus accompanied by a strong surge in trading volume. Before the pump, ChatCoin's trading volume was relatively low at $17,313, or 2.55 BTC. Less than 30 minutes after the pump signal, however, trading volume skyrocketed to $2.69 million.



Dhawan and Putnins (2023), Figure 7—Price fluctuations of CHAT around the BPS Pump

Figure 4 in Dhawan and Putnins (2023) depicts 15-second price fluctuations, highlighting the sudden surge in both price and trading volume immediately after the pump signal. Before the onset of the pump, ChatCoin displayed minimal trading activity, with its price maintaining a consistent level.

Due to the pump signal, the price began to increase steeply and sharply, with the price blowing up within mere seconds. As expected, ChatCoin's price did not stay elevated for long; after peaking, the price declined as manipulators and other quick actors began offloading their holdings.

Notably, it remained relatively high for about an hour past the initial pump signal, before it finally came back to its pre-pump state. The temporary price increase persisted due to lagging participants who continued buying into the scheme, hoping for profits, unaware that the price had already peaked.

The data indicates that post-pump trading volume was 3.6 times higher than ChatCoin's median daily volume recorded from December 2017 to July 2018. This illustrates the level of manipulation, as an instant surge of buyers responding to the pump message jacked up price and trading volume for ChatCoin in the shortest time frame. Having established positions prior to the pump, BPS administrators were able to sell ChatCoin at inflated prices early in the scheme, profiting significantly from the artificial price movement. Those coming in later, or who were not fortunate enough to sell at the peak, lost when the price returned to normal once the manipulators stepped out of their positions.

4.6. Private Key Compromises and Hacking

According to Grobys (2021), compromises of private keys and hacking incidents are major vulnerabilities within the cryptocurrency ecosystem. These vulnerabilities carry significant consequences for individual users and broader financial markets due to the irreversible nature of cryptocurrency transactions once a private key is compromised. Unlike traditional financial systems that may offer possibilities to reverse or dispute transactions, the native decentralization of cryptocurrencies makes their recovery almost impossible. This feature turns out very rewarding for hackers, who attack vulnerabilities in the security frameworks of both exchanges and individual wallets.

The main point of entry for cybercriminals is through cryptocurrency exchanges that retain users' private keys. Grobys (2021) reports that 73% of cryptocurrency exchanges retain clients' private keys, creating a “honeypot” scenario that attracts cybercriminal activity. Such exchanges, acting as custodians for substantial amounts of cryptocurrency, frequently become targets of hacking endeavors due to the aggregation of private keys within their custody. A successful cyber intrusion causes considerable financial loss, as has been well-illustrated by a number of high-profile cases over the years.

One of the major issues associated with the compromise of private keys involves the use of hot wallets, a form of digital storage facility that enhances easy access to financial resources but is highly vulnerable to possible cyberattacks. While many exchanges employ cold storage—offline techniques to safeguard private keys—these methods are not completely immune to attacks. Cybercriminals have devised advanced techniques for infiltrating cold storage systems, though Grobys (2021) emphasizes that around 90% of exchanges employ cold storage systems to secure the bulk of their assets. Regardless of this, limitations imbued by cold storage, particularly its vulnerability on critical instances of online transactions, still pose risks.

A private key compromise is especially severe, giving malicious actors full access to the corresponding cryptocurrency wallets. Upon the theft of a private key, the perpetrator can move all funds from the wallet to a different address, leaving the original owner without any means to recover their misappropriated assets. Grobys (2021) underscores that this susceptibility is intensified by the anonymity associated with cryptocurrency transactions, rendering the tracing of misappropriated funds exceedingly challenging. Furthermore, even when illicitly acquired funds are moved between wallets or exchanges, they frequently traverse obfuscation techniques such as mixers and tumblers, which further complicates the endeavors to trace and reclaim the stolen resources. From 2013 to 2017, Grobys (2021) notes that there were 1.1 million Bitcoin illicitly gained from 29 separate hacking incidents, which accounted for approximately $8.9 billion in financial losses at Bitcoin's 2018 value. These criminal actions occurred through many exchanges, demonstrating just how grave the threat is when a breach in private key security occurs. The staggering scale of these losses serves to point out the weaknesses in the cryptocurrency ecosystem, besides financial effects emanating from hacking incidents.

The compromise of private keys has important consequences for individual users, exchanges, but also for the cryptocurrency markets as a whole. Grobys (2021) discusses how hacking incidents are often followed by spurts in market volatility, particularly in the days following a security

breach. For example, the study finds that Bitcoin return volatility increased substantially in the days following a hacking incident, in a delayed fashion, peaking around five days after the hack. Such a lagged response indicates inefficiencies in the market, where the full implications of the damage from a hack are not immediately incorporated into prices by market participants. Such inefficiencies present avenues for speculators and traders to exploit the increased volatility that ensues subsequent to a security breach.

Ethereum is the second-largest cryptocurrency by market capitalization, and such incidents have equally taken a toll on it. Grobys (2021) finds evidence of similar volatility responses transmitted from Bitcoin to Ethereum, especially after major hacking incidents in the Bitcoin market. Contagion-a situation where volatility is transmitted from one cryptocurrency to others-is what the investors and market players who do not necessarily have Bitcoin but eventually are vulnerable to its changes through other cryptocurrencies, such as Ethereum-emphasize. The ways in which the compromise of private keys occurs are varied; however, phishing attacks remain one of the most widely used methods by cybercriminals to access users' private keys.

Grobys (2021) explains that phishing emails and malicious websites are commonly crafted to deceive users into disclosing private keys or exchange credentials. Once cyber thieves gain unauthorized access to an individual's cryptocurrency exchange account, they can withdraw the funds from the exchange and then move them through a series of transactions to further disguise their origin. Besides phishing, other very common methods of social engineering attacks and malware are used to compromise private key security. Grobys (2021) notes that malware targeting cryptocurrency wallets can locate stored private keys or track keystrokes as users type private keys.

On the other hand, social engineering attacks utilize people's habits of voluntarily revealing confidential information under the disguise of trustworthy sources, like customer support representatives from virtual currency exchanges. These techniques take advantage of psychological rather than technical vulnerabilities, which makes them particularly dangerous since they bypass traditional cybersecurity measures. Upon receiving private keys, various obfuscation techniques are tried, from using mixers and tumblers in an attempt to obscure the transaction trail. Grobys (2021) highlighted that such services make the work of law enforcement in tracing ill-gotten assets difficult because they have facilitated shuffling of cryptocurrencies across a host of wallets and transactions before their final apportionment. This obfuscation is a key reason why private key compromises are so effective for laundering stolen funds and evading detection.

The aftermath of private key compromise and hacking incidents is more than the financial loss of individuals and exchanges. Grobys (2021) further discusses the severe reputational damage that almost always follows after a major security breach. Trust is a crucial part of the cryptocurrency space, and a major hacking incident can shake trust in not just the exchange on which the breach occurred but also the broader market. Following a hack, users may be less willing to store assets on exchanges or engage in cryptocurrency markets, leading to reduced liquidity and increased volatility. Given the associated risks of private key compromise, some scholars, like Grobys (2021), support a combined approach, one which not only looks at technological improvements but also at regulatory strategies. As for the former, the development of multi-signature wallets and hardware wallets adds further layers of security, making the unauthorized access to private keys difficult for malicious actors.

Multisignature wallets require multiple private keys to confirm a transaction, hence reducing the risk of losing money by the compromise of a single key. Hardware wallets that store keys offline are more secure than hot wallets, but still vulnerable to different kinds of attacks. Other regulatory measures, such as the implementation of more robust Know Your Customer and Anti-Money Laundering for virtual currency exchanges, could further reduce the incidence of private key compromise. Grobys (2021) recommends that regulators enforce stricter security practices for exchanges, such as mandatory 2FA and enhanced encryption standards for storing users' private keys. It will upgrade the entire security infrastructure of the exchange and help regulators reduce the chances of large-scale hacking incidents and eventually protect the users from fund losses in case of compromised private keys.

Chapter 5: Preventing Criminal Activity Using Cryptocurrency

5.1. Blockchain as a Prevention to Counterfeits

Applying blockchain technology provides a feasible solution to combat the rise in counterfeit products across various industries, especially within the pharmaceutical sector. Globally, counterfeit goods have surged above $4.5 trillion, comprising over 3.3% of international trade. This increase is largely driven by digital platforms that provide anonymity and direct consumer access (Naoum-Sawaya et al., 2023). The emergence of blockchain technology, which provides a secure and unalterable record of product origins and transactions, has become a crucial tool in addressing this pervasive challenge. A variety of businesses, including high-end brands like Prada and Louis Vuitton, as well as large pharmaceutical companies such as Sanofi, have adopted blockchain-based approaches to track and verify products, aiming to prevent counterfeit goods from infiltrating the consumer market (Naoum-Sawaya et al., 2023).

Counterfeit goods have two types: deceptive and non-deceptive counterfeits. Deceptive counterfeits, such as counterfeit drugs, pose significant risks to public health and consumer safety due to Naoum-Sawaya et al., 2023. In the pharmaceutical industry, counterfeit drugs often contain improper ingredients or incorrect dosages; these characteristics make consumers unable to distinguish the products from the genuine ones. As a result, people unconsciously purchase counterfeit goods at market prices, which sometimes causes dangerous situations. Traditional methods for combating counterfeit drugs, such as unique serial numbers for tracking, have their limitations, as counterfeiters can manipulate these numbers, diminishing their effectiveness (Naoum-Sawaya et al., 2023).

Blockchain enhances traceability in the supply chain through decentralization and transparency, offering participants greater visibility across each step.

However, blockchain faces challenges, such as the potential for counterfeiters to manipulate digital records by verifying serial numbers, which could undermine product authenticity (Naoum-Sawaya et al., 2023). Despite these challenges, blockchain remains a hopeful tool for the pharmaceutical industry, though its success relies heavily on cooperation across the supply chain and a continuous awareness of evolving counterfeiting methods. The secure and immutable nature of blockchain records holds significant value for sectors that frequently encounter counterfeiting issues, including pharmaceuticals, luxury items, and clothing (Naoum-Sawaya et al., 2023). Through the facilitation

of transparency throughout the entire supply chain, blockchain improves the capacity of manufacturers and distributors to monitor product movements and identify possible occurrences of counterfeiting.

Additionally, the technology's effectiveness depends on the quality of input information and the regular updating of records. An effective blockchain system is expensive to maintain; meanwhile, the secure link between a physical product and its digital record is still a weak point. Counterfeiters could simply remove or clone a product and smart tag to further complicate things (Naoum-Sawaya et al., 2023). Strategically, blockchain can reduce the profitability of counterfeit transactions, making counterfeiting less economically attractive (Naoum-Sawaya et al., 2023). This study investigates the equilibrium that manufacturers must achieve between the expenses related to the implementation of blockchain technology and the prospective advantages of curtailing counterfeit sales.

