UNIVERSITY OF GDAŃSK—FACULTY OF ECONOMICS

Shobhit Navani

Field of science: Social Sciences

Scientific discipline: Economics and Finance

Cryptocurrency at the crossroads: navigating regulation, cybercrime, and market dynamics in the digital age

PhD dissertation prepared under supervision of

Prof. Dr. Giuseppe T. Cirella, *PhD*, *Hab*

Sopot, 2024

"The greatest glory in living lies is not in never falling, but in rising every time we fall."

Nelson Mandela

STRESZCZENIE

Kryptowaluty na rozdrożu: regulacje, cyberprzestępczość i dynamika rynku w erze cyfrowej

Shobhit Navani

Niniejsza dysertacja bada złożone powiązania między regulacjami dotyczącymi kryptowalut a cyberprzestępczością, analizując wyzwania i możliwości związane z walutami cyfrowymi w coraz bardziej zintegrowanym globalnym systemie finansowym. Struktura pracy obejmuje trzy rozdziały, które zgłębiają ciemne strony kryptowalut, analizują głośny upadek FTX oraz badają wpływ nastrojów w mediach społecznościowych na trendy na rynku kryptowalut.

Rozdział 1 zawiera szczegółowy przegląd literatury, podkreślając podwójną rolę kryptowalut jako przełomowego narzędzia finansowego oraz jako środka ułatwiającego nielegalne działania, takie jak pranie pieniędzy, finansowanie terroryzmu i ataki ransomware. Omówiono znaczenie darknetu w umożliwianiu nielegalnych transakcji oraz oceniono globalne podejścia regulacyjne w krajach takich jak Stany Zjednoczone, Chiny, Polska i Szwajcaria. Rozdział uwypukla trudności związane z międzynarodową współpracą w zakresie tworzenia adaptacyjnych ram regulacyjnych i kończy się wnioskami dotyczącymi pojawiających się zagrożeń oraz strategii równoważenia innowacji z bezpieczeństwem.

Rozdział 2 analizuje meteoryczny wzrost i dramatyczny upadek FTX, niegdyś wiodącej giełdy kryptowalutowej, przez pryzmat jej założyciela, Sama Bankmana-Frieda. Omówiono rozwój FTX, strategie marketingowe na dużą skalę, systemowe uchybienia w zarządzaniu oraz ostateczne bankructwo w obliczu zarzutów o oszustwa i niewłaściwe zarządzanie. Rozdział ten przedstawia szersze implikacje dla branży kryptowalutowej, podkreślając podatność na zagrożenia i pilną potrzebę zaostrzenia nadzoru i wprowadzenia zasad odpowiedzialności.

Rozdział 3 bada zależności między nastrojami w mediach społecznościowych a zachowaniami na rynku kryptowalut, koncentrując się na głównych walutach, takich jak Bitcoin, Ethereum i Monero. Analizuje także reakcje społeczne na skandal związany z FTX, uwypuklając etyczne i regulacyjne braki. Przy użyciu zaawansowanych technik analizy nastrojów, w tym modelu Bidirectional Encoder Representations from Transformers, rozdział ten pokazuje, jak wydarzenia, takie jak ataki hakerskie i ogłoszenia regulacyjne, wpływają na

krótkoterminowe trendy rynkowe. Wskazano ograniczenia, takie jak uproszczona kategoryzacja nastrojów i ograniczenia dostępu do danych, oraz zaproponowano przyszłe kierunki badań, obejmujące analizę wieloplatformową i integrację z tradycyjnymi wskaźnikami finansowymi.

Praca ta wnosi istotny wkład w rozwój wiedzy na temat kryptowalut, analizując wyzwania regulacyjne, podatności systemowe i dynamikę rynku. Podkreśla potrzebę skoordynowanych działań globalnych na rzecz ustanowienia solidnych, adaptacyjnych ram, które zapewnią bezpieczeństwo finansowe, wspierając jednocześnie innowacje w erze cyfrowej.

Słowa kluczowe: kryptowaluta; cyberprzestępczość; darknet; FTX; pranie pieniędzy; regulacja; Sam Bankman-Fried

ABSTRACT

Cryptocurrency at the crossroads: navigating regulation, cybercrime, and market dynamics in the digital age

Shobhit Navani

This dissertation explores the intricate intersection of cryptocurrency regulation and cybercrime, addressing the challenges and opportunities presented by digital currencies within an interconnected global financial system. Structured into three chapters, it investigates cryptocurrency's darker dimensions, analyzes the notorious collapse of FTX, and examines the impact of social media sentiment on cryptocurrency market trends.

Chapter 1 provides a thorough literature review, highlighting cryptocurrency's dual role as a groundbreaking financial tool and an enabler of illicit activities like money laundering, terrorism financing, and ransomware attacks. It delves into the darknet's significance in facilitating illegal transactions and evaluates global regulatory approaches across nations such as the United States, China, Poland, and Switzerland. The chapter underscores the challenges of international cooperation in crafting adaptive regulatory frameworks and concludes with insights into emerging threats and strategies to balance innovation with security.

Chapter 2 examines the meteoric rise and dramatic fall of FTX, a once-leading cryptocurrency exchange, through the lens of its founder, Sam Bankman-Fried. It explores FTX's growth, high-profile marketing campaigns, systemic governance failures, and eventual collapse amid allegations of fraud and mismanagement. Broader implications for the cryptocurrency industry are discussed, highlighting vulnerabilities and the pressing need for stricter oversight and accountability.

Chapter 3 investigates the interplay between social media sentiment and cryptocurrency market behavior, focusing on major currencies like Bitcoin, Ethereum, and Monero. It also analyzes public reactions to the FTX scandal, highlighting ethical and regulatory deficiencies. Using advanced sentiment analysis, including a Bidirectional Encoder Representations from Transformers model, the chapter demonstrates how events such as hacks and regulatory announcements influence short-term market trends. Limitations such as simplified sentiment categorization and data access restrictions are acknowledged, with recommendations for future research into cross-platform analysis and integration with financial metrics.

This dissertation significantly contributes to cryptocurrency scholarship by addressing regulatory challenges, systemic vulnerabilities, and market dynamics. It calls for coordinated global efforts to establish robust, adaptive frameworks that safeguard financial security while fostering innovation in the digital age.

Keywords: cryptocurrency; cybercrime; darknet; FTX; money laundering; regulation; Sam Bankman-Fried

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to Professor Giuseppe T. Cirella from the University of Gdansk, whose expertise, understanding, and patience, added considerably to my PhD experience. His unwavering support and guidance have been the key ingredients in steering my academic work in the right direction. Throughout my PhD journey, the world faced unprecedented challenges, including a global pandemic and a war in neighboring Ukraine. During these turbulent times, his mentorship exceeded anything I could have hoped for. He has been not only an outstanding academic advisor but also an invaluable mentor in my personal life. His high standards and unwavering belief in my abilities have inspired me to excel and strive for excellence in my research.

I am also immensely thankful for the presence of my beloved daughter, Anika Navani, in my life. Although she may not be physically present before me, she is always in my heart, inspiring me with her unwavering love. Her memory has been a constant source of strength and motivation throughout this journey. Her laughter and joy, though distant, have been my guiding light in times of challenge and introspection. During my PhD journey, I experienced the profound and heartbreaking loss of my father. His absence created a void in my life that no words can adequately express. Yet, his steadfast belief in my abilities and his unwavering support, even in his final days, became the guiding light that gave me the strength to persevere through the most challenging moments of my academic pursuit.

Lastly, I want to thank myself for not giving up, even in the face of countless challenges. I am deeply grateful for the strength, resilience, and determination I found within myself to push through every obstacle and keep believing in my abilities. It hasn't been an easy journey, but I'm proud of my growth and the strength I've cultivated to keep moving forward during this long journey.

LIST OF PUBLICATIONS

Journal Articles

[1] **Navani, S.**, & Cirella, G. T. (2024). Cybercrimes in the Cryptocurrency Domain: Identifying Types, Understanding Motives and Techniques, and Exploring Future Directions for Technology and Regulation. *Journal of Geography, Politics and Society*, *14*(2), 43. https://doi.org/10.26881/jpgs.2024.2.01

Points MEiN: 40

Data Availability Statement

The supplementary material for this study (Supplementary Data—S1, S2, S3, and S4) is available in the Figshare online repository. The materials can be accessed via the following repository link: https://doi.org/10.6084/m9.figshare.27075646.v1

Author Contributions Breakdown

Shobhit Navani: ***95%***

The doctoral candidate took the lead in conceptualizing the study, carefully defining its scope and identifying key research questions to guide the investigation. He developed the hypotheses, ensuring they were well-aligned with the research objectives and the emerging trends in cryptocurrency-related cybercrimes. The research methodology was meticulously designed, selecting appropriate data collection and analysis approaches, incorporating cutting-edge tools such as blockchain analysis software and statistical techniques to examine cybercrime activities within the cryptocurrency domain. Validation of these methods was a crucial step, ensuring the rigor and reliability of the analytical techniques used. In terms of software, the researcher expertly applied various data analysis tools, such as statistical software and blockchain monitoring technologies, to examine the data comprehensively. The formal analysis was conducted in depth, where the researcher interpreted the findings and drew well-supported conclusions based on the evidence gathered. Furthermore, he led the investigation phase, gathering relevant data, conducting an extensive review of existing literature, and identifying trends and patterns in cybercriminal behavior related to cryptocurrencies. Managing resources, the researcher efficiently coordinated the access to datasets, research materials, and necessary software

tools for the analysis. Data curation also played a significant role in the study, as the researcher organized and managed the data in a manner that ensured it was suitable for thorough analysis and effective dissemination. As the primary author, he was responsible for drafting the original manuscript, articulating the research findings in a coherent and comprehensive manner. Lastly, he took charge of the review and editing process, making substantial revisions to enhance the manuscript's clarity, flow, and overall quality.

Giuseppe T. Cirella: ***5%***

The supervisor played a key role in overseeing the manuscript's development, providing valuable guidance throughout the research process to ensure that the work aligned with the overarching goals and academic standards. He offered critical input during the review and editing phase, ensuring the manuscript met the required scholarly criteria and contributed to enhancing the quality of the final work. While he did not directly participate in the creation of visualizations, he supported the design of diagrams, figures, and tables by suggesting appropriate representations of the data. In terms of project administration, he coordinated tasks, managed timelines, and ensured that all deliverables were met efficiently. Furthermore, he took an active role in the funding acquisition process, helping identify potential sources of financial support and contributing to the preparation of funding proposals. Additionally, he was responsible for submitting the manuscript and coordinating with the journal's editor-in-chief to facilitate the publication process.

[2] **Navani, S.**, & Cirella, G.T. (2024). Deciphering Sentiment Dynamics in the Cryptocurrency Market: Insights from X Posts. *International Journal of Blockchain and Cryptocurrencies*, In Press. https://doi.org/10.1504/IJBC.2024.10068544

Points MEiN: 0

Author Contributions Breakdown

Shobhit Navani: ***90%***

The doctoral candidate took the lead for this paper and was responsible for conceptualizing the study, which included defining the research objectives, identifying key hypotheses, and framing the scope of the investigation. He took charge of formal analysis, utilizing statistical and computational methods to analyze the data and derive meaningful insights. He also led the application of software tools for data processing, employing

advanced platforms and algorithms tailored to sentiment analysis in the cryptocurrency domain. Additionally, he spearheaded the investigative efforts, collecting and examining data, reviewing relevant literature, and synthesizing findings. Resource coordination, including securing and organizing datasets and tools required for the research, was also undertaken by him. The original draft of the manuscript, encompassing the initial narrative of the findings, was prepared under his authorship.

Moreover, while both authors collaborated on the methodology, the doctoral candidate was primarily responsible for designing the research framework and implementing robust techniques to achieve the study's objectives. Validation efforts were also shared, ensuring the reliability and credibility of the analysis, though the doctoral candidate drove the process. Data curation, including organizing, structuring, and archiving the dataset for analysis, was another area of joint effort, with the doctoral candidate completing most of the tasks. The review and editing of the manuscript were collaborative, with both authors refining the draft to enhance its clarity, coherence, and adherence to academic standards.

Giuseppe T. Cirella: ***10%***

The supervisor contributed to visualization, providing guidance on creating graphs, charts, and visual representations that effectively illustrated the study's results. He also supervised the entire research process, offering critical oversight and ensuring alignment with scholarly and research objectives. Project administration was another area of his contribution, coordinating tasks, maintaining timelines, and ensuring that deliverables were met. Lastly, the supervisor took on the critical role of submitting the manuscript and liaising with the journal's editor-in-chief to facilitate the publication process. The supervisor provided oversight and support, ensuring the study aligned with academic and publication requirements.