One of the factors considered in this decision is the cost involved in creating counterfeit copies versus the market value of the original products. The higher the manufacturing cost of counterfeit goods, the lower the chances that valid producers will apply blockchain technology to protect their products. On the other hand, a high market price may reduce the intensity of blockchain adoption because costs related to maintaining the technology may be higher than the expected benefits derived (Naoum-Sawaya et al., 2023). Naoum-Sawaya et al. (2023) identify three types of products based on the relative cost of producing genuine versus counterfeit items. Blockchain will be less attractive for products whose counterfeit goods are much cheaper to make, such as luxury goods with high production costs. In other products, especially those with similar production costs between genuine and counterfeit items, the attractiveness of blockchain increases.

Counterfeiting can also be combated with blockchain technology used by manufacturers as a strategic complement to quality investment in products. In summary, the model of Naoum-Sawaya et al. (2023) illustrates that every manufacturer may invest either in the quality of the products or in blockchain technology. Both avenues inhibit the counterfeiters in different ways.

While blockchain can discourage counterfeiting, there is a potential downside. Heavy reliance on blockchain for counterfeit prevention could diminish manufacturers' incentives to invest in product quality. The results suggest that blockchain adoption could lead to lower product quality, as manufacturers may prioritize blockchain implementation over product improvement (Naoum-Sawaya et al., 2023). This trade-off is of considerable relevance in industries like pharmaceuticals, where the quality and traceability of products are essential in guaranteeing consumer safety. In

recent years, the adoption of blockchain technology into supply chains has increasingly become quite pervasive, mainly due to its great potentials for improving information sharing, reducing paperwork, process automation, and enhancement of verifiability. Blockchain technology application manifests signs of quality and reliability, motivating the opportunity for a competitive companies to collaborate in sharing information whenever benefit will be attained by the respective parties (Naoum-Sawaya et al., 2023).

Similar to technologies like Radio Frequency Identification (RFID), blockchain facilitates product tracking along the value chain, particularly benefiting industries like luxury goods and pharmaceuticals (Naoum-Sawaya et al., 2023).

The pharmaceutical sector faces a significant threat from counterfeiting activities. Counterfeiters frequently penetrate legitimate supply chains using misleading labeling and packaging, which complicates the identification of counterfeit products (Naoum-Sawaya et al., 2023). Blockchain technology presents a viable solution by enhancing transparency and traceability across these intricate supply chains. Nevertheless, the financial motivations for manufacturers to implement blockchain are not always evident. Government subsidies or pricing incentives may be necessary to boost blockchain adoption, especially in sectors where price differentiation between authentic and counterfeit goods is challenging (Naoum-Sawaya et al., 2023).

A substantial amount of modeling regarding the strategic decisions made by both manufacturers and counterfeiters has been undertaken in previous studies, with certain research suggesting that in scenarios involving deceptive counterfeiting, counterfeit and genuine products are marketed at equivalent prices. In contrast, other scholars highlight the significance of price differentiation in relation to non-deceptive counterfeits (Naoum-Sawaya et al., 2023). While blockchain cannot entirely eliminate counterfeiting, it offers a more secure and transparent method for tracking and authenticating products. The enhancement minimizes the chances of counterfeiting products while decreasing the economic incentives involved in dealing with counterfeit goods. Naoum-Sawaya et al. (2023) highlight the importance of considering the costs involved in implementing blockchain against the efficiency in detecting counterfeit products, particularly in industries that are prone to such cases.

5.2. Advanced Technologies for Preventing Criminal Activity

An integrated approach to AML and CFT can leverage advanced technologies to mitigate criminal behaviors across financial institutions, decentralized platforms, and regulatory bodies. Crucial technological innovations, including artificial intelligence (AI), machine learning (ML), blockchain analysis, and regulatory technology (RegTech), present significant opportunities to address the challenges associated with money laundering (ML) and terrorism financing (TF). The subsequent sections delineate essential preventive strategies, technological instruments, and the amalgamation of Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols.

5.2.1. AI and Machine Learning for Transaction Monitoring

Artificial intelligence and machine learning have transformed AML compliance by enhancing the effectiveness of detecting suspicious activities. AI-powered tools can analyze voluminous datasets to identify patterns that may indicate illicit transactions. For instance, these tools deploy algorithms on spending habits monitoring of customers, detecting anomalies, continuous learning of new tactics employed by criminals. Akartuna et al. (2022) present evidence that machine learning can reduce false positives by up to 55%, making it a game-changing tool for any financial institution overwhelmed by the enormous volume of transaction data it needs to process. The application of AI to transaction monitoring performs particularly well in interpreting behaviors related to cryptocurrency exchanges and DeFi platforms, the so-called hot spots where traditional monitoring solutions are becoming most challenged.

5.2.2. Blockchain Analytics

Blockchain analytics tools play a crucial role in tracking the source and destination of cryptocurrency transactions. These tools can show the flow of money in decentralized systems to help find patterns of illegal behavior, including money laundering using mixers, tumblers, and privacy coins. This could be realized through technologies such as Chainalysis and Elliptic, which, through real-time transaction tracking and risk assessment for a variety of cryptocurrencies, have considerably enhanced the possibility of investigations into ML and TF activities by law

enforcement and compliance officers. Akartuna et al. (2022) analyze blockchain data, underlining that these tools are able to show relations between wallets and exchanges, hence increasing transparency in decentralized financial ecosystems.

5.2.3. Know Your Customer (KYC) and Customer Due Diligence (CDD)

Know-Your-Customer (KYC) protocols are fundamental to anti-money laundering efforts, requiring financial institutions to verify customer identities before processing transactions. Akartuna et al. (2022) observe an increase in the use of biometric identification technologies in KYC for face recognition and fingerprinting purposes as means to enhance accuracy and reduce identity fraud. The scope of KYC is also expanding from traditional financial institutions to VASPs, cryptocurrency exchanges, and decentralized platforms. RegTech innovations have enabled firms to automate KYC processes, reducing onboarding time and improving compliance while ensuring that customers are screened for connections to high-risk individuals or countries flagged by AML/CFT regulations.

5.2.4. RegTech for Compliance Automation

RegTech solutions simplify regulatory compliance for financial institutions, helping to minimize operational costs. These technologies automate the KYC process, transaction monitoring, and report generation. With the use of RegTech in company systems, it helps them continuously monitor transactions. Transactions showing suspicious behavior are highlighted, reducing manual efforts. Certain tools within RegTech solutions perform cross-referencing of customer data against global lists of sanctions. Akartuna et al. (2022) also indicate financial gains that RegTech can offer to FinTech startups, as these are often burdened with high compliance costs. Compared to traditional AML systems, which are costly yet inefficient, RegTech has enabled more feasible ways of pursuing compliance, especially in decentralized financial services.

5.2.5. Distributed Ledger Technologies (DLTs) and Smart Contracts

Although distributed ledger technologies pose risks due to their decentralized nature, they also offer solutions for crime prevention. Smart contracts, for instance, can be programmed to embed mechanisms that make AML/CFT compliance mandatory, thus constraining the execution of a transaction based on specific conditions. For instance, embedding the condition of proof of identity or source of funds within a smart contract would impede the movement of illicit funds. Further, Akartuna et al. (2022) consider the possibility of infusing "smart controls" into the programming of cryptocurrencies, wherein law enforcement would act based on misconduct, thereby setting up ways of responding instantly to questionable transactions.

5.2.6. Privacy-Enhancing Technologies and AML Compatibility

One of the challenges in AML efforts involves balancing the need for privacy with the demand for greater transparency. Privacy coins, like Monero and Zcash, present unique challenges by anonymizing transactions and complicating traceability. EDD measures and privacy-enhanced transaction monitoring will be needed to act against that. Akartuna et al. (2022) suggest that while an outright ban on privacy coins is an approach that could be pursued, technological tools such as privacy-preserving analytics and cryptography-including zero-knowledge proofs could still enable surveillance of these currencies while maintaining user privacy.

5.2.7. Enhanced Due Diligence (EDD) and Wallet Provider Obligations

Enhanced Due Diligence (EDD) extends beyond KYC and CDD, requiring deeper scrutiny of a customer's funds, particularly in high-risk cases. Wallet providers, cryptocurrency exchanges, and DeFi platforms will need to develop EDD processes and procedures to comply with the AML/CFT regime. Akartuna et al. (2022) explain that wallet providers need to track not only transaction activity but also activity from related accounts, emails, and devices that indicate possible illicit activity. Besides this, the exchanges must scrutinize foreign deposits and large transfers particularly from jurisdictions with relaxed AML laws.

5.2.8. Global Regulatory Coordination and Information Sharing

Because of the global nature of financial crimes, international cooperation plays a key role in the process of effectively enforcing AML/CFT. Akartuna et al. (2022) propose the establishment of global regulatory bodies that would be responsible for harmonizing the AML measures across jurisdictions to ensure that criminals could not take advantage of loopholes by operating in less regulated countries. Besides, information sharing must be enhanced among financial institutions, regulators, and law enforcement agencies for the timely identification of suspicious activities and proportionate responses. Secure APIs and blockchain-based tracking systems are technologies that support cross-border data sharing, crucial for the improvement of cooperation in global AML/CFT efforts.

5.2.9. Detection Algorithms and Fraud Prevention in New Payment Methods

New payment methods (NPMs), such as mobile point-of-sale (POS) systems and social media payment platforms, present unique risks for money laundering and fraud. Detection algorithms can be employed to monitor transactions across these platforms, identifying suspicious patterns such as rapid fund transfers, fake services, or chargeback fraud. Akartuna et al. (2022) highlight the importance of implementing machine learning-based detection systems to track payments in real-time and flag anomalies in the use of NPMs. Further, integrating behavioral analysis tools can help differentiate between legitimate and illicit activities based on the transaction histories of users.

5.2.10. Centralized Control over Conversion Points

Controlling cryptocurrency-to-fiat conversion points, like crypto-exchanges and ATMs, is vital in preventing ill-gotten funds from entering the traditional financial system. Also, if regulators can make it even a little bit harder to allow suspicious activity to occur at these points, then tracking may start there and ensure the application of AML/CFT measures. According to Akartuna et al. (2022), increased control is required with clear identification of users through the verification process. It involves identifying large-value transactions and reporting suspicious ones to authorities.