LIST OF ACRONYMS

3AC	Three Arrows Capital
AI	artificial intelligence
AML	Anti-Money Laundering
AMM	automated market makers
API	Application Programming Interface
BERT	Bidirectional Encoder Representations from Transformers
BNB	Binance Coin
BNS	Blockchain Name Service
BSA	Bank Secrecy Act
BTC	Bitcoin
CaaS	Crypto-as-a-Service
CEA	Center for Effective Altruism
CEX	centralized exchange
CFTC	Commodity Futures Trading Commission
CISA	Cybersecurity and Infrastructure Security Agency
CZ	Changpeng Zhao (Founder of Binance)
DeFi	decentralized finance
DEX	decentralized exchange
DNS	Domain Name System
DOJ	United States Department of Justice
EA	effective altruism
ENS	Ethereum Name Service
ETFs	exchange-traded funds
ETH	Ethereum
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FTT	FTX Token
H	hypothesis
ICOs	Initial Coin Offerings
IPO	Initial Public Offering
IRS	Internal Revenue Service

ISIS	Islamic State of Iraq and Syria
KYC	Know-Your-Customer
LTC	Litecoin
MIH	Miami International Holdings
MIT	Massachusetts Institute of Technology
MTG	Mind The Gap
NLP	Natural Language Processing
NFTs	non-fungible tokens
PACs	Political Action Committees
PBoC	People's Bank of China
RBI	Reserve Bank of India
RQ	research question
SBF	Sam Bankman-Fried (Founder of FTX)
SEC	Securities and Exchange Commission
SOL	Solana
SVM	support vector machine
UNODC	United Nations Office on Drugs and Crime
USDC	USD Coin
USDT	USD Tether
VGX	Voyager Token
XMR	Monero
XRP	Ripple

TABLE OF CONTENTS

INTRODUCTION

Research Background and Knowledge Gap

Cryptocurrency, a digital or virtual form of currency that relies on blockchain technology, has fundamentally reshaped the global financial landscape. Its decentralized nature, offering transparency and efficiency in financial transactions, has led to widespread adoption and the promise of economic innovation. However, the rapid expansion of cryptocurrency markets has also introduced significant challenges, particularly concerning security and regulation. While blockchain technology enables secure, anonymous transactions, it has simultaneously created an environment ripe for cybercrime, including money laundering, fraud, ransomware attacks, and the financing of illegal activities like drug trafficking and terrorism. These emerging threats have raised serious concerns among regulators, law enforcement agencies, and policymakers, who are struggling to keep pace with the rapid evolution of cryptocurrency markets.

Despite efforts to regulate the cryptocurrency industry, existing frameworks remain fragmented and insufficient to address the full range of risks associated with digital currencies. While certain countries, such as the United States, China, and India, have implemented regulations aimed at mitigating cryptocurrency-related cybercrime, these measures often fall short due to the global, decentralized nature of the cryptocurrency market. Furthermore, the rise of decentralized finance (DeFi) platforms and the increasing use of the darknet for illicit cryptocurrency transactions complicates the ability of authorities to enforce laws effectively. Although various regulatory approaches have been proposed, the debate remains unresolved regarding the most effective global framework to combat cryptocurrency-related crime and ensure financial security.

This dissertation seeks to fill the knowledge gap by providing an in-depth analysis of the role cryptocurrency plays in facilitating cybercrime and the challenges faced by global regulators. It examines the intersections of cryptocurrency, cybercrime, and regulation, highlighting the critical need for coordinated international efforts to address these issues. By exploring the evolution of cryptocurrency, the growing prevalence of cryptocurrency-related crimes, and the effectiveness of current regulatory responses, this research aims to contribute to the development of a more comprehensive regulatory framework that can safeguard the benefits of digital currencies while mitigating their risks.

Aim of the Dissertation, Research Questions, and Hypotheses

The primary aim of this dissertation was to explore and analyze the critical intersections between cryptocurrency regulation, cybercrime, and market dynamics in the digital era. This research aims to assess how the rapid evolution of cryptocurrency has contributed to the rise of cybercrime and the global security risks associated with these developments. Specifically, the dissertation will analyze the influence of cryptocurrency on illicit activities, the role of decentralized finance platforms in enabling these crimes, and the strategies employed by different countries to regulate digital currencies. By evaluating the effectiveness of these regulatory measures, the study seeks to offer recommendations for strengthening global frameworks to ensure financial security while supporting innovation.

The dissertation is guided by nine research questions (*RQ*s), which are organized across three chapters as follows:

Chapter 1: Literature Review: Exploring the Dark Side of Cryptocurrency

RQ1: How has the evolution of cryptocurrency contributed to the rise of cybercrime, and what key challenges does it present for global security?

RQ2: What role does the darknet play in facilitating illicit cryptocurrency transactions, and how can its impact be mitigated through regulatory measures?

RQ3: How effective are current regulatory approaches in combating cryptocurrency-related cybercrime, and what improvements are needed to ensure global financial security?

Chapter 2: FTX: Unravelling the Saga of Crypto Scam

RQ4: What were the key factors contributing to the rise of FTX as a leading cryptocurrency exchange, and how did its strategic innovations influence the broader market dynamics?

RQ5: How did FTX's marketing strategy, including sports and celebrity endorsements, impact its public image and attract investors?

RQ6: What ethical dilemmas and governance failures within FTX and its affiliate, Alameda Research, contributed to the platform's collapse and the subsequent legal repercussions?

Chapter 3: Deciphering Sentiment Dynamics in the Cryptocurrency Market: Insights from X Posts

RQ7: How does sentiment expressed on X (formerly Twitter) influence cryptocurrency market trends and investor behavior?

RQ8: To what extent can real-time social media sentiment analysis predict short-term price movements in major cryptocurrencies like Bitcoin and Ethereum?

RQ9: What role do specific cryptocurrency-related events (e.g., hacks, regulatory news) play in shaping public sentiment and market dynamics on social media platforms?

This dissertation is grounded in the following eight hypotheses (*H*):

H1: The rise of cryptocurrency has directly facilitated the growth of cybercrime, with decentralized finance platforms providing new avenues for illicit activities such as money laundering and drug trafficking.

H2: Stronger and more coordinated international cryptocurrency regulations will significantly reduce the use of cryptocurrencies in illegal activities, including ransomware attacks and terrorism financing.

H3: Cryptocurrency-related cybercrimes are more prevalent in countries with less comprehensive regulatory frameworks, with the darknet acting as a major facilitator of these illegal transactions.

H4: FTX's marketing and public relations strategies, particularly its high-profile celebrity endorsements, were effective in creating a positive public image, which masked underlying operational and governance issues that contributed to its downfall.

H5: The legal and ethical challenges faced by FTX, including allegations of fraud and mismanagement, significantly influenced investor confidence and contributed to a market-wide decline in cryptocurrency trust and value.

H6: Public sentiment on X, specifically related to regulatory news or market interventions (e.g., announcements by figures like Gary Gensler), has a significant influence on the trading volumes and volatility of major cryptocurrencies such as Bitcoin and Ethereum.

H7: Real-time sentiment analysis of social media data, particularly during significant events such as the FTX crash and controversies surrounding Sam Bankman-Fried (SBF), can provide actionable insights for investors, enabling them to make more informed decisions and mitigate investment risks in volatile cryptocurrency markets.

H8: Cryptocurrency market trends exhibit a correlation with fluctuations in sentiment on social media platforms like X, with negative sentiment being linked to price declines and positive sentiment correlating with price increases.

Structure of the Dissertation

This dissertation is organized into three core chapters, each addressing a pivotal aspect of cryptocurrency regulation and its intersection with cybercrime. At the end of each chapter, key research questions and hypotheses relevant to the chapter are examined to draw conclusions, assess the findings, and offer insights into potential future strategies and solutions.

Chapter 1 "Literature Review: Exploring the Dark Side of Cryptocurrency" provides a comprehensive review of the complex and rapidly evolving cryptocurrency landscape, focusing on both its potential for innovation and its darker implications. The chapter begins by tracing the evolution of cryptocurrency, examining its rapid expansion, decentralized nature, and the associated risks. It explores the critical intersection between cryptocurrency and cybercrime, detailing how digital currencies have facilitated criminal activities such as money laundering, drug trafficking, and terrorism. A thorough analysis of the darknet, as a key hub for illicit cryptocurrency transactions, underscores its role in the global illicit economy.

The chapter also delves into emerging threats, such as cryptocurrency ransomware, and assesses the economic consequences of these evolving cybercrimes. The regulatory landscape is analyzed in detail, with a focus on the approaches taken by various countries, including the United States, China, India, Poland, and Switzerland. This comparison provides valuable insights into the diverse regulatory strategies aimed at mitigating the risks associated with digital currencies. Challenges in crafting effective regulations are explored, emphasizing the need for international cooperation and adaptive frameworks to address cryptocurrency-based crimes.

Moreover, the chapter introduces a methodological framework for categorizing cybercrimes linked to cryptocurrency, offering insights into the geographical and topological patterns of these activities. It critiques existing regulatory measures, advocating for a more integrated and global approach to addressing the dark side of cryptocurrency. The chapter concludes with recommendations for future research and regulatory strategies, with the goal of fostering a safer and more secure environment for cryptocurrency innovation, while mitigating its risks.

This foundation sets the stage for Chapter 2, which offers an in-depth examination of the FTX scandal—a real-world case study highlighting governance failures and systemic vulnerabilities in the cryptocurrency ecosystem.

Chapter 2 "FTX: Unraveling the Saga of Crypto Scam" investigates the rise and fall of FTX, one of the most notorious cryptocurrency exchanges, founded by SBF. It begins by

detailing SBF's early involvement in the cryptocurrency sector and the establishment of his trading firm, Alameda Research. The ethical dilemmas faced by the firm as it ventured into the crypto market are discussed, followed by an examination of FTX's founding and its early innovations. The chapter explores how FTX rapidly expanded during the 2021 crypto bull run, including its key acquisitions, such as Blockfolio and LedgerX, which solidified its place in the industry.

The chapter further explores FTX's marketing strategies, which included high-profile celebrity endorsements and sports partnerships, playing a significant role in the exchange's public image and investor appeal. However, the focus then shifts to the dramatic collapse of FTX, triggered by security breaches, regulatory scrutiny, and allegations of fraud and financial mismanagement. The legal fallout, including the indictment and conviction of SBF, is analyzed through sentiment analysis of social media reactions. This chapter underscores the ethical and governance failures that led to FTX's downfall, highlighting the need for enhanced regulatory oversight and greater accountability in the cryptocurrency market.

Chapter 3 "Deciphering Sentiment Dynamics in the Cryptocurrency Market: Insights from X Posts" explores the relationship between social media sentiment—specifically on X—and cryptocurrency market dynamics. By leveraging advanced sentiment analysis, the chapter examines how real-time public opinion on social media platforms can influence cryptocurrency markets. The chapter employs a BERT-based sentiment analysis model to assess how social media sentiment can predict short-term price movements of major cryptocurrencies like Bitcoin and Ethereum.

Additionally, the chapter details the methodologies used in sentiment analysis, including data collection, random sampling, and validation techniques, with an emphasis on using Python and advanced Natural Language Processing (NLP) tools to ensure robust and accurate results. Sentiments are categorized into positive, neutral, and negative posts, providing a nuanced view of public sentiment regarding cryptocurrencies and events such as hacks or regulatory announcements. The performance of the Bidirectional Encoder Representations from Transformers (BERT) model is compared with traditional sentiment analysis models like logistic regression and support vector machines (SVM), showing its superior accuracy in capturing sentiment-driven market dynamics.

Despite the model's success, the study acknowledges certain limitations, such as data access restrictions and the challenge of oversimplifying complex sentiments into three categories. The chapter also addresses the temporal constraints of conducting research during a holiday period, which may not fully reflect the dynamic nature of the cryptocurrency market. It

concludes with suggestions for future research, including cross-platform sentiment analysis and integration with traditional financial models, to deepen understanding of sentiment-driven market trends. This analysis contributes valuable insights into cryptocurrency market behavior, offering practical knowledge for investors and industry stakeholders.

In conclusion, this dissertation aims to contribute significantly to the existing literature on cryptocurrency regulation, focusing on its role in facilitating cybercrime, the limitations of current regulatory frameworks, and the urgent need for coordinated global efforts. By examining the complex relationship between cryptocurrency and illicit activities, this work emphasizes the critical importance of developing adaptive, forward-thinking regulatory measures to ensure financial security in the digital age.

CHAPTER 1

LITERATURE REVIEW: EXPLORING THE DARK SIDE OF CRYPTOCURRENCY

1.1. The Evolution and Challenges of Cryptocurrency

The bankruptcy and fraud at FTX, a Bahamas-based cryptocurrency exchange led by Sam Bankman-Fried, have underscored the societal risks tied to cryptocurrencies. Cryptography, the foundational technology behind cryptocurrencies, originates from ancient methods of concealing information. The term itself derives from the Greek words *kryptos* (hidden) and *graphein* (writing) (Aggarwal & Jaiswal, 2011). Modern cryptography laid the groundwork for Bitcoin (BTC), the first cryptocurrency, introduced in 2008 by the pseudonymous creator Satoshi Nakamoto. In a seminal white paper, Nakamoto outlined the vision for a peer-to-peer electronic cash system designed to enable direct transactions without relying on financial institutions (Nakamoto, 2009). This concept was further detailed in the document commonly referred to as the Bitcoin Manifesto, which described a fully decentralized electronic money system allowing online payments to flow directly between users, bypassing traditional financial intermediaries.

Cryptocurrencies, including BTC, Ethereum (ETH), Ripple (XRP), Litecoin (LTC), and Monero (XMR), operate on decentralized systems powered by blockchain technology (Agarwal et al., 2024; Bajra et al., 2024). This technology ensures secure and transparent peer-to-peer transactions while eliminating the need for intermediaries such as banks. These digital assets rely on cryptography to safeguard transactions and regulate the creation of new units, functioning independently of central banks or governments (Dyntu & Dykyi, 2019; Phugger, 2021; Taylor et al., 2021). With thousands of cryptocurrencies now in circulation, Bitcoin remains the most widely recognized, while Ethereum is renowned for its smart contract capabilities (Bajra et al., 2024; Mthembu et al., 2022), Ripple for enabling fast cross-border payments (Grasselli & Lipton, 2021), and Monero for prioritizing transaction privacy (S. Lee et al., 2019; Möser et al., 2018; Sovbetov, 2018). Others, such as Litecoin and many emerging digital tokens, continue to expand the diversity of the cryptocurrency landscape (Sovbetov, 2018).

One of the defining characteristics of cryptocurrencies is their reliance on a decentralized structure where transactions are verified and recorded on a public ledger known

as the blockchain (Y. Chen et al., 2020; Schneider, 2019). This ledger is maintained by a distributed network of computers worldwide, ensuring transparency and security. Cryptocurrencies typically follow limited supply models to prevent inflation, with Bitcoin being a prime example. Its finite supply of 21 million coins has contributed to its reputation as "digital gold" and a hedge against inflation (dos Reis et al., 2024; Liao et al., 2016). Additionally, the use of advanced encryption techniques and complex mathematical algorithms further enhances the reliability and integrity of these digital assets (Liao et al., 2016).

The appeal of cryptocurrencies lies in their ability to facilitate fast, low-cost transactions while providing users with an alternative to traditional fiat currencies. They offer financial inclusion to individuals without access to conventional banking systems, enabling seamless cross-border payments and secure storage of value (Gohwong, 2019; Manjula et al., 2022). Cryptocurrencies also appeal to investors seeking diversification in their portfolios, as well as to tech enthusiasts intrigued by blockchain's innovative potential.

However, the very features that make cryptocurrencies attractive—decentralization, pseudonymity, and lack of regulation—also present significant risks. These assets are often used for illicit activities, including scams, fraud, and cybercrime. The absence of a centralized authority and the pseudonymous nature of transactions make it challenging to trace and prevent criminal activities (Kerr et al., 2023; Kutera, 2022; Reddy & Minaar, 2018). High price volatility adds another layer of complexity, making cryptocurrencies both an exciting and precarious investment.

As cryptocurrencies gain traction globally, their dual nature as tools for financial empowerment and potential misuse underscores the need for balanced regulation. Governments and regulatory bodies face the challenge of fostering innovation while mitigating risks. Addressing these concerns will be crucial to shaping the future of digital finance and ensuring cryptocurrencies achieve their transformative potential responsibly.

Governments worldwide have adopted varied and cautious approaches to regulating cryptocurrencies, reflecting the distinct priorities of their national contexts. In some countries, like Japan and South Korea, the focus has been on fostering technological innovation and capturing the economic potential of blockchain and digital assets. These nations have implemented clear regulatory frameworks aimed at supporting the cryptocurrency industry while maintaining oversight (Rieckmann & Stuchtey, 2023; Șcheau et al., 2020). Conversely, other countries, such as China and India, emphasize mitigating risks like fraud, money laundering, and tax evasion, leading to stricter regulations or outright bans (Mubarak & Manjunath, 2021; Phugger, 2021; Rajagopal, 2020; Xie, 2019). These divergent strategies

highlight the challenges of balancing innovation with risk management in the evolving digital finance landscape.

In the United States, regulatory oversight is fragmented across multiple agencies, each addressing different aspects of cryptocurrency. The Securities and Exchange Commission (SEC) treats certain cryptocurrencies as securities and enforces regulations accordingly. The Commodity Futures Trading Commission (CFTC) classifies cryptocurrencies as commodities and regulates their derivatives markets. Meanwhile, the Financial Crimes Enforcement Network (FinCEN) enforces anti-money laundering policies for cryptocurrency exchanges and other entities handling digital assets (ICE, 2020; Kayani & Hasan, 2024; Watters, 2023; Widhiyanti et al., 2023). This multi-agency approach reflects the complexity of integrating cryptocurrencies into existing legal and financial systems.

Globally, governments face the shared challenge of navigating the trade-offs between protecting consumers, preventing illicit activities, and fostering innovation. Countries like the United Kingdom and Singapore are exploring comprehensive frameworks that aim to balance these priorities, while others remain cautious, responding incrementally to the rapid developments in cryptocurrency technology (Kamps & Kleinberg, 2018; Rueckert, 2019).

As the cryptocurrency market continues to grow and evolve, the need for coherent and balanced global standards becomes increasingly evident. Such frameworks will be critical for addressing challenges like market volatility, fraud, and cross-border financial crime, ultimately fostering trust and stability in the digital economy. By harmonizing regulations and promoting international collaboration, policymakers can create an environment that encourages innovation while mitigating the risks inherent in this transformative technology.

1.2. Unveiling Cybercrime and the Need for Global Cryptocurrency Regulation

Specifically, this chapter explores the intricate relationship between cryptocurrency and cybercrime, addressing the challenges and risks posed by the decentralized nature of digital currencies. While cryptocurrencies have unlocked tremendous potential for technological innovation, they have also given rise to a darker side, fraught with misuse. As the adoption of cryptocurrencies expands globally, the anonymity and pseudonymity associated with these digital assets make them attractive to illicit actors, enabling crimes such as money laundering, organized crime, and other illegal activities (Bayramova et al., 2021; Brown, 2016; Kethineni & Cao, 2020; Nazzari, 2023; Paquet-Clouston et al., 2019).

To gain a deeper understanding of these challenges, a systematic review was conducted, focusing on cybercrime within the cryptocurrency sector. The selected studies were carefully analyzed and categorized to provide a comprehensive overview of the various types of cybercrimes associated with cryptocurrencies, the methods employed by cybercriminals, and the regulatory actions taken by governments and institutions. Notably, the review excludes common frauds related to Initial Coin Offerings (ICO), such as exit scams and pump-and-dump schemes, and instead concentrates on more complex cybercrimes that exploit the distinctive characteristics of cryptocurrencies.

Similar to other major technological advancements in history, cryptocurrencies can be either a force for societal progress or a tool for exploitation. The anonymity of cryptocurrencies, particularly within the darknet, has facilitated their use in a range of illicit activities, including drug trafficking, terrorism, money laundering, and the distribution of child sexual exploitation material (CSEM) (Rudesill et al., 2015). The coding process of the review seeks to identify specific criminal activities, synthesize findings related to regulatory responses, and categorize publications by geographic location, publication year, and publisher.

1.3. Methodology for Analyzing Cybercrime in Cryptocurrency

The methodology for conducting a comprehensive systematic literature review on the intersection of cryptocurrency and cybercrime involved an extensive search across various electronic journal databases. These included Bing, Directory of Open Access Journals, Google, Google Scholar, Publons, ResearchGate, Scopus, Semantic Scholar, and Web of Science. In the search process, specific English language keywords, such as “bitcoin + criminality,” “bitcoin + international regulations,” “bitcoin + volatility,” “cryptocurrency + child pornography,” “cryptocurrency + organized crimes,” “cryptocurrency + regulations,” “cryptocurrency + scams,” “cybercrime,” “darknet,” “drug trafficking,” “illegal weapon sales,” “money laundering,” “crypto ransomware,” “rug pull,” “terrorism,” and “wallet hack,” were systematically employed. After compiling the literature, a systematic analysis was conducted to identify publications presenting specific findings on the darknet, cybercrime, crypto ransomware, organized crime, hacking, computer viruses, and regulatory law related to cryptocurrency. This analysis was conducted using strategic and critical reading methods (Matarese, 2013; Renear & Palmer, 2009).

In the initial literature review, over 4,000 articles, reviews, and grey literature were identified. To refine the focus, articles published before 2008 were excluded, as cryptocurrency

was in its infancy prior to the launch of Bitcoin. After this initial filtering process, 845 peer-reviewed publications related to cryptocurrency and cybercrime were selected. Further in-depth reviews narrowed this down to 228 publications, including books, journal articles, and technical reports. This study relies on desk research, gathering and analyzing data from diverse secondary sources and cryptocurrency-related websites. After filtering these sources, the findings were compiled and discussed to provide insights into the nature and extent of cybercrime associated with cryptocurrencies. Since the review is based on secondary data, it does not employ a specific sample; however, careful attention is given to ensuring the relevance and currency of the data collected. The findings are expected to offer valuable insights into the contemporary landscape of cybercrime within the cryptocurrency sector, contributing significantly to the development of more effective preventive measures against such crimes in the future.

1.4. Exploring the Dark Side of Cryptocurrency

1.4.1 Geographic and Timeline Results

In the analysis, the literature underscores the worldwide significance of cybercrime and cryptocurrency as a central focus of research. Notably, leading research endeavors from the US highlight the nation's influential role in shaping discussions and advancements in this sphere (DOJ, 2015; Dupont & Holt, 2022; ICE, 2020; Kayani & Hasan, 2024; Raman et al., 2023; Widhiyanti et al., 2023). Ukraine and Russia, interestingly for example, have emerged as prominent hubs for cybercrimes linked to cryptocurrency, revealing a thriving crypto landscape predating current geopolitical events and indicating significant interest and investment among Ukrainians and Russians (Cong et al., 2022; Dyntu & Dykyi, 2019; Ivaniuk & Banakh, 2020; Pushkarev et al., 2020; Turchyn & Turchyn, 2021).

European research also provides substantial contributions, offering diverse perspectives and regulatory frameworks that enhance our understanding of cryptocurrency and crime. Topics such as regulatory approaches, adoption rates, and technological innovations are extensively explored, shedding light on the nuanced complexities of the cryptocurrency landscape (Godlove, 2014; Lapuh Bele, 2021; Nazzari & Riccardi, 2024). Similarly, contributions from Asia, including regions like China, India, and Indonesia, offer invaluable insights into adoption trends, blockchain technology developments, and regulatory challenges specific to the region (Chuan & O'Leary, 2021; Mubarak & Manjunath, 2021; Piazza, 2017).

North and Central America, with their vibrant cryptocurrency ecosystems, contribute essential research on market trends, regulatory frameworks, and the impact of cryptocurrency on traditional financial systems (Bhaskar et al., 2019; Biswas, 2018; Kayani & Hasan, 2024; Kethineni et al., 2018). Contributions from other continents, such as South America (Pop & Colonescu, 2021; Pushkarev et al., 2020; Virga, 2015), Africa (Interpol, 2020; Reddy, 2020; Reddy et al., 2020; Sanusi & Dickason-Koekemoer, 2022), and Australia (Australian Home Affairs, 2022; Dupont & Holt, 2022; Morelato et al., 2020), enrich our understanding by exploring diverse cultural, economic, and regulatory contexts (Figure 1). This amalgamation of research from various continents underscores the global nature of cryptocurrency and highlights its profound implications over illicit activities via finance and technology. This global perspective fosters a comprehensive understanding of the evolving cryptocurrency landscape, facilitating informed decision-making and policy development in the field.

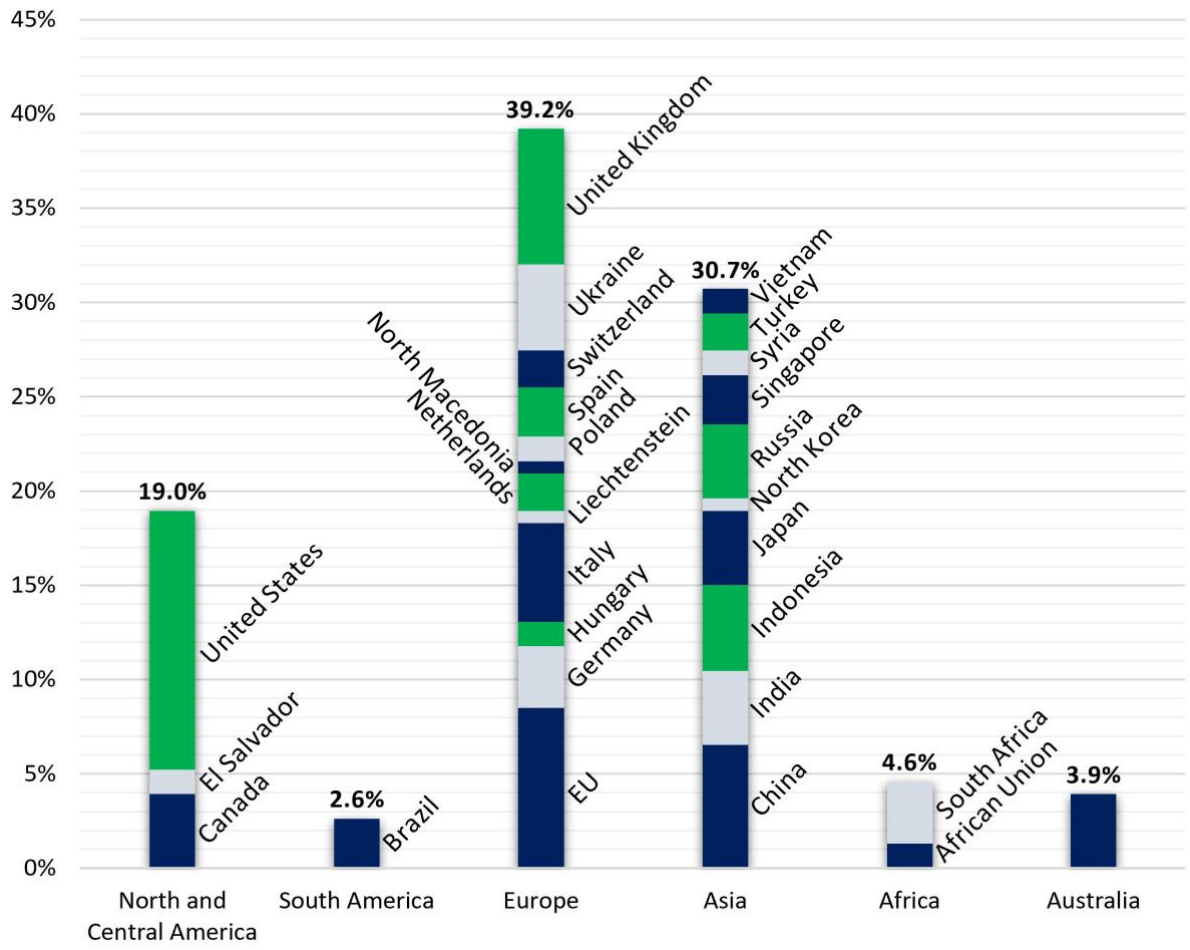

Figure 1. Geographic distribution of the reviewed literature by continent.