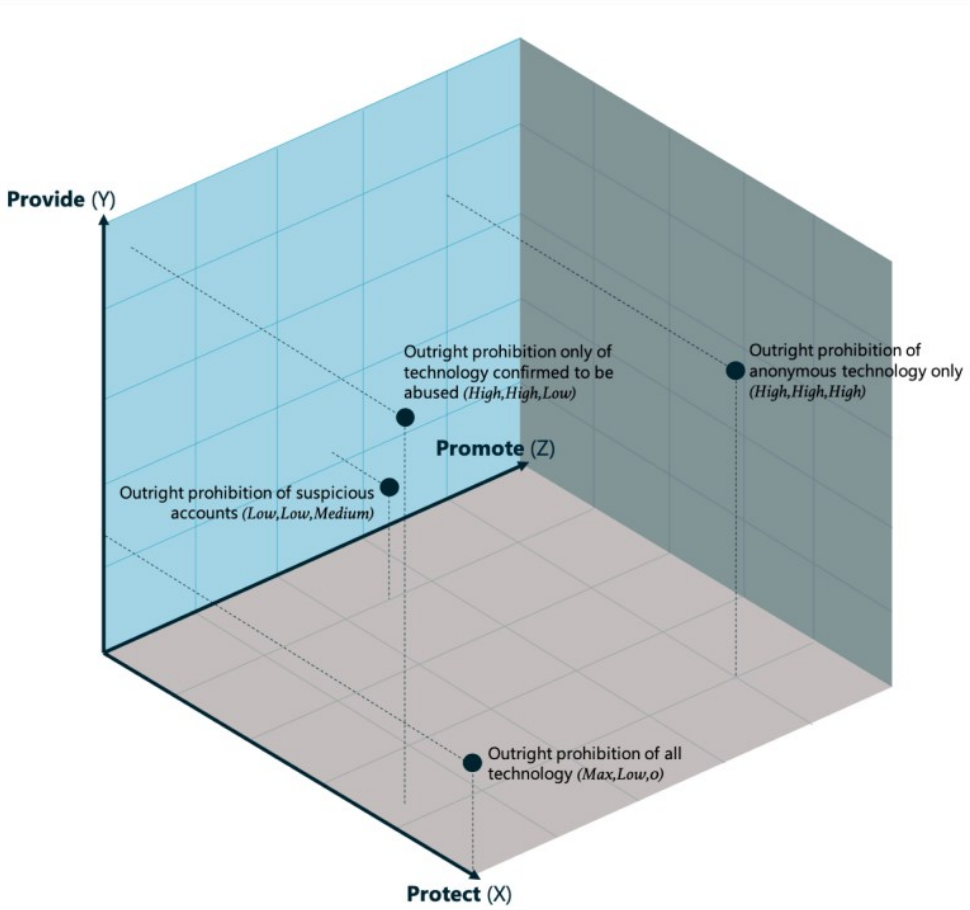
5.2.11. Public Awareness and Education Campaigns

Public education plays a critical role in preventing the recruitment of crypto-mules and reducing the vulnerability of certain populations, such as students and the elderly, to financial crime. Akartuna et al. (2022) propose widespread education campaigns to inform the public about the risks of scams, fraudulent investment schemes, and the dangers of participating in money laundering schemes. Such campaigns could also encourage individuals to report suspicious activities and seek advice before engaging in cryptocurrency transactions.

5.3. The Future of AML and CFT Technologies

With financial technologies rapidly evolving, it is important to futureproof the AML/CFT frameworks in order to keep them up to date with the latest risks. Akartuna et al. (2022) continue to stress the need for collaboration between regulators, financial institutions, and technology companies in the development of scalable and cost-effective prevention. AI integrated with blockchain analytics and advanced RegTech will be integral in the fight against criminals exploiting new technologies. In addition, the flexibility of regulatory frameworks that avoid hampering innovation is needed for continued long-term success related to anti-financial crime.

All in all, prevention of criminal behavior in the digital financial space requires state-of-the-art technologies, oversight, and supervision through regulation and international cooperation. AI, blockchain analytics, reg-tech, and enhanced Know-Your-Customer/AML practices provide the right toolkit to identify and reduce illicit activities in real time, while public education and harmonization of regulatory frameworks present effective barrier mechanisms against emerging risks. According to Akartuna et al. (2022), all these technologies and frameworks together can help stakeholders minimize the risk of money laundering and terrorism financing within the modern financial ecosystem.



Mishra and Prasad (2024), Figure 8—An example 3P model for different implementation strategies of ‘outright prohibition’

Chapter 6: Central Bank Digital Currencies (CBDCs)

Central bank digital currencies are transforming the global financial landscape, with central banks worldwide exploring pilot programs and, in some cases, full-scale retail CBDC launches. Some of the key drivers of CBDC include the growing usage of digital payment technologies and reduced reliance on physical cash globally. Consequently, many central banks are exploring CBDCs to enhance payment systems, promote financial inclusion, and strengthen monetary stability (Mishra and Prasad, 2024). Indeed, innovative countries like the Bahamas, the Eastern Caribbean Currency Union, and Nigeria already introduced CBDCs into their economic systems. In the meantime, several major countries like China, India, Japan, and Sweden are carrying out pilot programs to test their viability and implications.

Essentially, CBDCs are fundamentally distinct from both cash and existing electronic payment systems. Cash is still the physical medium of exchange and a liability of the central bank, while retail CBDCs represent its digital equivalent, also a claim on the central bank, distributed via either the commercial banking system or other types of payment service providers.

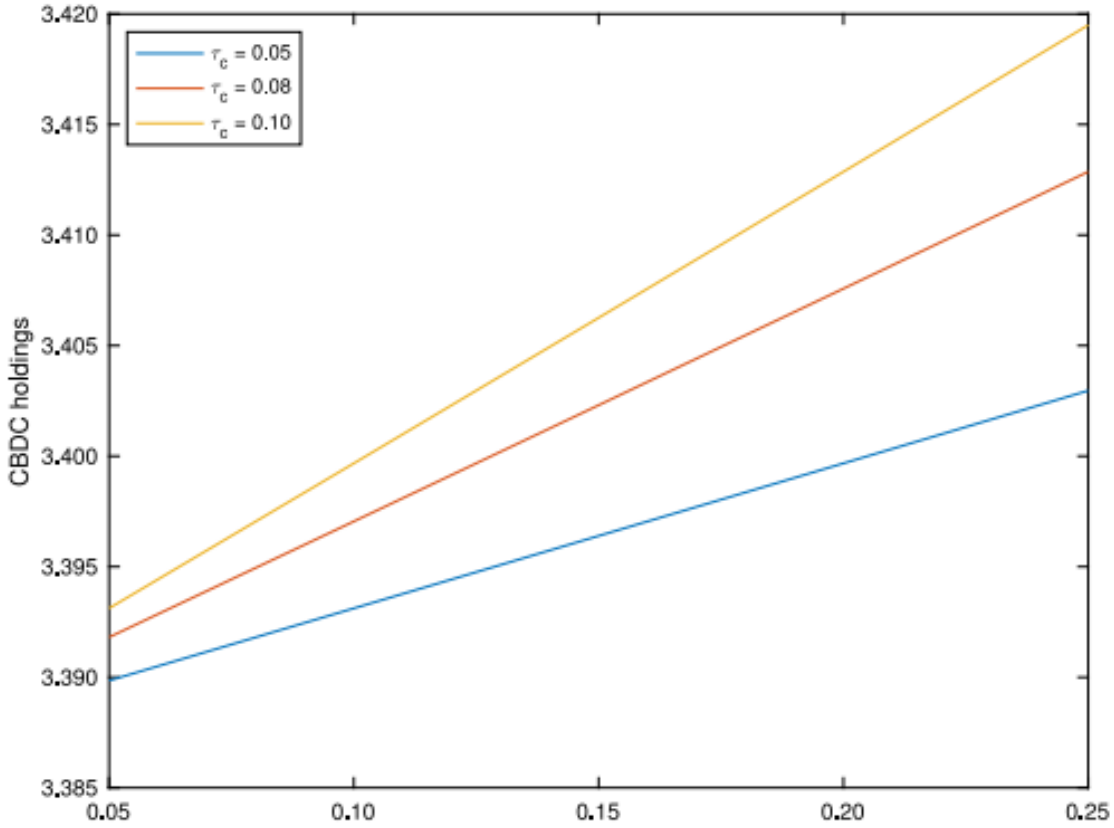
Unlike electronic balances maintained by financial institutions, CBDCs are designed for direct accessibility to all participants in the economy (Mishra and Prasad, 2024). This accessibility is crucial for financial inclusion, as CBDCs can provide a convenient digital payment option for unbanked or underbanked individuals, many of whom still rely heavily on cash due to limited banking infrastructure. Among the motives for central banks to develop CBDCs, one important factor is their need to create a reliable, government-backed digital means of paying that could perform a balancing role against privately operated and confidence-shocked-vulnerable payment systems. This growing dominance by private sector platforms for payments does engender concerns over financial stability-particularly during crises wherein loss of confidence in these systems would provoke great disruption. A central bank-managed CBDC could provide a backstop, offering a more stable and secure alternative to private digital currencies and payment methods (Mishra and Prasad, 2024).

The CBDC model of Mishra and Prasad (2024) focuses mainly on account-based or register-based CBDCs that have the potential to provide immediate and inexpensive settlement. These CBDCs can be held in digital wallets, working just like normal bank accounts, but under the direct management of central banks. As CBDCs make their way into existing financial systems, that opens a host of complex economic trade-offs between cash and digital currencies. In their

framework, Mishra and Prasad (2024) outline how CBDCs, despite their higher transaction efficiency and lower costs compared to cash, will likely coexist with physical currency, especially given the political, privacy, and socioeconomic considerations surrounding the use of cash.

One of the critical advantages of CBDCs is their potential to let illicit activities be curbed by reducing the anonymity linked with cash transactions. According to Kenneth Rogoff (2017), CBDCs would provide a way of combating the illicit use of central bank money, such as tax evasion or money laundering, due to traceability. Besides, CBDCs would permit central banks to perform monetary policy with more flexibility. With CBDC, this constraint on the zero lower bound on interest rates could be avoided by the central banks by simply changing the nominal rate on CBDCs, thereby implementing negative nominal rates in times of crisis to spur economic activities without driving people to hoard cash. According to Mishra and Prasad (2024), even in conditions of negative interest rates, demand for CBDCs would continue because of their efficiency in making transactions compared to cash. However, the coexistence of cash and CBDCs presents challenges. While CBDCs may offer greater transaction efficiency and allow central banks to levy taxes on digital transactions, cash remains an attractive option for tax evaders due to its anonymity and the lack of transaction costs.

Mishra and Prasad (2024) explore how government policies, such as adjusting CBDC returns, enhancing tax evasion detection, and imposing penalties, influence cash and CBDC preferences. Their analytical framework shows that the share of CBDCs in total assets is fairly sensitive to changes in the nominal return on it. Higher returns to CBDC and improvements in the efficiency of its use have major welfare gains due to the induced substitution out of cash. Notwithstanding these advantages, there are fears that if CBDCs attain large-scale adoption, they will disrupt the banking system. A significant movement of money from bank deposits to CBDCs could threaten the lending functions of banks and hurt economic growth. Mishra and Prasad (2024) suggest a design for CBDC interest rates with conditions under which any significant holdings of CBDCs would be subjected to charges in order to maintain a balance between the use of CBDCs and other traditional financial instruments like bonds.