In recognition of the need to disseminate credible information amid the rapid pace of technological advancements and emerging threats, an examination of the literature based on publishing houses and sources was conducted. This approach aimed to enhance the reliability and credibility of the reviewed literature. Among the prominent publishers, Springer emerged as the leading contributor, reflecting its commitment to advancing scholarly discourse in the field. Significant contributions were also made by Elsevier, Emerald, Frontiers, IEEE, MDPI, Oxford University Press, Routledge, SAGE, and Taylor and Francis, highlighting their crucial role in fostering research dissemination. Notably, nearly half of the reviewed sources (97) originated from a variety of publishing sources, including university press publishers, governmental reports, and specialized cryptocurrency websites. This diverse range of sources enriched the research by providing multiple perspectives and insights from various sectors and disciplines.

The literature reviewed, covering the period from 2008 to 2024, revealed distinct patterns in the publication trends related to cryptocurrency and cybercrime. One of the most notable observations was the sharp increase in the volume of sources published in recent years, indicating a heightened focus on these issues within the research community. A particularly significant surge occurred in 2020, which emerged as the year with the highest number of reviewed sources, totaling 43 publications. This marked increase in scholarly interest was closely followed by 33 sources in 2022, 30 in 2021, 28 in 2023, and 26 in 2024, as illustrated in Figure 2. These figures reflect a clear trend of growing attention towards the intersection of cryptocurrency and cybercrime, especially in the context of emerging technological challenges and the expanding use of digital currencies in society. This surge in publications highlights a variety of factors driving the increased scholarly interest. The rapid development of cryptocurrency technologies, coupled with their increasing integration into various economic and social systems, has raised new concerns about their potential misuse (Del Monaco, 2020; Rieckmann & Stuchtey, 2023). The anonymity and decentralization inherent in cryptocurrencies have made them attractive to cybercriminals, contributing to the rise of illicit activities such as money laundering, ransomware attacks, and fraud within the cryptocurrency ecosystem. As these digital currencies become more deeply embedded in global financial systems, the need for research to understand and address the cybercrime risks associated with them has grown significantly.

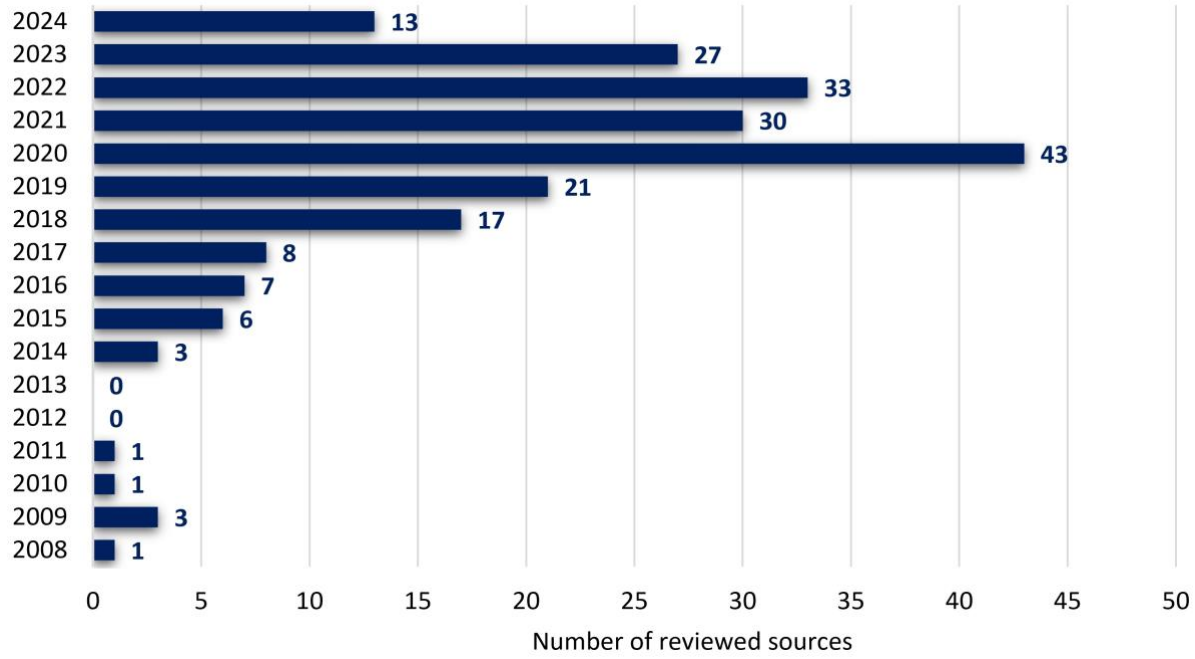

Figure 2. Publication timeline of the reviewed literature.

Furthermore, the increasing prevalence of high-profile cybercrime cases involving cryptocurrencies, such as ransomware attacks and darknet transactions, has underscored the urgency of tackling these challenges (Almomani, 2023; Moore & Rid, 2016; Nialldawson, 2015; Rudesill et al., 2015). Researchers, policymakers, and regulatory bodies are increasingly recognizing the need to develop robust frameworks to address these issues, which is reflected in the growing volume of academic work on the subject. The sharp rise in publications in recent years serves as a testament to the pressing need for continued exploration of the vulnerabilities and threats posed by cryptocurrency-based cybercrime, as well as the strategies required to mitigate these risks effectively.

As a result, the rapid technological advancements in the cryptocurrency space, coupled with the expansion of cybercrime tactics exploiting these technologies, necessitate a comprehensive and ongoing investigation into the evolving landscape of digital crime. As cryptocurrencies continue to play a more prominent role in global economies, the need for effective regulatory measures and a deeper understanding of cybercrime in this context remains paramount.

Moreover, the proliferation of research in this area suggests a concerted effort to understand and combat the evolving threats posed by cybercriminal activities leveraging cryptocurrencies (Dudani et al., 2023; Patsakis et al., 2023; Volevodz, 2024). As these digital assets continue to gain traction and prominence in global economies, it becomes imperative to

stay abreast of the latest developments and challenges in safeguarding against illicit activities in the digital realm (Bahamazava & Nanda, 2022; dos Reis et al., 2024; Kayani & Hasan, 2024). Overall, the upward trajectory of research publications in cybercrime and cryptocurrency reflects a proactive response to the dynamic landscape of digital finance (Auer & Tercero-Lucas, 2022; Kayani & Hasan, 2024) and underscores the collective commitment to fostering a safer and more secure digital environment.

1.4.2 Topological Findings

A comprehensive analysis of the literature uncovered the prevalent types of cybercrimes associated with cryptocurrencies, along with their distinguishing characteristics, in accordance with predefined criteria. A broad array of scholarly sources was utilized to identify key themes and emerging trends related to crimes involving digital currencies, providing in-depth insights into the complexities of these illicit activities and the diverse regulatory responses enacted by governments worldwide. The typological findings were systematically organized into key categories: the darknet, cybercrime, crypto ransomware, and organized crime. Within the organized crime category, further subdivisions were made to include specific criminal activities, including drug trafficking, terrorism, money laundering, and CSAM. In cases where a specific cryptocurrency was not mentioned, it was classified under Bitcoin and cryptocurrencies more broadly. A detailed comparison of centralized and decentralized cryptocurrency exchanges was also included, highlighting their key differences, advantages, and disadvantages.

1.4.2.1. Centralized Cryptocurrency Exchange

A centralized cryptocurrency exchange (CEX) functions as a trading platform where cryptocurrencies are exchanged under the control of a central authority. Acting as intermediaries between buyers and sellers, these exchanges oversee the order book, user accounts, and security protocols. Notable examples include Binance (www.binance.com), Kraken (www.kraken.com), and Coinbase (www.coinbase.com). Figure 3 illustrates the CEX Binance platform.

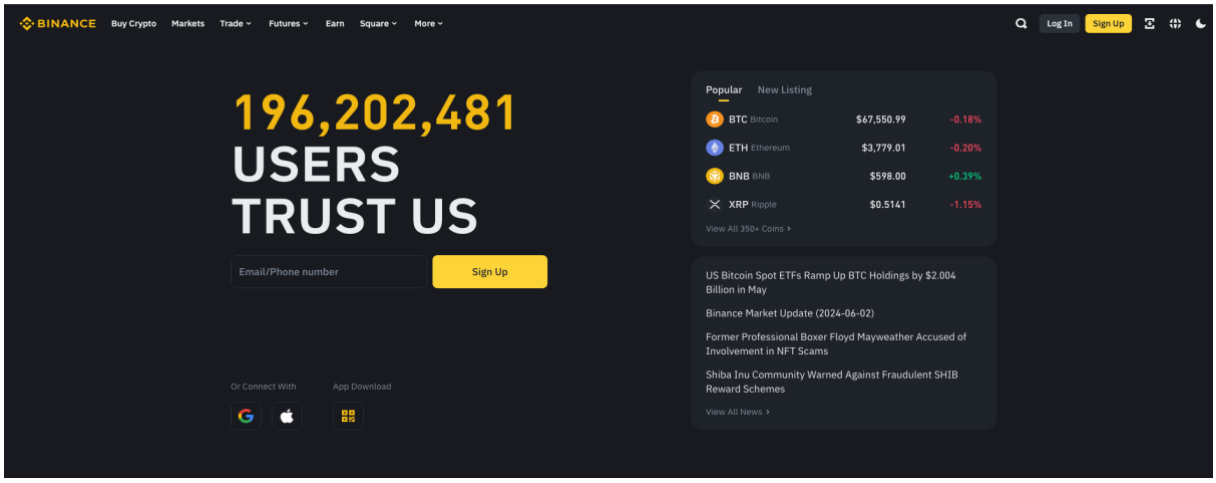

Figure 3. CEX: Binance platform.

Source: Binance website, 2024.

It should be noted that CEX offer several advantages that make them appealing to users. One major benefit is custody, as CEX platforms hold users' funds in their own wallets, taking responsibility for the security and management of assets. Additionally, these exchanges typically require users to complete Anti-Money Laundering (AML) and Know-Your-Customer (KYC) processes, helping to prevent illegal activities like money laundering and fraud. CEX platforms are also known for their ease of use, providing user-friendly interfaces, customer support, and features such as simple registration, portfolio management, and trading tools, making them suitable for beginners. Liquidity is another advantage, as centralized exchanges tend to have higher liquidity due to a larger user base and higher trading volumes, allowing users to execute large trades quickly without significantly impacting the market price (Clements, 2021; Ghalwesh et al., 2020; Phugger, 2021). Security measures on CEX platforms, such as encryption, multi-factor authentication, and cold storage of funds, add an extra layer of protection, although these platforms remain targets for hackers due to the large amounts of assets stored. CEX platforms typically charge fees for trading, deposits, withdrawals, and other services, which can vary and are generally higher compared to decentralized exchanges. However, they often offer excellent customer support, and users can easily reach out via email, chat, website, or phone. CEX platforms also provide a wide range of services, including futures trading, staking, lending, and more.

On the other hand, there are notable disadvantages to using centralized exchanges. One of the main drawbacks is the lack of control over private keys, as users entrust the exchange with their assets. The requirement for KYC, while beneficial for regulatory compliance, can be a privacy concern for users who may not wish to share personal information. Furthermore, CEX

platforms are vulnerable to security risks, as they are a prime target for hackers due to the centralized storage of assets. If a centralized exchange is hacked, users' funds could be compromised.

1.4.2.2. Decentralized Cryptocurrency Exchange

A decentralized cryptocurrency exchange (DEX) operates independently of a central authority. Trades are conducted directly between users (peer-to-peer) through an automated process, typically utilizing smart contracts on a blockchain. Examples of DEX platforms include Uniswap (https://uniswap.org/), UniDex (https://www.unidex.exchange/), and RocketX (https://www.rocketx.exchange/). Figure 4 illustrates the DEX Uniswap platform.