Mishra and Prasad (2024), Figure 9—Relationship between probability of cash holding above threshold and CBDC holdings.

The paper also addresses why cash, despite being less efficient than CBDCs, will likely continue to play a role in the financial system. Eliminating cash altogether could have negative consequences, particularly for the poor and for those concerned about privacy. Cash offers financial anonymity, which remains important, particularly in regions where political or economic instability increases surveillance concerns. Mishra and Prasad (2024) argue that, while such governmental policies can be utilized to reduce the demand for cash, such as the taxation of large cash holdings or even the imposition of transaction taxes, eliminating cash entirely is neither practically possible nor desirable in most economies.

Above and beyond the direct effects on financial inclusion and monetary policy, CBDCs also interact with broader questions about the coexistence of official currencies and private

decentralized cryptocurrencies such as Bitcoin. CBDCs are a means of digital currency that is regulated and stable, whereas private cryptocurrencies operate independently of traditional financial systems and are often typified by impaired regulatory oversight and heightened volatility. As Mishra and Prasad (2024) note, their model has clarified how both CBDCs and private cryptocurrencies could coexist, especially in economies where wide differences in transaction costs, tax policies, and the likelihood of monitoring distinctly differentiate between the two. This, in turn, defines some key areas of exploration in the current literature regarding the design of CBDCs, especially with regard to aspects of anonymity, security, and how they are related and embedded within financial markets. Some models treat CBDCs as complementary to bank deposits, while others consider them in competition with deposits, potentially disrupting financial stability and lending activities.

According to Mishra and Prasad (2024), the relative attractiveness of CBDCs will depend significantly on government policy choices, particularly as relates to tax treatment of CBDC transactions, penalties for cash-related tax evasion, and the interest rate structure on CBDCs. One of the most valuable contributions of their paper is a general equilibrium model that analyzes the fundamental dissimilarities between cash and CBDCs based on their efficiency in carrying out transactions, tax implications, and penalties for evasion. In this model, agents maximize utility from private and public consumption, considering budget constraints for various forms of wealth, including cash, CBDCs, bonds, and physical capital. Importantly, the model reveals how the government can affect the relative attractiveness of cash and CBDCs through the use of certain parameters, like tax rates, monitored transactions, or fines for tax fraud.

Mishra and Prasad (2024) further explore the impact of helicopter drops of money—direct transfers of CBDCs into accounts—as a tool for stimulating demand during economic downturns. Their model suggests that such measures could increase CBDC holdings without destabilizing the broader financial system, provided that interest rates and penalties on large CBDC holdings are managed with care. The flexibility of monetary policy design affords central banks with a strong instrument to control economic fluctuations, further consolidating the case for CBDCs to be adopted as part of the modern financial infrastructure.

CBDCs represent a pivotal innovation in global finance, offering transaction efficiency, improved financial inclusion, and enhanced flexibility in monetary policy. However, the successful implementation of CBDCs will depend on carefully balancing their introduction with the continued use of cash and other financial assets. Mishra and Prasad (2024) provide a very inclusive structure

through which such trade-offs have to be understood, with great importance given to governmental policy in influencing the future trajectory that could be taken by digital currencies in their function of deterring criminality. Their research underlines how CBDCs may complement existing financial systems instead of substituting for them and simultaneously offer novel mechanisms for dealing with illegality and ensuring economic stability.

Chapter 7: Conclusion

7.1. Key Findings

This thesis centers on the dual role of cryptocurrencies as tools for both legitimate financial exchanges and instruments for unlawful activities. Cryptocurrencies, including Bitcoin and privacy-centric coins like Monero, provide a level of anonymity and facilitate decentralized transactions, rendering them appealing for nefarious activities such as money laundering, financing of terrorism, drug trafficking, and ransomware attacks. One of the main concerns that has been stressed is that the features which make cryptocurrencies appealing to the general user—decentralized and anonymous—are the features utilized by criminals, thus making it a standing problem for regulators and law enforcement agencies.

Bitcoin's pseudo-anonymity is frequently exploited to facilitate ransom payments.Sokolov (2021) highlights that during ransomware surges, high transaction volumes from ransom payments lead to blockchain congestion and elevated fees, complicating tracing efforts. According to Amiram et al. (2022), terrorist groups exploit cryptocurrency's traceability issues, using mixing services and anonymous wallets to obscure funding sources. The 2019 Easter bombing in Sri Lanka exemplifies how substantial Bitcoin transactions, potentially linked to money laundering or terrorist financing, occurred just before the attack (Amiram et al., 2022).

Privacy-focused cryptocurrencies like Monero and Zcash employ advanced encryption, making transaction tracking significantly harder (Almaqbleh et al., 2023). These currencies are popular in countries with weak regulatory frameworks, like Argentina and Venezuela, where they serve as a hedge against hyperinflation. However, the very features facilitating easy adoption complicate AML and KYC efforts, as traditional monitoring methods are difficult to apply to decentralized models. Akartuna et al. (2022) link inconsistent global regulation to challenges in enforcement, noting that despite FATF's efforts, a lack of cohesive coordination allows offenders to exploit jurisdictional differences. The results additionally demonstrate the intricacy involved in overseeing cryptocurrencies while simultaneously fostering innovation.

Overregulation will deter legitimate use of cryptocurrency, while underregulation will allow the continuance of criminal and illegal acts. The very underlying nature of the decentralized cryptocurrencies makes things very complicated: though blockchain transparency offers some

amount of traceability, several anonymity-enhancing tools, such as mixers and tumblers, mask the origin of funds, thus further complicating regulatory efforts.

Foley et al. (2019) examine the use of cryptocurrencies on darknet markets and demonstrate that Bitcoin remains the dominant cryptocurrency used in drug trading, and is subject to obfuscation techniques, such as tumbling, to hide the origin of transactions.

Dhawan and Putnins (2023) and Meyer et al. (2024) provide evidence of widespread pump-and-dump manipulation in cryptocurrency markets, often targeting illiquid coins for artificial price inflation. Many proponents of such schemes seek social networks to increase participation, with the overconfidence and FOMO of a gambling environment in which one would participate despite the high likelihood of loss. Blockchain analytics, combined with AI and machine learning, offers potential for detecting dubious activities, though ethical concerns around privacy and surveillance persist. However, ethical implications regarding privacy and surveillance remain very valid. Artificial intelligence-driven tools are being tried to apply in tracing questionable transactions by protecting users' privacy. Akartuna et al. (2022) develop the argument that those tools are in an early developmental stage and will need further updates to make them effective. The worldwide characteristics of cryptocurrency markets intensify the issue, given that inadequate regulations in specific areas enable illicit actors to function without consequence. Facing regulatory challenges, offenders adapt by moving operations to countries with fewer restrictions, as seen with the Chatex exchange’s relocation to Estonia after U.S. sanctions (Akartuna et al., 2022). This study underscores the ongoing challenge of balancing innovation, privacy, and security in cryptocurrency. Furthermore, they illuminate the necessity for synchronized global initiatives aimed at addressing regulatory gaps and mitigating the exploitation of cryptocurrencies for illicit activities.

7.2. Implications for Future Research

Cryptocurrency’s association with misconduct will have far-reaching implications for future scholarly research, as the field evolves and gains prominence in global finance. Along with ongoing adoption, there are a few high-priority areas beyond which more research is needed to fully capture the potential benefits of digital assets and reduce the risks of using them in unlawful activities.

Developing more advanced blockchain forensic tools is another key research priority. As the technology in cryptocurrencies evolves, so too have methods for making tracking on them more difficult. While blockchain analytics and transaction tracing have improved, challenges remain in tracking funds across multiple wallets. Future investigations should be directed toward the enhancement of these forensic technologies to further increase their capability to deanonymize transactions while still protecting legitimate users' privacy. Presumably, this work will also involve cryptography advances and the creation of novel algorithms that could unearth questionable activities even within those blockchain environments that are either highly encrypted or oriented toward privacy.

The researchers pointed out that another promising direction of research is “the use of AI and ML in identifying patterns in illegal activities on blockchain platforms”. AI and ML can detect anomalies indicating money laundering, terrorist financing, and other illicit activities. Akartuna et al. (2022) have suggested that this might be combined with blockchain analytics platforms to offer real-time insights of suspicious behavior.

Future studies should examine privacy and data protection issues arising from AI monitoring in decentralized financial transactions. The balancing of security needs with the safeguarding of the right to privacy will constitute a core challenge in this regard. Another essential domain that research is warranted involves the effectiveness of the regulatory frameworks across different jurisdictions. The current situation indicates a significant gap between countries that enforce strict regulations related to cryptocurrencies and those countries that either keep the regulatory environment lax or non-existent. Studies should investigate how regulatory discrepancies allow criminal organizations to exploit weaker systems. A global regulatory framework is likely needed to combat illegal cryptocurrency use, balancing international financial rules with fostering industry innovation (Akartuna et al., 2022). It does call for collaboration between governments, an international approach, and a contribution in extensive studies from the private sector on the best methods of harmonization across borders.

Future research should focus on social implications and ethical outcomes related to the regulation of virtual currencies. The conflict between the concepts of privacy and security is central to discussions surrounding cryptocurrency, exemplified by the instance of privacy coins such as Monero, which are supported by both proponents of privacy and individuals engaged in illicit activities. Future research should explore the societal impacts of stricter cryptocurrency regulations, especially in regions where digital assets provide a safeguard against hyperinflation,

such as Venezuela and Argentina (Almaqbleh et al., 2023). What is being called for are investigations into the optimal balance in limiting criminal activity and the protection of citizens' financial privacy.Overly strict regulation may stifle innovation and legitimate digital currency use.

The increasing use of cryptocurrencies in terrorist financing is another area that requires closer investigation. While blockchain transparency does enable some degree of tracking in transactions, as conducted in studies by Amiram et al. (2022), the use of mixers, tumblers, and cryptocurrencies focused on privacy complicates these efforts. Future research should explore advanced methods to identify terrorist financing schemes using digital currencies, particularly in lightly regulated jurisdictions. Moreover, case studies of past terrorist activities whose funding sources have used cryptocurrencies, like the Easter bombing in Sri Lanka (Amiram et al., 2022), can give valuable insight into the trends and methods that terrorists use to transfer funds and mask their financial activities.

One avenue of future research in this domain, which has garnered too little attention so far, is how CBDCs can contribute to and advance efforts at the prevention of crime. Central Bank Digital Currencies (CBDCs) offer the benefits of decentralized cryptocurrencies while enabling regulatory oversight to reduce criminal misuse (Mishra and Prasad, 2024). Nonetheless, considerable uncertainties remain concerning the interactions between CBDCs and current financial systems, the regulatory frameworks that would govern them, and the extent to which they might genuinely curtail the use of cryptocurrencies for unlawful activities. CBDC research should, therefore, target the achievement of a balance between privacy and regulation so that a digital currency option is safe, secure, yet misused nowhere.

Moreover, there is a need for further research on the broader economic and social impacts related to cryptocurrency-related crimes. According to Foley et al. (2019), the use of Bitcoin and other cryptocurrencies on darknet markets has been responsible for facilitating the growth in global drug trafficking and other illicit trades. Future research should explore the macroeconomic impacts of cryptocurrency markets, their effect on national economies, and the societal costs associated with their misuse. These investigations should research the resiliency of cryptocurrency markets to law enforcement actions, as has been evidenced by the persistence of illicit markets after law enforcement actions against them, such as what happened with the shutdown of Silk Road.

Future studies should examine the psychological and behavioral factors driving cryptocurrency-based crime. Research by Dhawan and Putnins (2023) reveals that a large portion of participants in pump-and-dump schemes are influenced more by overconfidence and gambling tendencies than

a logical evaluation of possible risks and benefits. Research into the psychological drivers of criminal activity in cryptocurrency markets might provide a better understanding of what keeps people from doing these activities, which, in turn, could help in framing better regulatory mechanisms and law enforcement strategies by factoring in human behavior. Lastly, future research should delve deeper into the role of influencers and social media in promoting cryptocurrency-related criminal activities. Meyer et al. (2024) demonstrated that such influential individuals have increasingly been instrumental in orchestrating a pump-and-dump by capitalizing on their large follower networks. The subtleties of such interactions-from how influencers manipulate the trust of their followers to the influence of social media on the manipulation of cryptocurrency markets-will be important in devising more effective methods of countering this type of financial misconduct. Research should examine how social media and digital currencies interact in financial regulation, considering both regulatory action and public awareness to protect investors. This means that the implications for future studies within the field of cryptocurrency and criminal activities are multi-layered and timely.

There is a growing need for technological solutions to track illicit transactions, coordinated global regulations, and an understanding of the social, psychological, and economic impacts of cryptocurrency crime. Approaches will also need to evolve on the part of researchers, policymakers, and law enforcement methodologies to mitigate misuse without destroying the legitimate potential of cryptocurrencies as they themselves keep changing.

References

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting & Social Change, 179*, 121632.

Alexakis, C., Anselmi, G., & Petrella, G. (2024). Flight to cryptos: Evidence on the use of cryptocurrencies in times of geopolitical tensions. *International Review of Economics and Finance, 89*, 498–523.

Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., & Wallace, D. (2022). An investigative study of links between terrorist attacks and cryptocurrency markets. *Journal of Business Research, 147*, 177–188.

Almaqableh, L., Wallace, D., Pereira, V., Ramiah, V., Wood, G., Veron, J. F., Moosa, I., & Watson, A. (2023). Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can. *International Journal of Information Management, 71*, 102488.

Amiram, D., Jørgensen, B. N., & Rabetti, D. (2022). Coins for bombs: The predictive ability of on-chain transfers for terrorist attacks. *Journal of Accounting Research, 60*(2), 427–472.

Buckley, P. J., Enderwick, P., Hsieh, L., & Shenkar, O. (2024). International business theory and the criminal multinational enterprise. *Journal of World Business, 59*, 101553.

Chiu, J., Davoodalhosseini, S. M., Jiang, J., and Zhu, Y. (2023). *Bank market power and central bank digital currency: Theory and quantitative assessment.* Journal of Political Economy, 131(5), 1213-1239.

Dhawan, A., and Putniņš, T. J. (2024). A new wolf in town? Pump-and-dump manipulation in cryptocurrency markets. *Review of Finance*. (Forthcoming).

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853.

Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: Market analysis and perspectives. *Journal of Industrial and Business Economics, 47*(1), 1–18.

Glenn, N., & Reed, R. (2023). Cryptocurrency, security, and financial intermediation. *Journal of Money, Credit and Banking, 56*(1), 186–202.

Goel, R. K., & Mazhar, U. (2024). Cryptocurrency use and tax collections: Direct and indirect channels of influence. *Journal of Financial Stability, 72*, 101251.

Grobys, K. (2021). When the blockchain does not block: On hackings and uncertainty in the cryptocurrency market. *Quantitative Finance, 21*(8), 1267–1279.

Meyer, E. A., Welpe, I. M., and Sandner, P. (2024). Testing the credibility of crypto influencers: An event study on Bitcoin. *Finance Research Letters, 60*, 104864.

Mishra, B., and Prasad, E. (2024). *A simple model of a central bank digital currency*. *Journal of Financial Stability, 73*, 101282.

Naoum-Sawaya, J., Elhedhli, S., & De Carvalho, P. (2023). Strategic blockchain adoption to deter deceptive counterfeiters. *European Journal of Operational Research, 311*(2), 373–386.

Sapkota, N., and Grobys, K. (2021). Asset market equilibria in cryptocurrency markets: Evidence from a study of privacy and non-privacy coins. *Journal of International Financial Markets, Institutions and Money, 74*, 101402.

Sokolov, K. (2021). Ransomware activity and blockchain congestion. *Journal of Financial Economics, 141*(3), 771–782.

Walker, C. B. (2024). Going mainstream: Cryptocurrency narratives in newspapers. *International Review of Financial Analysis, 94*, 103305.

Appendix

Glossary of Terms

Blockchain: A decentralized, digital ledger that records transactions across multiple computers so that the record cannot be altered retroactively. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

Cryptocurrency: A digital or virtual currency that uses cryptography for security and operates independently of a central authority, relying on blockchain technology to record and verify transactions.

Bitcoin: The first decentralized cryptocurrency, introduced in 2009 by an anonymous entity known as Satoshi Nakamoto. Bitcoin remains the most widely used and valued cryptocurrency.

Altcoin: Any cryptocurrency that is not Bitcoin, including Ethereum, Ripple, Litecoin, and thousands of other digital coins. Altcoins often serve various purposes beyond Bitcoin's initial use case as a decentralized currency.

Mining: The process of validating transactions and adding them to the blockchain. Miners use computational power to solve complex cryptographic problems, which secure the network and, in the case of proof-of-work systems, are rewarded with cryptocurrency.

Proof of Work (PoW): A consensus mechanism used in blockchain networks, notably Bitcoin, that requires miners to solve cryptographic puzzles to validate transactions and create new blocks, providing security through computational difficulty.

Proof of Stake (PoS): An alternative consensus mechanism where validators are chosen based on the amount of cryptocurrency they hold and are willing to "stake" as collateral, reducing the need for intensive computational power.

Smart Contract: Self-executing contracts with terms directly written into code. These are typically hosted on blockchain platforms like Ethereum and execute automatically when certain conditions are met, eliminating intermediaries.

Initial Coin Offering (ICO): A fundraising mechanism where new cryptocurrencies or tokens are sold to investors in exchange for other cryptocurrencies (like Bitcoin or Ethereum) or fiat money, similar to an IPO in the traditional stock market.

Token: A digital asset issued on a blockchain that represents assets, utility, or rights within a specific platform or project. Tokens can be fungible (e.g., ERC-20 tokens) or non-fungible (NFTs).

Stablecoin: A type of cryptocurrency that aims to maintain a stable value, often pegged to a fiat currency (e.g., USD). Examples include Tether (USDT) and USD Coin (USDC).

Wallet: A digital tool (software or hardware) that stores a user's cryptocurrency keys (public and private) and allows them to interact with the blockchain to send and receive digital assets.

Private Key: A cryptographic key that allows a user to access and control their cryptocurrency. It must be kept secure, as anyone with the private key has control over the assets in the associated wallet.

Public Key: A cryptographic key that is shared publicly and acts as an address for receiving cryptocurrency. It is derived from the private key but cannot be used to access the assets without the private key.

Decentralized Finance (DeFi): A financial ecosystem built on blockchain networks that aims to provide financial services (like lending, borrowing, and trading) without intermediaries, using smart contracts instead.

Non-Fungible Token (NFT): A unique digital asset stored on a blockchain that represents ownership of a specific item, artwork, or collectible. NFTs are not interchangeable and are typically used for digital art, gaming, and collectibles.

Fork: A split in a blockchain network due to changes or updates in the protocol. A fork can result in two separate blockchains, such as Bitcoin and Bitcoin Cash, each with distinct rules.

Consensus Mechanism: The method by which a blockchain network reaches an agreement on the state of the ledger. Examples include Proof of Work (PoW) and Proof of Stake (PoS).

Decentralized Autonomous Organization (DAO): An organization governed by smart contracts and decentralized voting rather than traditional management. DAOs operate on the blockchain, with decisions made by token holders or stakeholders.

Exchange: A platform where cryptocurrencies are bought, sold, and traded. Exchanges can be centralized (CEX), where a central authority controls transactions, or decentralized (DEX), where peer-to-peer transactions occur without intermediaries.

Gas Fee: A transaction fee on a blockchain, particularly Ethereum, required to pay for computational resources. Gas fees can vary widely based on network congestion and transaction complexity.

Ledger: A record of financial transactions. In blockchain, the ledger is distributed and immutable, meaning it is spread across multiple nodes and cannot be altered once recorded.

Whale: A term for an individual or entity holding large amounts of cryptocurrency, with the potential to impact the market with their buying or selling actions.

Whitepaper: A detailed document outlining a cryptocurrency project's goals, technology, and roadmap, usually published before an ICO to inform potential investors.

Pump and Dump: A scheme in which a group promotes a cryptocurrency to increase its price artificially (pump) and then sells off their holdings at the peak, leaving others with the loss (dump).

Ransomware: A type of malicious software that encrypts a victim's data, making it inaccessible until a ransom is paid, often in cryptocurrency. Ransomware attacks have surged as cryptocurrencies allow attackers to receive payments anonymously.

Money Laundering: The process of concealing the origins of illegally obtained funds, typically by passing them through complex banking systems or businesses. In the cryptocurrency context, money laundering often involves moving funds through multiple transactions or using mixers and tumblers to obscure the source.

Counterfeit: An unauthorized imitation of goods, currency, or documents, often with the intent to deceive or defraud. In the digital space, blockchain technology is sometimes used to verify the authenticity of items and help prevent the proliferation of counterfeits.

Mixers and Tumblers: Tools used in the cryptocurrency world to obfuscate the origin and destination of funds. Mixers (also known as tumblers) break down cryptocurrency transactions into smaller amounts, mix them with other users' funds, and send them to the intended recipient in a way that makes tracking difficult. These services are often used to increase privacy but can also facilitate money laundering.