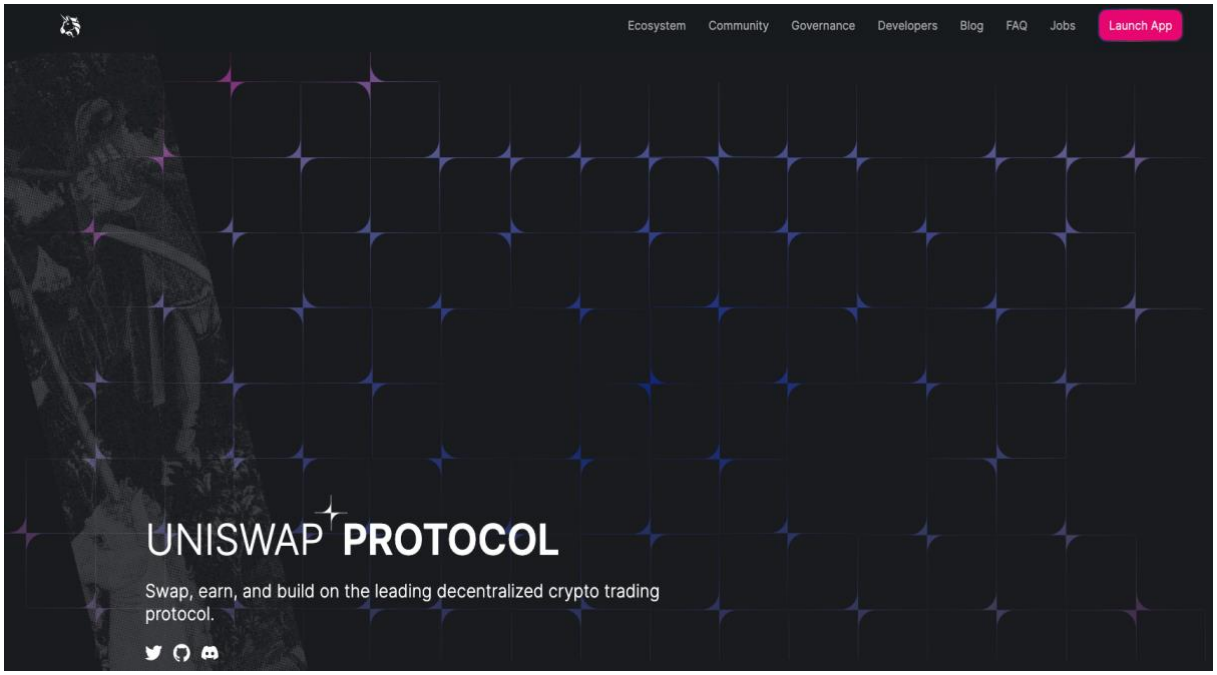

Figure 4. DEX: Uniswap platform.

Source: Uniswap website, 2024.

Decentralized exchanges (DEXs) offer several advantages. One key benefit is custody: users retain control of their funds, with trades occurring directly from their personal crypto wallets. This reduces the risk of centralized hacks and allows users to be solely responsible for their own security. DEXs also offer enhanced anonymity, as they typically do not require AML or KYC procedures, allowing users to trade without revealing their identities. Another advantage is decentralization, as DEXs operate on blockchain technology with smart contracts that facilitate trades, eliminating the need for intermediaries. This potentially increases transparency and reduces the risk of manipulation. Additionally, DEXs provide liquidity,

although it may be lower compared to CEXs. Liquidity pools and automated market makers (AMMs) are used to mitigate this issue, though trades may take longer to execute and large orders could impact the market price more significantly. Security is another strength of DEXs due to their decentralized nature and reliance on smart contracts. While they are less susceptible to large-scale hacks, vulnerabilities in smart contracts can still pose risks (Dyntu & Dykyj, 2021; Ghalwesh et al., 2020; Ilijevski et al., 2023). Fees on DEXs are typically lower, with most costs stemming from blockchain transaction fees (gas fees), which can fluctuate but may be more cost-effective for users.

However, DEXs also have their disadvantages. One is complexity, as they can be more challenging for beginners to navigate. Additionally, DEXs often have lower liquidity and trading volumes compared to CEXs. Customer support on DEXs is generally less accessible, often limited to platforms like Telegram Channels or Discord rooms, which may be difficult for less tech-savvy users to utilize effectively.

1.4.2.3. Comparison Between CEX and DEX

While both CEXs and DEXs offer unique benefits, the choice between the two largely depends on an individual's priorities and level of experience in the cryptocurrency market. Beginners or individuals seeking a more straightforward trading experience may find CEXs to be the ideal option, thanks to their ease of use and liquidity. On the other hand, experienced traders or those with a stronger focus on privacy and security might prefer DEXs for the autonomy and control they offer over funds and transactions. Ultimately, each platform type has its own set of strengths and challenges, and understanding these differences is crucial for making an informed decision that aligns with personal trading goals and risk tolerance. Table 1 provides a detailed comparison between CEXs and DEXs, highlighting their key differences in terms of user experience, security, liquidity, and regulatory oversight.

Table 1. Key Differences Between CEX and DEX.

	CEX	**DEX**
Control and custody	Funds are held by the exchange, which acts as a custodian.	Users retain full control over their funds through their personal wallets.
AML/KYC	Mandatory AML and KYC procedures for compliance with regulations.	Typically, no AML/KYC requirements, offering greater privacy.
User experience	Generally, more user-friendly with better customer support services.	Can be more complex and may require understanding of blockchain technology and wallet management.

Liquidity	Higher liquidity, supporting large trade volumes with minimal price impact.	Variable liquidity, often lower, but liquidity pools and AMMs help mitigate this.
Security	Centralized security measures but higher risk of large-scale hacks.	Security relies on blockchain technology and smart contracts; less risk of centralized hacking but smart contract vulnerabilities exist.
Fees	Fees for various services, often higher.	Lower transaction fees, mainly blockchain (gas) fees, which can fluctuate.
Regulation	Heavily regulated, requiring compliance with financial laws.	Less regulated, offering more freedom but also potential legal uncertainties.

1.4.2.4. Key Cybercrimes Involving Cryptocurrencies and Regulatory Responses

The analysis of the finalized literature revealed the most commonly reported types of cybercrimes associated with cryptocurrencies, along with their defining characteristics, aligned with the predefined criteria. A thorough examination of the literature highlighted key topics related to these crimes and the corresponding actions taken by governments worldwide. The crimes were organized into four main categories: (1) drug trafficking, (2) terrorism, (3) money laundering, and (4) CSAM. For each crime type, the relevant literature was synthesized, focusing on cryptocurrency-related aspects, and updated scientific terminology was incorporated. The review also included an investigation into government regulations and factors influencing cryptocurrency development and pricing. This comprehensive approach provided valuable insights into how various countries and regions are addressing the emerging challenges and advancements in the rapidly evolving cryptocurrency sector. Table 2 presents a detailed breakdown of the cybercrime landscape involving cryptocurrencies and the regulatory framework that shapes this dynamic field.

Table 2. Overview of Cybercrimes Involving Cryptocurrencies and the Regulatory Framework in the Reviewed Literature.

Categorization	Coin	N	References
Darknet	Bitcoin and cryptocurrencies in general	51	Ahuja et al. (2021), Alfieri (2022), Bahamazava & Nanda (2022), Bayramova et al. (2021), Bhaskar et al. (2019), Böhme et al. (2015), Broadhead (2018), Butler (2019), Chertoff & Simon (2015), Choi et al. (2020), Collins (2022), Davies (2020), Del Monaco (2020), DOJ (2017), dos Reis et al. (2024), Dupuis & Gleason (2020), Dyntu & Dykyi (2019, 2021), ElBahrawy et al. (2020), Finklea (2017), Gupta et al. (2021), Hatta (2020), Holt et al. (2023), Jung et al. (2022), Keane (2020), Kethineni et al. (2018), Kethineni & Cao (2020), Lacson & Jones (2016), Lee et al. (2022), Lee et al. (2019), Luong (2023), Mackenzie (2022), Mataković (2022), Meland et al. (2020), Mirea et al. (2019), Morelato et al. (2020), Naqvi (2018), Nazzari (2023), Piazza (2017), Raman et al. (2023), Reddy & Minaar (2018), Rubasundram (2019), Rudesill et al. (2015), Șcheau et al. (2020), Silfversten (2020),

				Stroukal & Nedvědová (2016), Tan (2024), UNODC (2020, 2023), van Wegberg et al. (2018), Virga (2015)
		Monero	2	Bahamazava & Nanda (2022), Florea & Nitu (2020)
Cybercrime		Bitcoin and cryptocurrencies in general	79	Agarwal et al. (2024), Alfieri (2022), Alqahtany & Syed (2024), Andres Rodriguez-Nieto & Eremina (2023), Auer & Tercero-Lucas (2022), Badawi &,Jourdan (2020), Bajra et al. (2024), Balaskas & Franqueira (2018), Bartoletti et al. (2021), Blasco & Fett (2019), Boehm & Pesch (2014), Bray (2016), Broadhead (2018), Brown (2016), Caporale et al. (2020), CERT-Bund (2022), Choi et al. (2009), Choi et al. (2020), Choi & Parti (2022), Ciphertrace (2023), Cong et al. (2022), Connolly & Wall (2019), Conventus Law (2021), Corbet et al. (2020), Courtois (2014), Critien et al. (2022), Custers et al. (2020), Del Monaco (2020), DOJ (2015), Dudani et al. (2023), Dupont & Holt (2022), Dyntu & Dykyj (2021), Dyson et al. (2018), Etto (2017), FBI (2022), Fosso Wamba et al. (2020), Gercke (2009), Gryszczyńska (2021), Gupta et al. (2021), Higbee (2018), Ivaniuk & Banakh (2020), Jung et al. (2022), Kerr et al. (2023), Kethineni et al. (2018), Kristoufek (2015), Kutera (2022), Lapuh Bele (2021), Lee (2019), Liao et al. (2016), Luong (2023), Mackenzie (2022), Mataković (2022), Mthembu et al. (2022), Pilinkiene et al. (2022), Priyambudi & Sinaga (2021), Recskó & Aranyossy (2024), Reddy & Minaar (2018), Riahi et al. (2024), Rieckmann & Stuchtey (2023), Rudesill et al. (2015), Saiedi et al. (2021), Sanusi & Dickason-Koekemoer (2022), Shinder & Cross (2008), Sigler (2018), Taylor et al. (2021), Team (2024), Thamizhisai et al. (2024), Trozze et al. (2022), UNODC (2020), van Nguyen et al. (2022), van Wegberg et al. (2018), Verduyn (2018), Virga (2015), Volevodz (2024), Watters (2023), Wronka (2022a, 2022b), Zheng (2024)
		Monero	3	Dyson et al. (2018), Gohwong (2019), Zimba et al. (2020)
		Ethereum	8	Andres Rodriguez-Nieto & Eremina (2023), Auer & Tercero-Lucas (2022), Bajra et al. (2024), Caporale et al. (2020), Dyson et al. (2018), Etto (2017), Kerr et al. (2023), Mthembu et al. (2022)
		Tether	2	Kerr et al. (2023), Mthembu et al. (2022)
		Binance	2	Kerr et al. (2023), Mthembu et al. (2022)
		USD Coin	1	Kerr et al. (2023)
Crypto ransomware		Bitcoin and cryptocurrencies in general	22	Badawi & Jourdan (2020), Broadhead (2018), Butler (2019), CERT-Bund (2022), CISA (2023), Cong et al. (2022), Connolly & Wall (2019), Custers et al. (2020), Gercke (2009), Ghalwesh et al. (2020), Gómez-Hernández & García-Teodoro (2024), Gray et al. (2023), Hernandez-Castro et al. (2020), Kerr et al. (2023), Meland et al. (2020), Muslim et al. (2019), Naqvi (2018), Nazzari (2023), Paquet-Clouston et al. (2019), Reddy & Minaar (2018), Sherer et al. (2016), Turner et al. (2020)
		Monero	5	CERT-Bund (2022), Gómez-Hernández & García-Teodoro (2024), Gohwong (2019), Patsakis et al. (2023), Zimba et al. (2020)
Organized crime	Drug trafficking	Bitcoin and cryptocurrencies in general	16	Ali (2021), Bertola (2020), Bhaskar et al. (2019), Butler (2019), Durrant (2018), Europol (2021), Godlove (2014), Kabra & Gori (2023), Keane (2020), Luong (2023), Mirea et al. (2019), Naheem (2021), Nurhadiyanto (2020), Pieroni (2018), Saiedi et al. (2021), Zaunseder & Bancroft (2020)
	Terrorism	Bitcoin and cryptocurrencies in general	20	Alfieri (2022), Biswas (2018), Dion-Schwarz et al. (2019), DOJ (2015), Durrant (2018), Gercke (2009), Gupta et al. (2021), Ilijevski et al. (2023), Keane (2020), Kfir (2020), Luong (2023), Moore & Rid (2016), Patel & Richter (2020),

				Reynolds & Irwin (2017), Rubasundram (2019), Thamizhisai et al. (2024), Teichmann & Falker (2020, 2024), Wang & Zhu (2021), Zavoli (2022)
	Money laundering	Bitcoin and cryptocurrencies in general	58	Agarwal et al. (2024), Ambrus & Mezei (2022), Barone & Masciandaro (2019), Boehm & Pesch (2014), Brown (2016), Butler (2019), Ciphertrace (2023), Clements (2021), Collins (2022), Custers et al. (2020), Del Monaco (2020), Dupuis & Gleason (2020), Durrant (2018), Dyntu & Dykyi (2019, 2021), Europol (2021), Gercke (2009), Godlove (2014), Goldbarsht (2024), Goodell & Aste (2019), Helwig et al. (2022), Hendrickson & Luther (2022), Holt et al. (2023), Ilijevski et al. (2023), Irwin & Slay (2010), Johari et al. (2019), Keane (2020), Kutera (2022), Leuprecht et al. (2022), Luong (2023), Manjula et al. (2022), Masciandaro et al. (2019), Munawa (2023), Naheem (2021), Nazzari (2023), Nazzari & Riccardi (2024), Nurhadiyanto (2020), Perkins (2021), Pieroni (2018), Pilinkiene et al. (2022), Pushkarev et al. (2020), Reddy & Minaar (2018), Reynolds & Irwin (2017), Riahi et al. (2024), Rubasundram (2019), Saiedi et al. (2021), Sanz-Bas et al. (2021), Schneider (2019), Sicignano (2021), Soni (2024), Teichmann & Falker (2020a, 2020b), van Wegberg et al. (2018), Virga (2015), Widhiyanti et al. (2023), Wronka (2022a), Yunandi & Leksono (2023), Zavoli (2022)
		Monero	3	Gohwong (2019), Teichmann & Falker (2020a, 2020b)
		Zcash	5	Dyson et al. (2018), Leuprecht et al. (2022), Silfversten (2020), Teichmann & Falker (2020a, 2020b)
		Ethereum	3	Leuprecht et al. (2022), Lin et al. (2023), Munawa (2023)
	CSAM	Bitcoin and cryptocurrencies in general	13	Broadhead (2018), Celiksoy & Schwarz (2023), Davies (2020), Finklea (2017), Gercke (2009), ICE (2020), Kristoufek (2015), Maxwell (2022), Naheem (2021), Nouwen (2017), Sayid (2023), UNODC (2020), van Nguyen et al. (2022)
Government regulations and factors influencing cryptocurrency development and pricing			79	Adam & Dzang Alhassan (2020), Aitken (2020), Alvarez et al. (2022), Al-Zubaidie & Jebbar (2024), Ambrus & Mezei (2022), Andronova et al. (2020), Auer & Tercero-Lucas (2022), Australian Home Affairs (2022), BaFin (2018), Boehm & Pesch (2014), Böhme et al. (2015), Bokovnya et al. (2020), Botha et al. (2023), CFTC (2017), Chand et al. (2024), Chen (2023), Cherniei et al. (2021), Chimienti et al. (2019), Chuan & O'Leary (2021), Clements (2021), Davies (2020), Del Monaco (2020), DOJ (2015), Dupuis & Gleason (2020), Dyntu & Dykyi (2019, 2021), Europol (2021), FBI (2022), Gercke (2009), Godlove (2014), Grasselli & Lipton (2021), Harryarsana (2022), Ilijevski et al. (2023), Interpol (2020), Kamps & Kleinberg (2018), Kavitha & Golden (2024), Kayani & Hasan (2024), Kethineni & Cao (2020), Kien & Binh (2021), Legge (2023), Liao et al. (2016), Lipton (2021), Mazambani (2024), Moffett (2023), Mthembu et al. (2022), Mubarak & Manjunath (2021), Omeljaniuk (2020), Otabek & Choi (2024), Özer et al. (2024), Ozturk & Sulungur (2021), Perkins (2021), Pernice & Scott (2021), Phugger (2021), Piazza (2017), Pop & Colonescu (2021), Priyambudi & Sinaga (2021), Pushkarev et al. (2020), Rajagopal (2020), Reddy (2020), Reiff et al. (2023), Reynolds & Irwin (2017), Rizzo (2017), Rueckert (2019), Sanz-Bas et al. (2021), Sicignano (2021), Sidhpurwala (2023), Sovbetov (2018), Suslenko et al. (2022), Tan (2024), Teichmann & Falker (2020a, 2020b), Turchyn & Turchyn (2021), van Nguyen et al. (2022), Verduyn (2018), Wen et al. (2024), Widhiyanti et al. (2023), Xie (2019), Zheng (2024), Zavoli (2022)

Note: Sources may fall into multiple categories.

1.5. The Darknet: Hub of Illicit Transactions

Throughout the reviewed literature, a consensus has emerged regarding the pivotal role of the darknet as a hub for illicit activities, largely facilitated by transactions conducted using cryptocurrencies, which present significant challenges for tracking (Cong et al., 2022; Reynolds & Irwin, 2017). The anonymity inherent in the dark web frequently links it to illegal activities, encompassing a range of illicit actions such as drug trafficking, arms sales, hacking services, counterfeiting, distribution of CSAM, and financial fraud (Chertoff & Simon, 2015; Hatta, 2020; Raman et al., 2023). It is essential, however, to recognize that not all dark web activities are nefarious; it also provides refuge for whistleblowers, activists, and individuals seeking privacy, particularly in the face of authoritarian regimes (Böhme et al., 2015; Kfir, 2020; Patsakis et al., 2023). The combination of relatively easy access and the use of cryptocurrencies in transactions underscores the absence of a universal regulatory framework, effectively perpetuating bank secrecy within the dark web (Chertoff & Simon, 2015; Hatta, 2020; Piazza, 2017; Raman et al., 2023).

In 2011, Ross William Ulbricht launched Silk Road, a website accessible via the darknet, designed as a global online marketplace catering to illicit transactions (Figure 5). Silk Road primarily focused on facilitating the trade of narcotics, cybercrime exploit kits, stolen credit card information, and counterfeit passports. It leveraged Bitcoin as its exclusive payment method, enhancing user anonymity. Moreover, Silk Road provided money laundering services, employing tools such as mixers and tumblers to obfuscate transaction trails (Bhaskar et al., 2019; Courtois, 2014; Kethineni et al., 2018; Lacson & Jones, 2016; Reddy & Minaar, 2018).

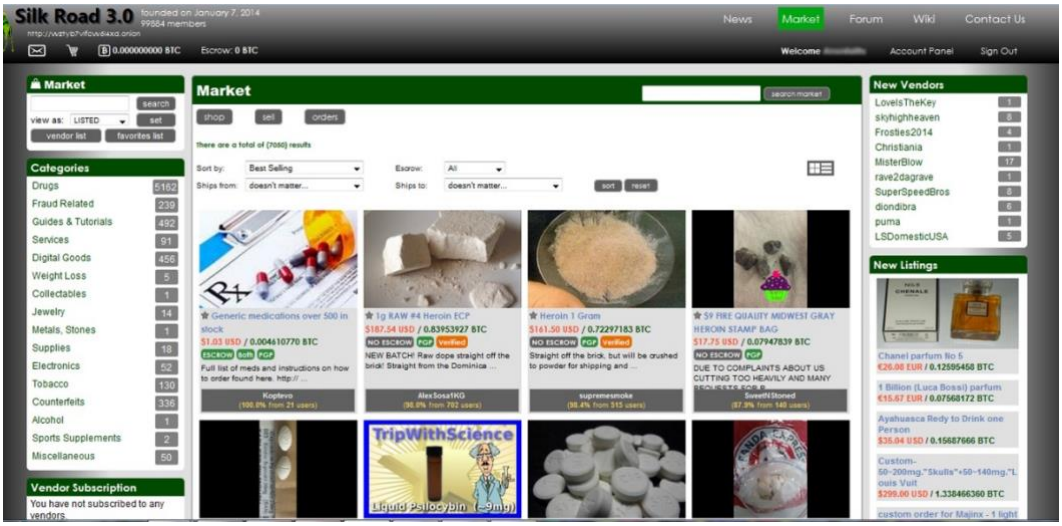

Figure 5. Silk Road 3.0 website, a darknet black market platform.

Source: Screenshot taken by Nialldawson (2015) from Wikimedia Commons on April 17, 2015.

Bitcoin plays an essential role in the dark web ecosystem due to its pseudonymous and decentralized nature (Bahamazava & Nanda, 2022; S. Choi et al., 2020; Kethineni et al., 2018). Unlike traditional currencies, Bitcoin transactions are not directly tied to individual identities, offering a level of anonymity. Instead, these transactions are recorded on a public ledger known as a blockchain, showcasing the movement of funds between Bitcoin addresses (Blasco & Fett, 2019; Phugger, 2021; Verduyn, 2018). While transaction details are visible, tracing the real-world identities behind the addresses proves challenging (Figure 6). Furthermore, Bitcoin's smart contract functionality enables the implementation of escrow services on dark web marketplaces. Escrow ensures the secure holding of buyer funds until the transaction is completed, mitigating the risk of scams or fraud. To enhance transaction privacy, Bitcoin tumblers or mixers are employed, which blend multiple transactions to obfuscate the origins of funds (Broadhead, 2018; Brown, 2016; Kethineni et al., 2018).

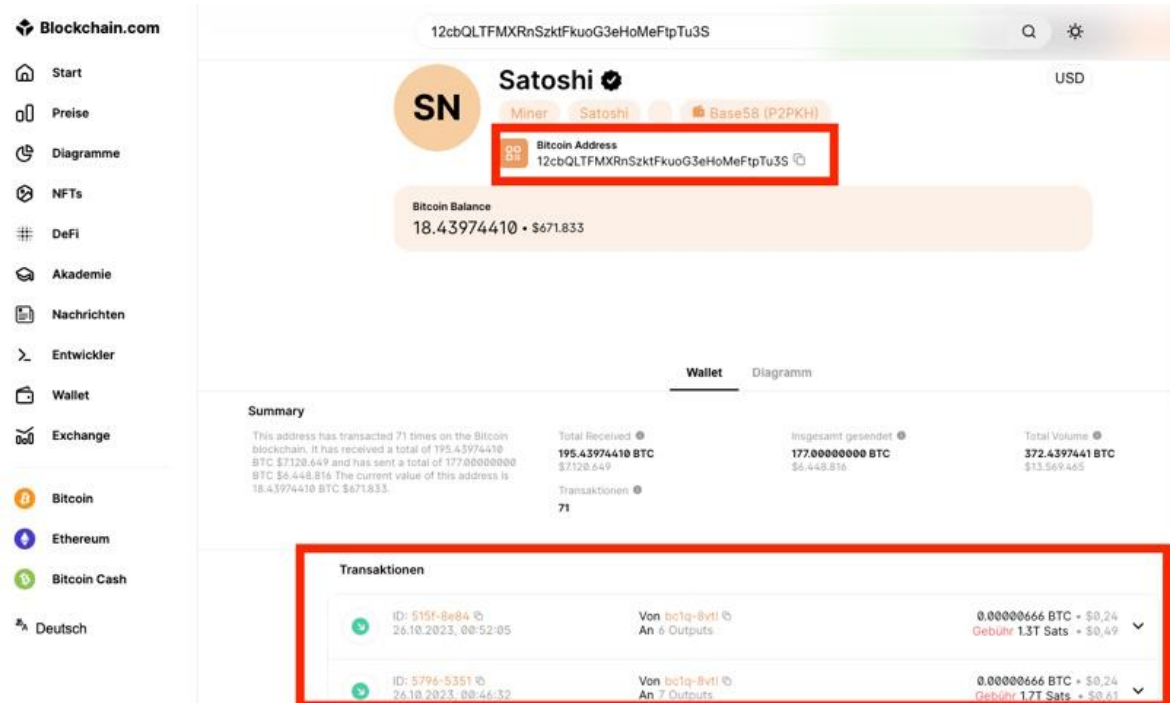

Figure 6. Visualization of Bitcoin wallet transactions on the https://www.blockchain.com/ website, showcasing the account of Satoshi with a balance of over 18 Bitcoins. The Bitcoin address and transaction details are illustrated.

Source: Screenshot taken by Shobhit Navani on November 10, 2023.

Moreover, privacy-focused cryptocurrencies such as Monero and Zcash present heightened anonymity features, offering both advantages and obstacles for law enforcement. Monero's transaction structure complicates the tracing process as signatures are pooled among a large group, making it challenging to link specific users to transactions (Bahamazava &

Nanda, 2022; Kethineni & Cao, 2020; Zimba et al., 2020). Conversely, Zcash operates by obliterating transaction history post-execution (Silfversten et al., 2020). Unlike Bitcoin transactions, which can be monitored on public networks like blockchain.com, tracking transactions involving privacy coins like Monero or Zcash poses significant difficulties (Etto, 2017; Pilinkiene et al., 2022; Reddy et al., 2020).

Darknet activities, as demonstrated, leverage various technologies to enable and conceal illicit transactions. Cybercriminals primarily use cryptocurrencies which provide the necessary anonymity for these transactions. The Tor network is another critical technology, facilitating anonymous browsing and access to darknet markets, where illegal goods and services are bought and sold. Additionally, mixing and tumbling services are employed to obfuscate transaction trails, making it challenging for law enforcement to trace the origins and destinations of funds. To suppress these activities, enhancing blockchain analytics is crucial (Bajra et al., 2024; Raman et al., 2023). Leveraging machine learning and artificial intelligence (AI) can help detect patterns indicative of illicit transactions and trace these activities across the blockchain. Improved regulation and strict enforcement of AML and KYC procedures at cryptocurrency exchanges can significantly reduce the anonymity that criminals rely on. Collaborations with technology providers are also essential. By partnering with companies that provide internet infrastructure, authorities can monitor and shut down darknet sites more effectively (dos Reis et al., 2024; FinCen, 2024; Nialldawson, 2015). These combined efforts can create a more hostile environment for cybercriminals operating on the darknet.

1.6. Cybercrime in the Era of Digital Advancement

Cybercrime encompasses a broad spectrum of illicit activities committed through the internet or digital networks, constituting a significant threat in the modern era (Dupont & Holt, 2022; Lapuh Bele, 2021; Shinder & Cross, 2008). The allure of cryptocurrencies for both cautious investors and criminal elements is undeniable (Ali, 2021; Barone & Masciandaro, 2019; Dyntu & Dykyi, 2019). Criminal entities perceive cryptocurrencies as ripe targets for exploitation, serving as not only a means of payment but also as tools for money laundering and avenues for launching cyberattacks (Ciphertrace, 2023; Custers et al., 2020; Dyntu & Dykyi, 2019). Regulators increasingly acknowledge the empowerment cryptocurrencies provide to criminal enterprises, paving the way for the emergence of novel cybercrimes.