Privacy Coins: Cryptocurrencies designed with enhanced privacy features to obscure transaction details, including sender, receiver, and amount. Popular privacy coins include Monero, Zcash, and Dash. These coins are often favored in privacy-sensitive transactions but face scrutiny due to their potential use in illicit activities.

Ethereum: A decentralized blockchain platform, created by Vitalik Buterin, that enables the creation of smart contracts and decentralized applications (dApps). Ether (ETH) is the native cryptocurrency of the Ethereum network, and the platform's flexibility has made it a foundation for decentralized finance (DeFi) and non-fungible tokens (NFTs).

Cold Wallet: A type of cryptocurrency wallet that is not connected to the internet, used for securely storing cryptocurrencies offline to protect them from hacking. Cold wallets can take the form of hardware devices or paper wallets.

Hot Wallet: A cryptocurrency wallet connected to the internet, allowing users quick access to funds for trading or spending. Hot wallets are convenient but are more vulnerable to hacking compared to cold wallets.

FOMO (Fear of Missing Out): A psychological phenomenon that drives investors to buy into assets, including cryptocurrencies, due to the fear of missing out on potential profits. FOMO often leads to impulsive buying, especially in volatile markets like cryptocurrency.

Hash Rate: The total computational power used by a cryptocurrency network to process transactions and mine new coins, typically measured in hashes per second. A higher hash rate generally indicates a more secure network, as it is harder for attackers to control the network.

Immutable: A characteristic of blockchain data that prevents it from being altered once recorded. This immutability provides a reliable, transparent, and tamper-resistant history of transactions on the blockchain.

KYC (Know Your Customer): A process used by financial institutions and exchanges to verify the identity of customers, often required by regulations to prevent money laundering and fraud. In the crypto space, KYC requirements vary, with decentralized exchanges usually less stringent.

Liquidity: The ease with which an asset can be bought or sold without affecting its price. High liquidity means the asset can be easily traded, while low liquidity can lead to price volatility. Cryptocurrency liquidity varies widely across assets and exchanges.

Fiat Currency: Government-issued currency not backed by a physical commodity like gold; its value is instead derived from the trust and stability of the issuing government. Examples include USD, EUR, and JPY. Fiat currencies are often used to purchase cryptocurrencies.

Airdrop: A distribution method where free tokens are sent to users' wallets, often as part of a promotional campaign or to reward early adopters. Airdrops aim to create awareness and incentivize adoption.

Figures

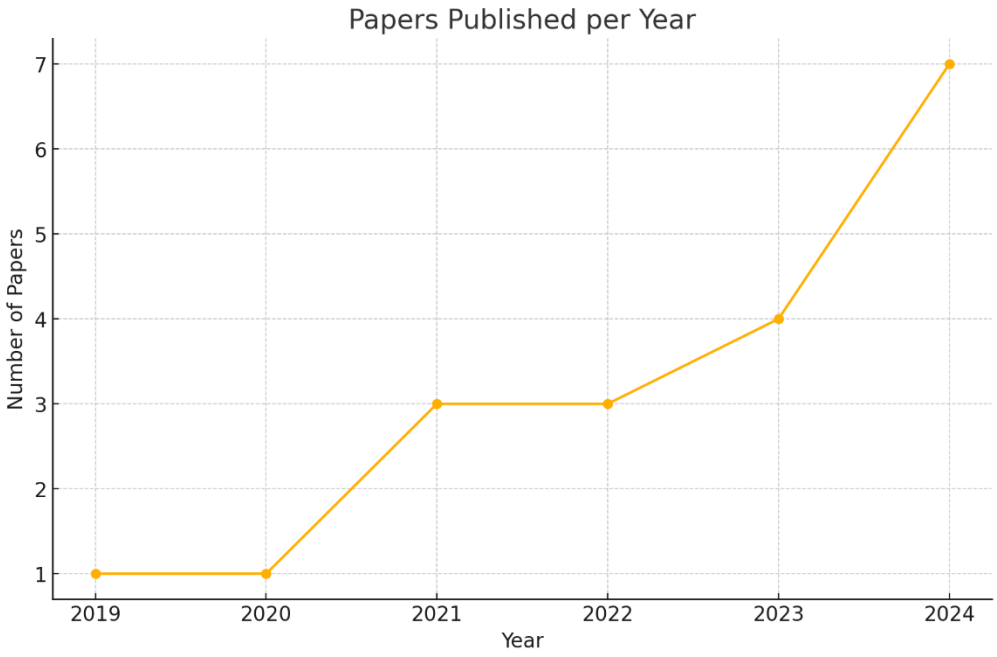


Figure 1—Number of cited papers published in each yearshows the trends in the number of published academic papers relating to cryptocurrency and its involvement in criminal activities between 2019 and 2024. That trend of data clearly shows the steady rise in research output over the years, indicating an increased academic and regulatory interest in the field.

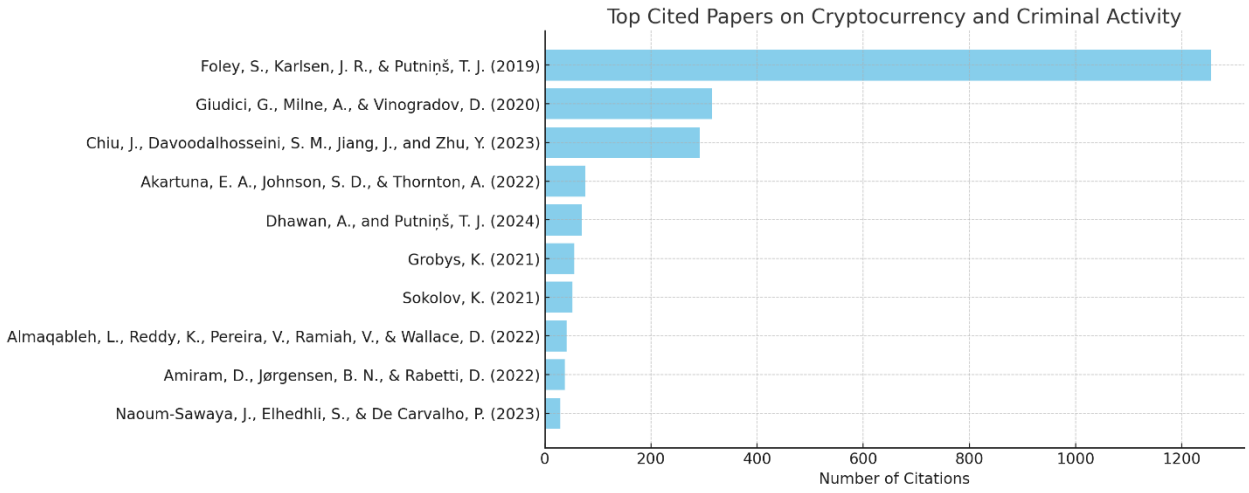


Figure 2—Top Cited Papers on Cryptocurrency and Criminal Activity—shows the ten most-cited papers among the references used in this research. Foley, Karlsen, and Putniņš's (2019) work, with 1253 citations, is the most influential, exploring the extent of illegal activities financed through cryptocurrencies. Following it, Giudici, Milne, and Vinogradov (2020) and Chiu et al. (2023) also have high citation counts, indicating significant contributions to the understanding of cryptocurrency markets and regulatory implications. These highly cited works underscore the foundational role of these studies in shaping the academic discourse on cryptocurrency-related crime and regulation. This analysis shows pivotal studies providing valuable insights and theoretical frameworks that inform ongoing research in cryptocurrency and its intersection with criminal activities.

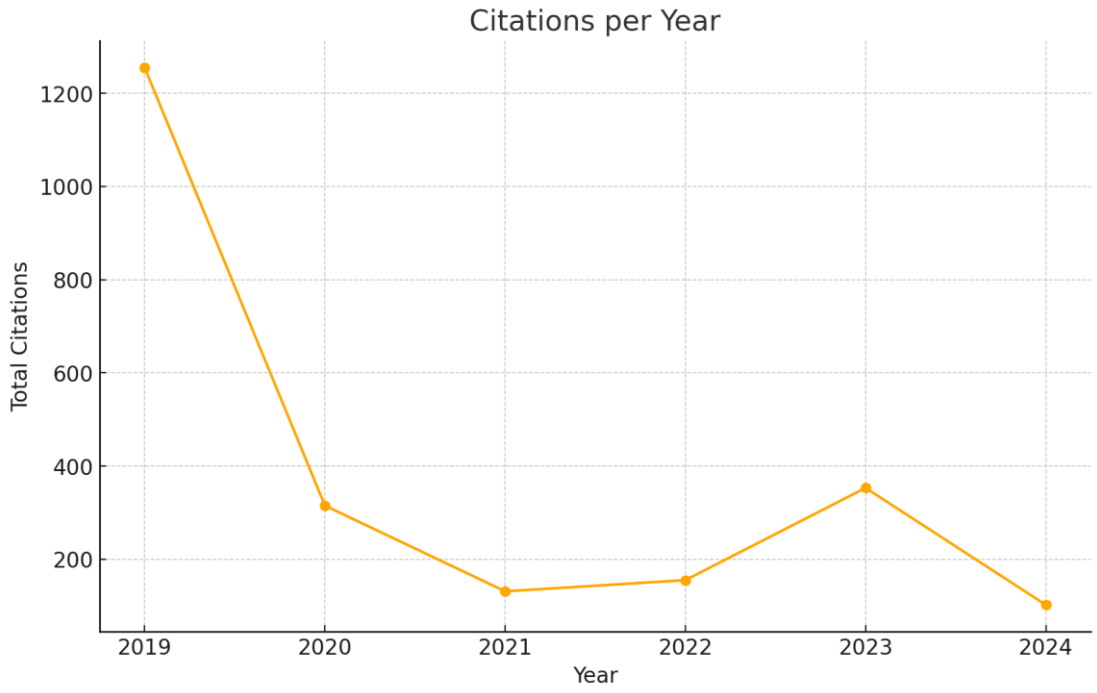


Figure 3—Citations per year—presents the total number of citations per year for research papers referenced in this paper, focusing on cryptocurrency and criminal activity. The sharp peak in 2019 is primarily due to Foley et al.'s highly influential study. The following years show a decline in total citations, with smaller peaks in 2020 and 2023, indicating periodic increases in academic interest as new issues and global events arise.

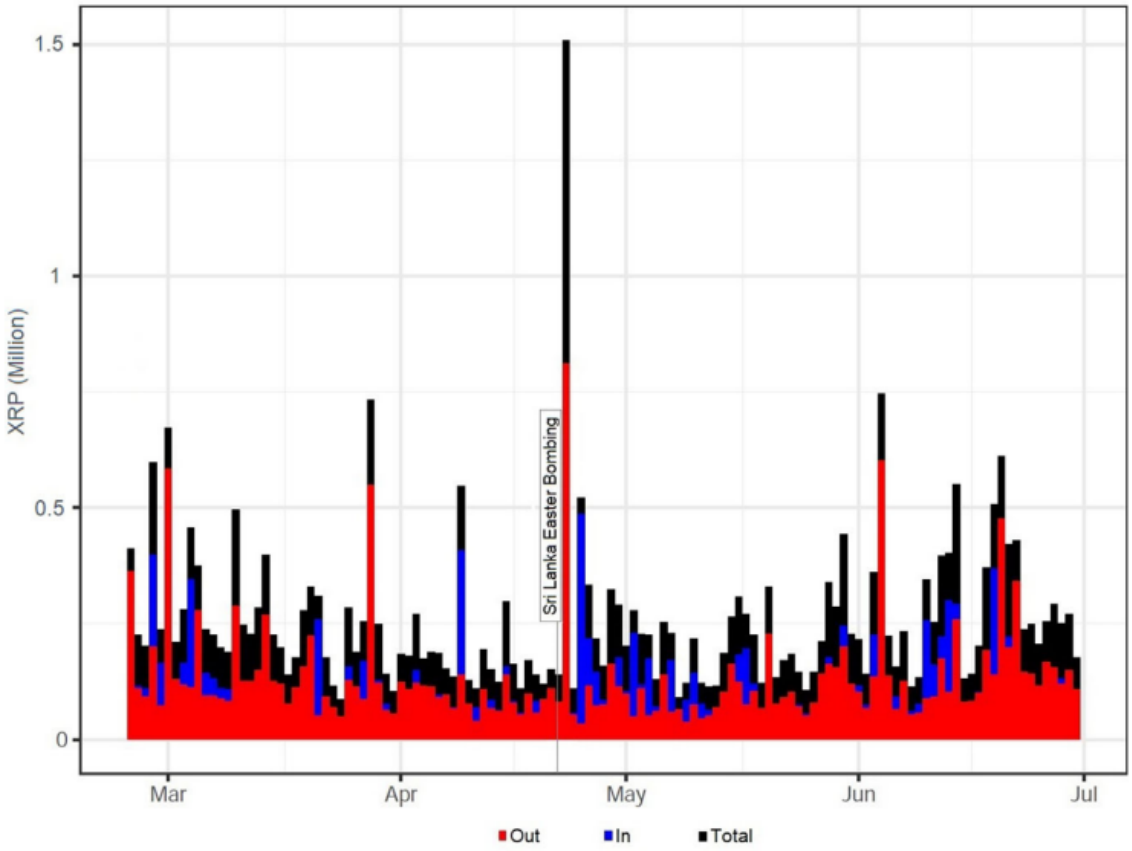


Figure 4—Amiram et al. (2022)— This figure illustrates aggregated daily inbound (blue), outbound (red), and total (black) XRP transfers on the Ripple network's Gateway Ripple Wallet (GRW) during 2019. The transfers are measured in millions of XRP units. Notably, there's a significant spike in transfers, reaching approximately 0.7 million XRP, which occurred in the early hours following the Sri Lanka Easter bombing. This spike may indicate a correlation between the terrorist event and unusual activity within the network, suggesting potential use of cryptocurrency in the aftermath of critical events. This graph helps visualize typical transaction volumes and highlights anomalies that may relate to external events.

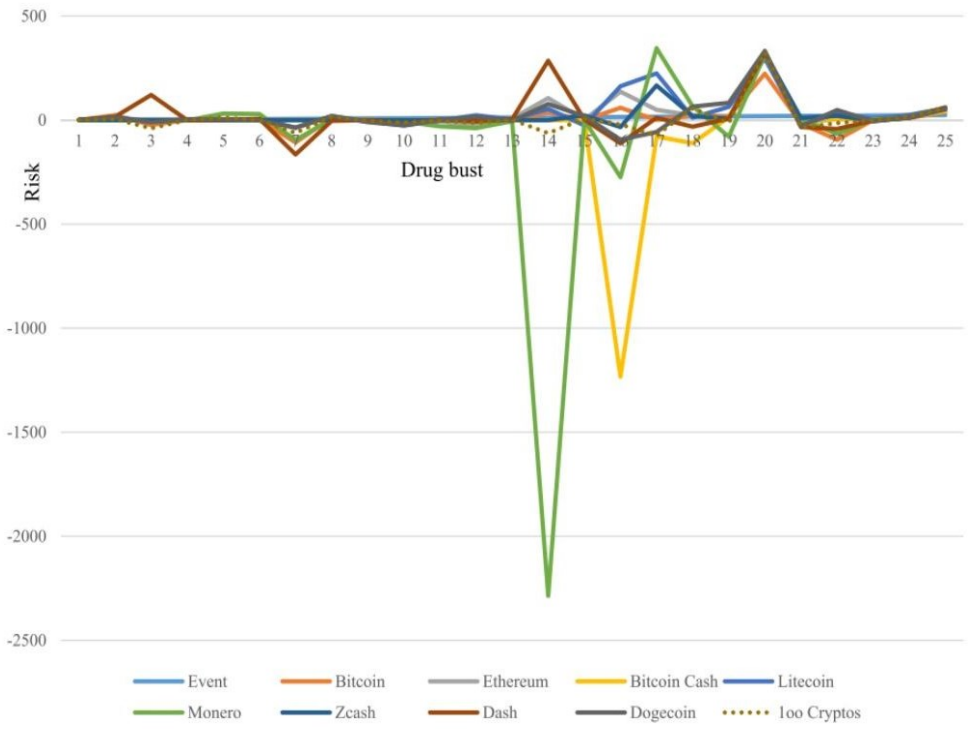


Figure 5—Almaqableh et al. (2022)—In Figure 2 from Almaqableh et al. (2022), the study investigates the impact of news related to drug busts on the short-term systematic risk (measured by beta) of various cryptocurrencies. Each line represents a different cryptocurrency, including Bitcoin, Ethereum, Monero, Zcash, and others, with each peak or dip reflecting the changes in their systematic risk in response to drug bust events. The graph shows notable volatility in certain cryptocurrencies, such as Monero and Zcash, which experience significant risk deviations after a drug bust. These fluctuations suggest that certain cryptocurrencies might be more sensitive to external, crime-related news, likely due to their privacy features or association with illicit markets. This figure highlights the varying degrees of risk impact across different cryptocurrencies, illustrating how real-world events can influence the perceived stability of these digital assets.

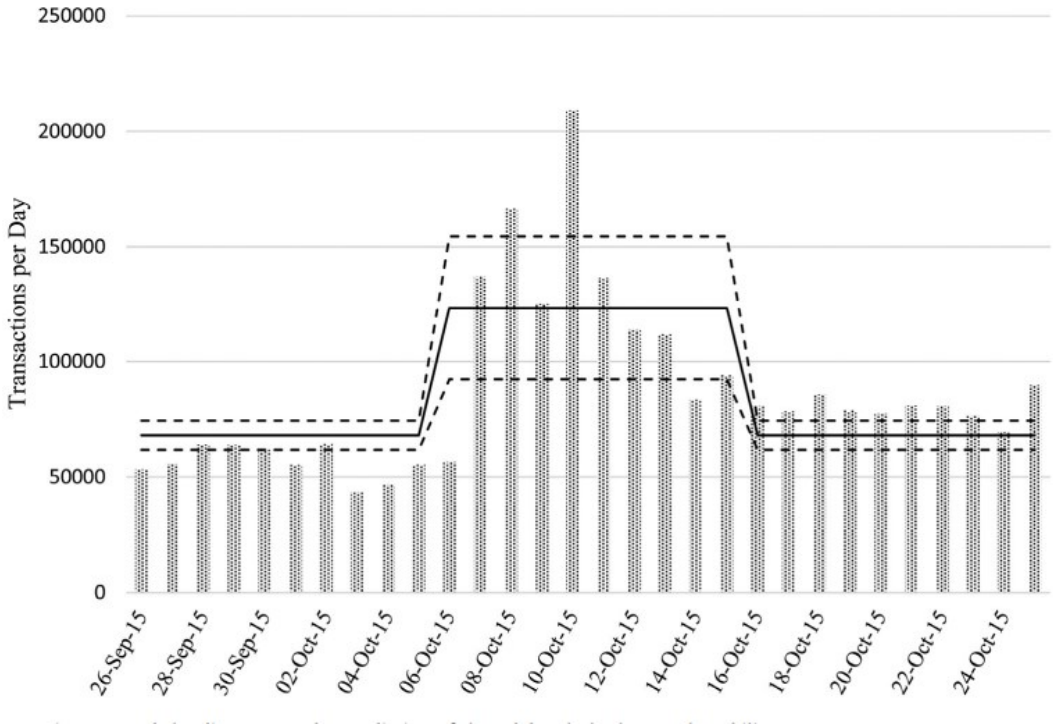


Figure 6—Sokolov (2021)—This figure shows the daily volume of Bitcoin transactions surrounding the discovery and subsequent recovery period of the Adobe Flash Player vulnerability, also known as the Pawn Storm attack. This chart highlights a noticeable spike in transactions shortly after the vulnerability was publicized, with daily transaction counts exceeding typical levels. The solid line represents the average daily transactions, while the dashed lines indicate transaction volume fluctuations around this period. The sharp increase in Bitcoin transactions during this time suggests that the Pawn Storm attack may have influenced users' behavior, possibly due to increased concerns about digital security or a rise in illicit activities leveraging Bitcoin's pseudonymous nature. The pattern also underscores how cybersecurity events can impact cryptocurrency transaction volumes, reflecting shifts in user activity in response to external threats.