Cryptocurrencies, notably Bitcoin, reign supreme as the preferred mode of financial exchange on the dark web, facilitating the trade of illicit goods, services, and data integral to

cybercriminal operations (Brown, 2016; Caporale et al., 2020; S. Choi et al., 2020). Criminal syndicates extensively leverage Crime-as-a-Service, a form of cloud computing, to perpetrate cybercrimes with alarming efficiency, further fueling the expansion of cybercrime year after year (Gryszczyńska, 2021; Higbee, 2018; Lapuh Bele, 2021). Bitcoin, often associated with cybercrime, remains a focal point due to its intrinsic security vulnerabilities and widespread usage in underground economies. While its pseudo-anonymous nature and global accessibility appeal to money launderers and criminals, it is imperative to discern that Bitcoin's fundamental technology is not inherently nefarious (Kristoufek, 2015; Nakamoto, 2009; Rueckert, 2019). Individuals seeking privacy amid pervasive surveillance systems also utilize cryptocurrencies, highlighting the nuanced landscape in which these technologies operate.

However, combatting organized cybercrime poses formidable challenges, particularly in navigating the intricate technicalities of cryptocurrencies. Digital forensics teams encounter not only sophisticated cybercriminal syndicates but also the complex cryptographic underpinnings of digital currencies, often tipping the scales in favor of cybercriminals (Balaskas & Franqueira, 2018; Cong et al., 2022; Naqvi, 2018; Patsakis et al., 2023). For instance, the United States saw a concerning rise in cyber threats in 2022, as revealed by the internet crime report from the Federal Bureau of Investigation (FBI). Over 800,000 complaints related to cybercrime were filed, resulting in total losses surpassing USD 10 billion, significantly surpassing the previous year's total of USD 6.9 billion. This underscores the urgent need to enhance cybersecurity measures and proactive law enforcement efforts to address the escalating cyber threat landscape (FBI, 2022).

Regarding the wide range of technologies used to facilitate this illicit activity. Crime-as-a-Service (CaaS) platforms have emerged as a significant threat, offering illicit services for hire, ranging from hacking services to the distribution of malware. Cryptocurrencies serve as a preferred medium for CaaS transactions due to their inherent anonymity, allowing cybercriminals to conduct financial exchanges without easily traceable identities (Ciphertrace, 2023; Hendrickson & Luther, 2022; Mazambani, 2024). Furthermore, cybercriminals leverage sophisticated hacking tools and exploit kits to infiltrate systems and pilfer sensitive data, exacerbating cybersecurity vulnerabilities (Gohwong, 2019; Interpol, 2020; Patsakis et al., 2023). To effectively combat this cybercrime, the deployment of advanced threat detection systems is imperative. AI-powered cybersecurity solutions are pivotal in this regard, capable of detecting and mitigating threats in real-time. These technologies bolster defenses against sophisticated cyber attacks, providing organizations with proactive security measures (Kutera, 2022; Mazambani, 2024; Volevodz, 2024). Additionally, fostering public-private partnerships

is crucial. Collaboration between law enforcement agencies and cybersecurity firms enables the sharing of intelligence and resources, enhancing the collective ability to respond swiftly to cyber threats and criminal activities.

Moreover, comprehensive education initiatives are essential to raise awareness among users and organizations about prevalent cyber threats such as phishing attacks (Cong et al., 2022; Gray et al., 2023; Nazzari & Riccardi, 2024). By educating the public about cybersecurity best practices and emerging threats, individuals and entities can better safeguard themselves against cybercriminal tactics. This multifaceted approach integrates technological advancements with collaborative efforts and educational outreach to fortify defenses against the evolving landscape of cybercrime.

1.7. Crypto Ransomware: Emerging Threats and Economic Considerations

The Cybersecurity and Infrastructure Security Agency (CISA) of the United States defines malware as any software crafted to illicitly breach IT systems, with the intent to pilfer data, disrupt services, or cause harm to networks (CISA, 2023). Ransomware, a specific type of malware, operates by encrypting targeted data or systems and withholding access until a ransom is paid. Notably, the evolution of ransomware has given rise to a particularly pernicious variant known as crypto ransomware, wherein perpetrators demand payment in cryptocurrency for the release of encrypted data or system access (Brown, 2016; CERT-Bund, 2022; Custers et al., 2020; Gray et al., 2023). This shift to cryptocurrency payments enhances anonymity for cybercriminals and complicates traditional law enforcement efforts to track and apprehend perpetrators.

The rise of crypto ransomware represents a significant cybersecurity challenge, exacerbated by the intricate interplay of social and technical factors within its ecosystem. As noted in a study by Connolly and Wall (2019), the impact of crypto ransomware has become increasingly pronounced in recent years, reflecting the adaptability and sophistication of cybercriminal tactics. The proliferation of cryptocurrency-based extortion schemes underscores the need for robust cybersecurity measures and proactive defense strategies to mitigate the risks posed by ransomware attacks (CISA, 2023; Meland et al., 2020; Muslim et al., 2019).

Examples of crypto ransomware demonstrate the evolving landscape of cyber threats. For instance, Crypto Locker emerged on September 5, 2013, heralding a new era of ransomware. This malicious software encrypted files on victims' systems, withholding

decryption keys until a ransom was paid, typically within a strict 72-hour window. Payment methods often included Bitcoin or MoneyPak, adding layers of anonymity for cybercriminals (Liao et al., 2016). A significant blow to the distribution of Crypto Locker came in June 2014 with Operation Tovar. This international effort, spearheaded by the United States Department of Justice (DOJ), CISA, the FBI, Europol, and other law enforcement agencies, targeted the Game Over Zeus botnet, a primary distributor of Crypto Locker. The operation's success dealt a severe blow to the prevalence of Crypto Locker and disrupted its criminal infrastructure (Hernandez-Castro et al., 2020).

Furthermore, an economic model proposed by Hernandez-Castro et al. (2020) sheds light on the nuanced dynamics of crypto ransomware payments. This model considers the victim's willingness to pay, with cybercriminals adjusting ransom demands based on the perceived value and characteristics of targeted victims. This price discrimination strategy aims to maximize profits by tailoring ransom amounts to victims' financial capabilities. Given the escalating threat posed by crypto ransomware, organizations and individuals must prioritize prevention and preparedness efforts (Brown, 2016; Gohwong, 2019; Meland et al., 2020; Muslim et al., 2019). This includes implementing comprehensive cybersecurity protocols, such as regular data backups, network segmentation, and user training to recognize and respond to phishing attempts. Additionally, maintaining up-to-date software patches and employing advanced threat detection technologies can help mitigate the risk of ransomware infections (Fosso Wamba et al., 2020; Gray et al., 2023; Meland et al., 2020; Paquet-Clouston et al., 2019). By adopting a proactive approach to cybersecurity, stakeholders can bolster their resilience against ransomware threats and safeguard critical data and systems from exploitation. As such, understanding the intricacies of crypto ransomware payments is crucial in developing effective strategies for prevention and response in the face of evolving cyber threats.

Crypto ransomware represents a significant cybersecurity challenge, where attackers use malware to encrypt data and demand ransom payments in cryptocurrency. Ransomware attacks typically involve anonymous communication channels like Telegram for negotiating ransoms. To mitigate the risk of crypto ransomware, regular data backups are essential (Gómez-Hernández & García-Teodoro, 2024; Patsakis et al., 2023; Sherer et al., 2016; Team, 2024). Network segmentation is another critical measure, as it helps to isolate critical systems and prevent the spread of ransomware within an organization. Developing and regularly updating incident response plans is also crucial, enabling organizations to respond quickly and effectively to ransomware attacks, minimizing the impact on operations. The best prevention is not to have crypto ransomware installed by persons and organization devices. To prevent this,

it involves a multi-faceted approach: regular software updates and patching, firewalls and endpoint protection, encryption of sensitive data both at rest and in transit, multi-factor authentication, regular audits and assessments, regularly updating access control, utilization of AI and machine learning to detect anomalies, and zero trust architecture. By integrating these measures, one can create a robust defense against hacking attempts via crypto ransomware (CERT-Bund, 2022; Gómez-Hernández & García-Teodoro, 2024; Gray et al., 2023; Nazzari, 2023; Patsakis et al., 2023; Team, 2024).

1.8. Organized Crime: Utilization of Cryptocurrency

Organized crime is categorized into four predominant types, each marked by the extensive use of cryptocurrencies: drug trafficking, terrorism, money laundering, and the distribution of CSAM.

1.8.1 Drug Trafficking

Drug trafficking involves the illicit production, transportation, and distribution of controlled substances, encompassing narcotics, hallucinogens, stimulants, and other banned drugs (Bahamazava & Nanda, 2022; Bertola, 2020; Holt et al., 2023). The World Drug Report 2020 by the United Nations Office on Drugs and Crime (UNODC) emphasizes that drug transactions, including new psychoactive substances, occur across both the open internet and the darknet. Notably, purchases made on various darknet marketplaces are frequently settled using cryptocurrencies, particularly Bitcoin, which are also prevalent in legitimate transactions on the open web. As previously highlighted, Silk Road, a notorious platform operating on the dark web, gained infamy for its vast array of illicit products, prominently featuring illegal drugs (Figure 5). In 2022, marijuana emerged as the top-selling drug on Silk Road, with transactions exceeding USD 46 million. Cocaine closely followed with 82,582 transactions totaling USD 17.4 million, while heroin sales reached an estimated USD 8.9 million. Additional sales of popular drugs such as methamphetamine, lysergic acid diethylamide, ecstasy, and various narcotics, including oxycodone and fentanyl, collectively generated around USD 19.2 million (Alfieri, 2022).

In a significant development, the DOJ announced the seizure of AlphaBay, the largest criminal marketplace on the internet, after operating for over two years on the dark web. AlphaBay facilitated the sale of a wide array of illegal goods, including deadly drugs, fraudulent

identification documents, malware, firearms, and toxic chemicals worldwide. The coordinated international effort to dismantle AlphaBay involved law enforcement agencies from Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, along with the European law enforcement agency Europol. Alexandre Cazes, also known as Alpha02 and Admin, a Canadian citizen residing in Thailand and the alleged creator and administrator of AlphaBay, was apprehended by Thai authorities on behalf of the United States. Tragically, Cazes reportedly took his own life while in custody in Thailand on July 12, 2017, following his arrest on July 5, 2017 (DOJ, 2017).

To suppress drug trafficking facilitated by cryptocurrencies, enhanced surveillance of darknet markets is necessary. Using advanced analytics and AI, authorities can monitor and infiltrate these markets more effectively (Bertola, 2020; Kabra & Gori, 2023; Raman et al., 2023). Blockchain monitoring tools can track cryptocurrency transactions related to drug trafficking, providing valuable leads for law enforcement. Additionally, strengthening international cooperation is crucial. By collaborating with global law enforcement agencies, coordinated efforts can be made to dismantle drug trafficking networks and bring perpetrators to justice.

1.8.2 Terrorism

Interconnections between terrorism financing, money laundering, cybercrime, and traditional criminal activities have been well-documented (Irwin & Slay, 2010). In 2015, a DOJ press release highlighted the case of Ali Shujri Amin, a 17-year-old who pleaded guilty to aiding the Islamic State of Iraq and Syria (ISIS), a militant terrorist group, through social media platforms like X. Amin, under the aliases of “Amreeki” and “American Witness,” advocated for Bitcoin as an anonymous, decentralized, and encrypted means of transferring funds to ISIS, making tracking transactions challenging (DOJ, 2015).

Similarly, in 2017, Indonesia’s financial intelligence unit, Pusat Pelaporan dan Analisis Transaksi Keuangan, reported that ISIS was utilizing online payment services like PayPal and Bitcoin to finance domestic operations, with Bahrun Naim, the orchestrator of the 2016 Jakarta attacks, allegedly utilizing these services (Rizzo, 2017). Additionally, in January 2018, the al-Qaeda-linked webzine al-Haqiqa published an article instructing readers on using cryptocurrencies for terrorism financing (Kfir, 2020).

To combat terrorism financing via the dark web and cryptocurrencies, advanced technological and intelligence tools are imperative. The inherent anonymity of transactions and

users presents a significant challenge, necessitating the development of pattern recognition algorithms, behavioral maps, rule bases, and predictive models (Andronova et al., 2020; Dyntu & Dykyj, 2021; Ilijevski et al., 2023). It is essential to establish systems capable of autonomously identifying potential instances of money laundering and terrorist financing, enhancing proactive detection and intervention (Dyntu & Dykyj, 2021; Kfir, 2020; Rubasundram, 2019; S. Wang & Zhu, 2021). Moreover, terrorist organizations have increasingly turned to cryptocurrencies to finance their activities, taking advantage of the anonymity provided by these digital assets. Encrypted communication tools like Telegram and Signal are also used to coordinate activities and transfer funds anonymously. This combination of technologies presents significant challenges for counter-terrorism efforts.