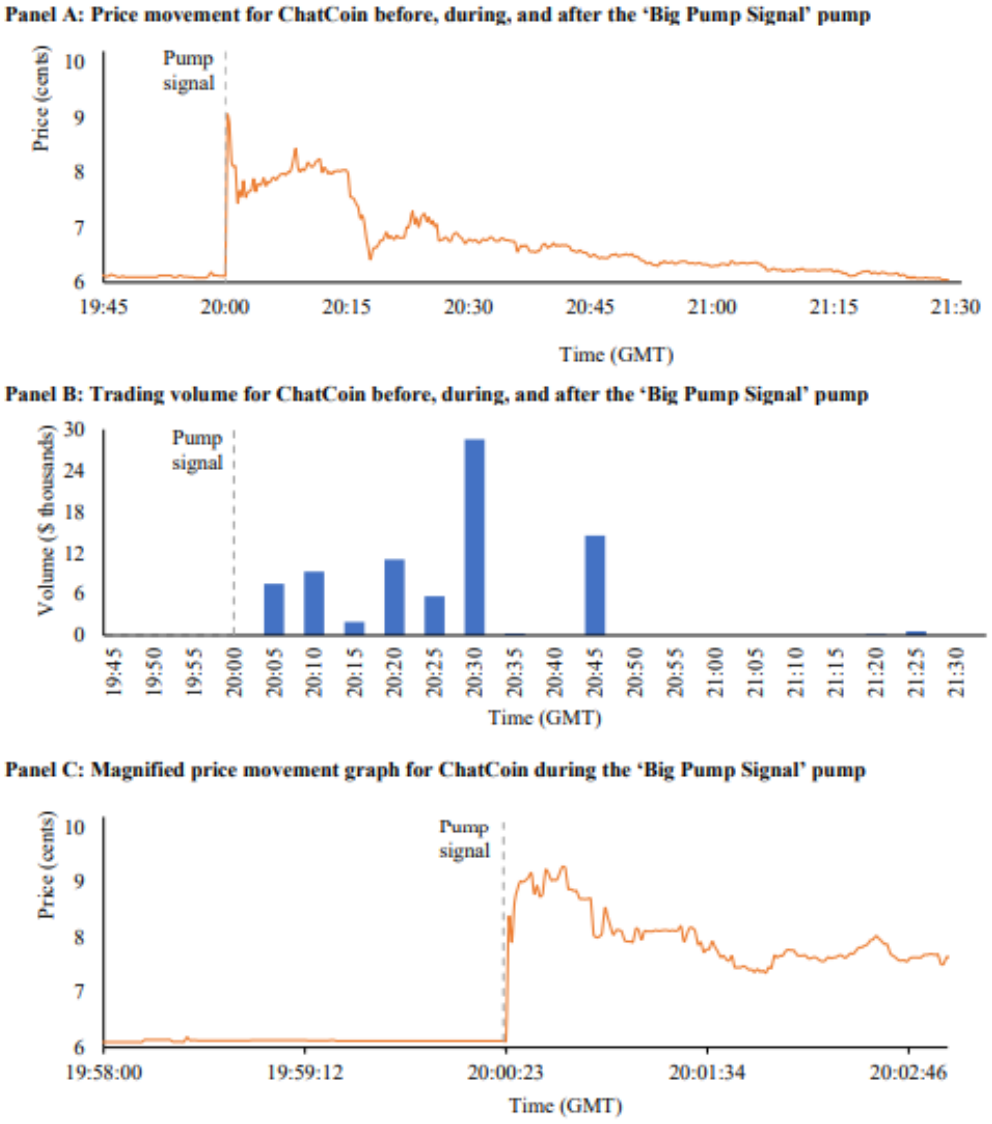


Figure 7—Dhawan and Putnins (2023)—Figure 4 illustrates the effects of a "Big Pump Signal" (BPS) on ChatCoin's price and trading volume, broken down into three panels. Panel A displays the overall price movement of ChatCoin from before the pump signal until after the effects dissipated. The pump signal led to an immediate spike in price, climbing sharply as traders joined the rush. Shortly after the peak, the price began to drop, eventually returning to its pre-pump level, indicating a brief, artificial inflation due to the pump. Panel B shows the trading volume for ChatCoin across the same timeframe. This panel highlights the surge in transaction volume that coincided with the pump signal. Initially low, the volume increased dramatically when the pump started, reaching a peak shortly after, then gradually declining as the price fell. This pattern reflects

typical pump-and-dump behavior, where high volume accompanies the price peak before subsiding. Panel C provides a magnified view of the immediate price fluctuations during the pump signal. This closer look captures the rapid rise and fall in price, emphasizing how quickly the pump influenced ChatCoin's value and how fast it reverted to normal once the hype subsided.

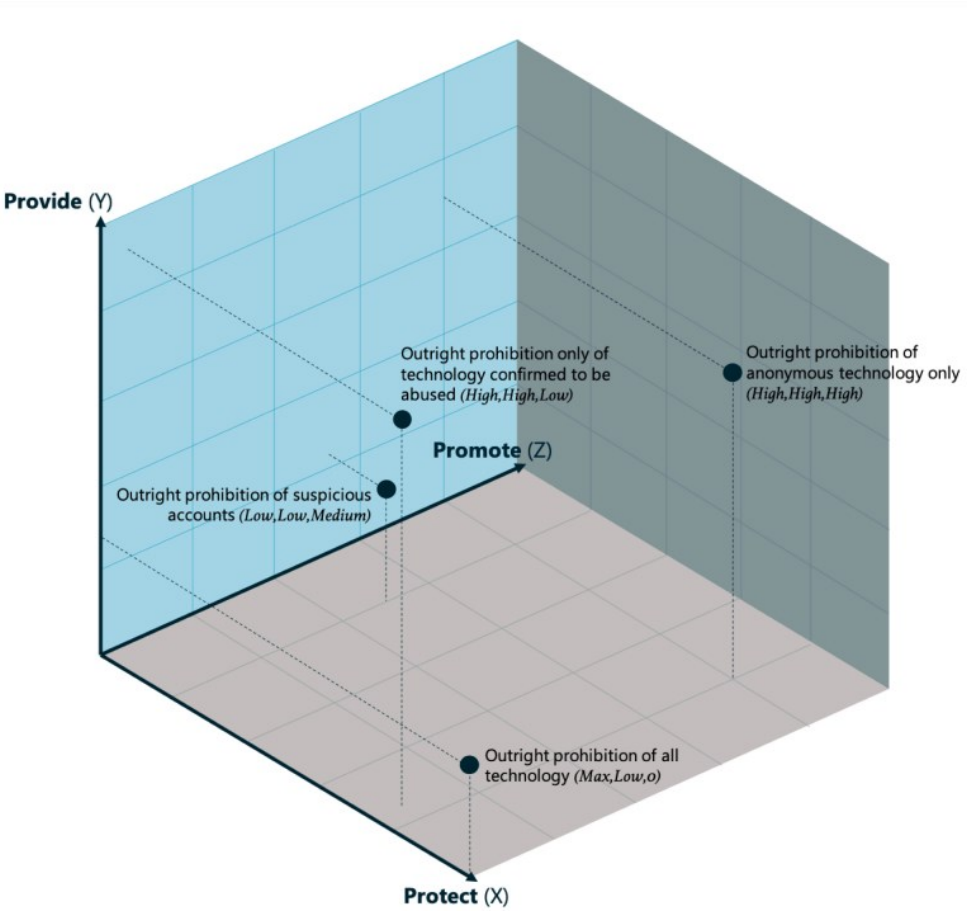


Figure 8—Mishra and Prasad (2024)—This is a 3P model to illustrate various "outright prohibition" strategies in regulating potentially harmful or anonymous technologies. The model is structured as a 3D cube with three axes, each representing a different dimension of policy implementation. The Protect (X-axis) indicates the level of protection sought by restricting technology use. Moving along this axis represents stricter protective measures, ranging from selective restrictions on suspicious accounts to the complete prohibition of all technology. The Provide (Y-axis) shows the extent to which technologies are allowed or provided within the system, differentiating between allowing technologies with no confirmed abuse to limiting those that are only slightly suspicious. The Promote (Z-axis) represents the promotion or acceptance of

technology in society, with points along this axis ranging from low promotion (e.g., outright prohibition for high-risk, anonymous technology) to high promotion (allowing technology if there is no confirmed abuse). Each point within the cube represents a distinct regulatory stance. For instance, the bottom point at (Max, Low, 0) suggests an outright prohibition of all technology to maximize protection, with no provision or promotion. The point at (High, High, High) represents a more flexible strategy, such as prohibiting only anonymous technology, which balances allowing some technology use while prohibiting high-risk aspects. Other points suggest intermediate levels, such as prohibiting only technology confirmed to be abused or prohibiting only suspicious accounts.

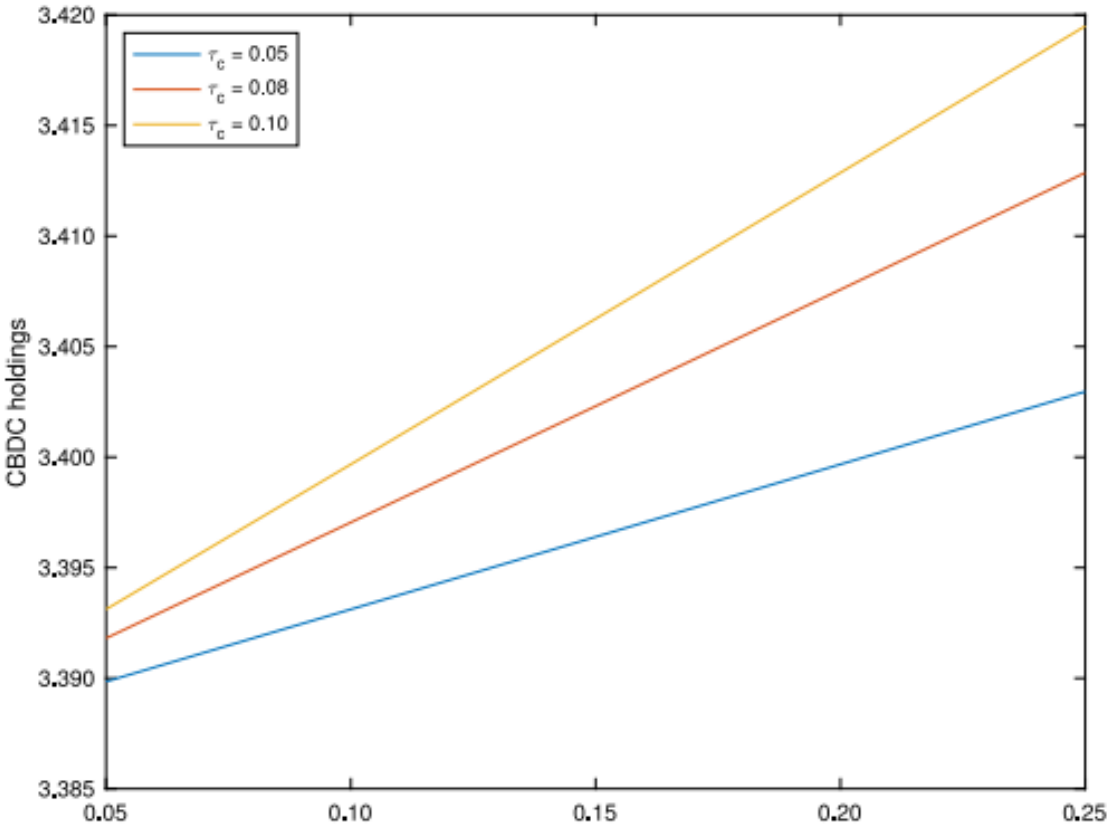


Figure 9—Mishra and Prasad (2024)—This figure plots CBDC holdings as a function of the probability that cash holdings exceed threshold level, where the tax on cash holdings exceeding threshold is 5% (blue line), 8% (red line), and 10% (yellow line).