To combat terrorism financing via cryptocurrencies, establishing dedicated financial intelligence units is imperative. These units can monitor and analyze suspicious cryptocurrency transactions, identifying potential terrorist financing activities. Investing in decryption technologies can also help law enforcement agencies intercept and decode encrypted communications, revealing the networks and plans of terrorist organizations. Implementing global standards for cryptocurrency regulation is another critical step. By ensuring consistent enforcement against terrorist financing, the international community can prevent the misuse of digital currencies for terrorist activities. As such, banning crypto mixers, such as Sindbad.io, removes a critical tool used by terrorists to anonymize and move funds, enhancing the traceability of transactions and disrupting financial networks that support terrorism (Dion-Schwarz et al., 2019; Kfir, 2020; Rubasundram, 2019; Teichmann & Falker, 2024). By increasing transparency, deterring illicit use of cryptocurrencies, enhancing law enforcement capabilities, and fostering international cooperation, such bans play a crucial role in curtailing terrorism. This combined approach makes it more difficult for terrorist organizations to finance their operations, thereby contributing to global security efforts.

1.8.3 Money Laundering

Money laundering via cryptocurrencies, particularly Bitcoin, typically unfolds in several distinct stages. One common method is to engage with a Bitcoin trader (Custers et al., 2020; Otabek & Choi, 2024). In this approach, the trader facilitates face-to-face exchanges, where Bitcoins are traded for fiat currency. During these transactions, both parties bring their devices, and the trader immediately exchanges Bitcoins for the agreed-upon fiat currency, either in cash or via online banking. This method typically involves either a cybercriminal or an

intermediary as the client, and due to the risks and complexities involved, transaction fees are generally high. Another method involves using online money laundering services, which offer an additional channel for converting illicit proceeds.

Bitcoin is frequently utilized in such activities, offering a clear example of the process (Custers et al., 2020). As such, the initial phase often begins after a victim pays a ransom to cybercriminals or when an individual attempts to obscure the origins of illicit funds. When transferring Bitcoin to the cybercriminal, this transaction technically constitutes money laundering and thus carries legal repercussions (BaFin, 2018; Florea & Nitu, 2020; Johari et al., 2019). To execute such transactions, one must possess Bitcoin in their virtual wallet. Acquiring Bitcoin can be done through centralized exchanges such as Binance.com or Kraken.com. Alternatively, individuals can exchange other cryptocurrencies like Monero and Zcash, which offer enhanced privacy features, on decentralized platforms like UniDex, where KYC requirements are not mandatory (Figure 7).

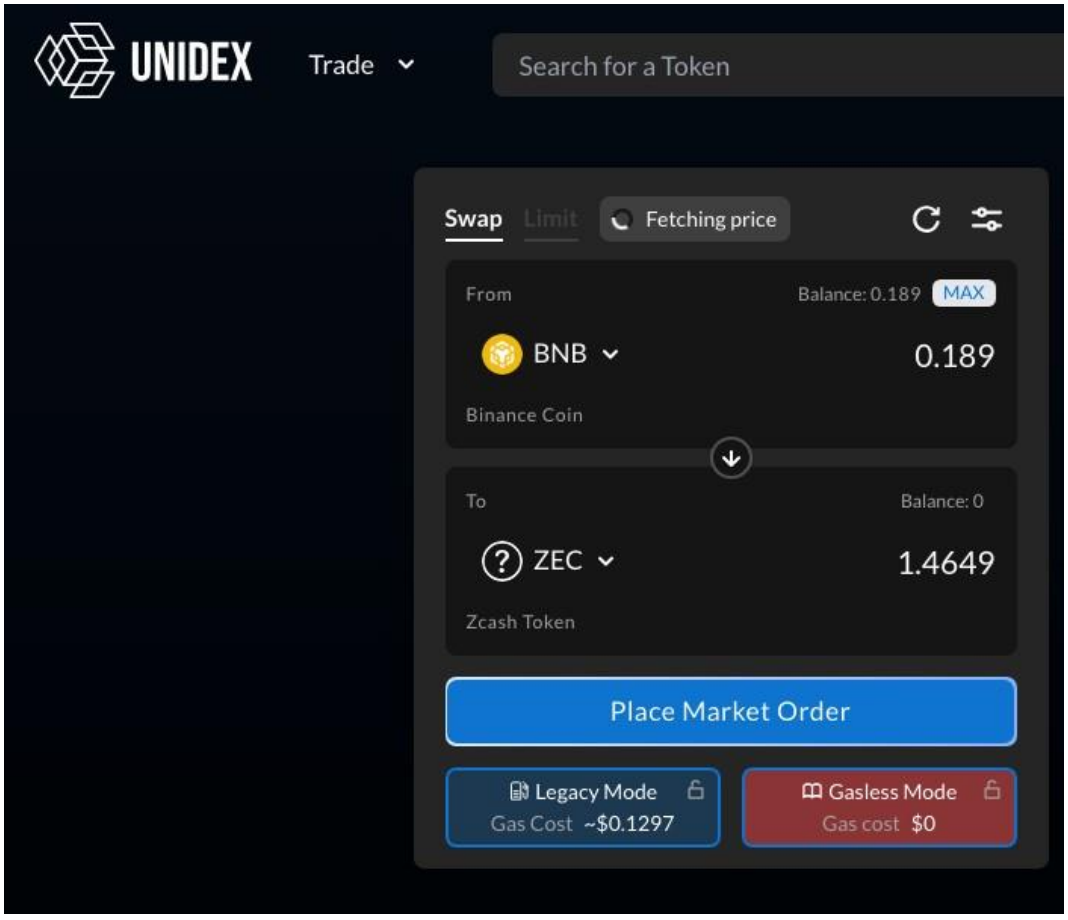

Figure 7. Visual representation of UNIDEX, a coin-swapping platform accessible on the https://www.unidex.exchange/ website.

Source: Screenshot taken by Shobhit Navani on December 15, 2023.

Furthermore, platforms like Coinbase Wallet, MetaMask, and Trust Wallet streamline the transfer of cryptocurrencies between various wallet addresses. While these wallets do not inherently support money laundering, they serve as cryptocurrency wallets and browser extensions, facilitating blockchain interaction. Figure 8 demonstrates a typical transfer of the cryptocurrency Ethereum using MetaMask, highlighting its efficiency and ease of use. However, due to the decentralized and difficult-to-track nature of these transactions, they present challenges for authorities in monitoring and controlling such activities. Consequently, like other tools such as UniDex, they can be exploited by individuals seeking to engage in illicit activities like money laundering.

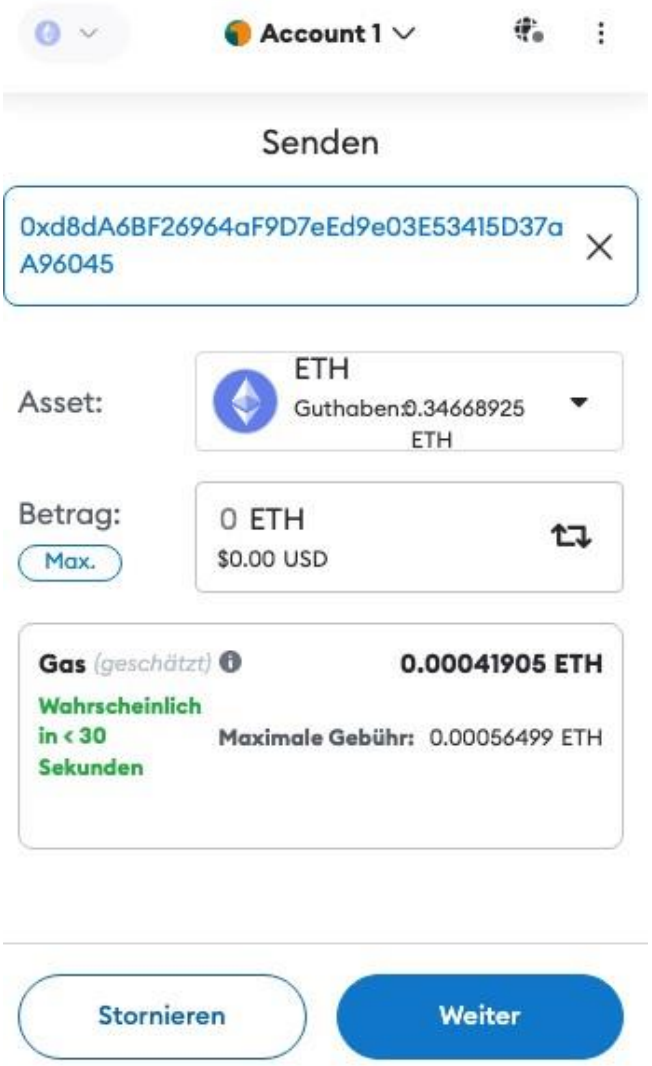

Figure 8. Illustration of transferring Ethereum cryptocurrency using the MetaMask wallet for interaction with the Ethereum blockchain, accessed through the https://metamask.io website.

Source: Screenshot taken by Shobhit Navani on December 9, 2023.

The second phase involves the concealment or expenditure of virtual currency. Cybercriminals often initiate Bitcoin transfers across a series of Bitcoin addresses to obfuscate the trail. Subsequently, they turn to cryptocurrency mixing services, as depicted in Figure 9, which exchange Bitcoins for Bitcoins, charging a fee in the process, with the aim of heightening anonymity. These services effectively sever the link between the sender and recipient, complicating monitoring efforts by authorities or cyber analysts (Del Monaco, 2020; Dyntu & Dykyj, 2021; van Wegberg et al., 2018). However, legally, utilizing mixing services likely constitutes concealment, potentially qualifying as money laundering. For instance, German law (i.e., § 261 German Criminal Code) defines money laundering as concealing the source of unlawfully obtained assets (German Federal Office of Justice, 2021). Thus, mixing services primarily serve to obscure the connection between parties in a cryptocurrency transaction, hindering the traceability of fund flows (Watters, 2023) and complicating efforts to identify the origin and destination of virtual asset (Wronka, 2022b).

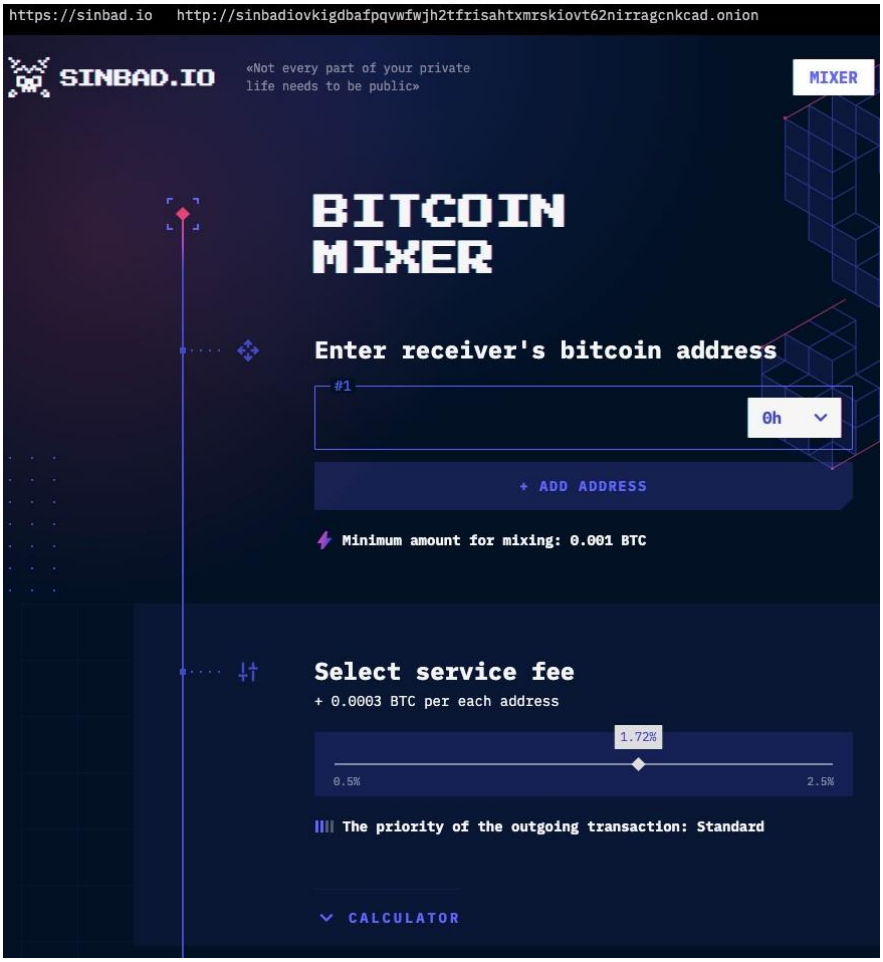

Figure 9. Demonstration of utilizing the SINBAD cryptocurrency mixing service, accessible via the https://sindbad.io/ website.

Source: Screenshot taken by Shobhit Navani on December 10, 2023.

In the next stage, the Bitcoins typically reach the primary account of the cybercriminals, often through one or more intermediaries. At this point, the cybercriminals have the option to convert the Bitcoins into electronic money via a cryptocurrency exchange (Figure 10) for fiat currencies such as dollars and euros. They can initiate the transfer by sending Bitcoin from their wallet to the wallet address of the cryptocurrency exchange, followed by selling the Bitcoin on the exchange for international fiat currency. When utilizing the services of a cryptocurrency exchange, the Bitcoins are sent to a designated Bitcoin address provided by the exchange. Subsequently, the equivalent amount in dollars or euros, minus any applicable fees, is transferred to an online banking account specified by the client. Remarkably, this entire process can be completed in less than an hour.

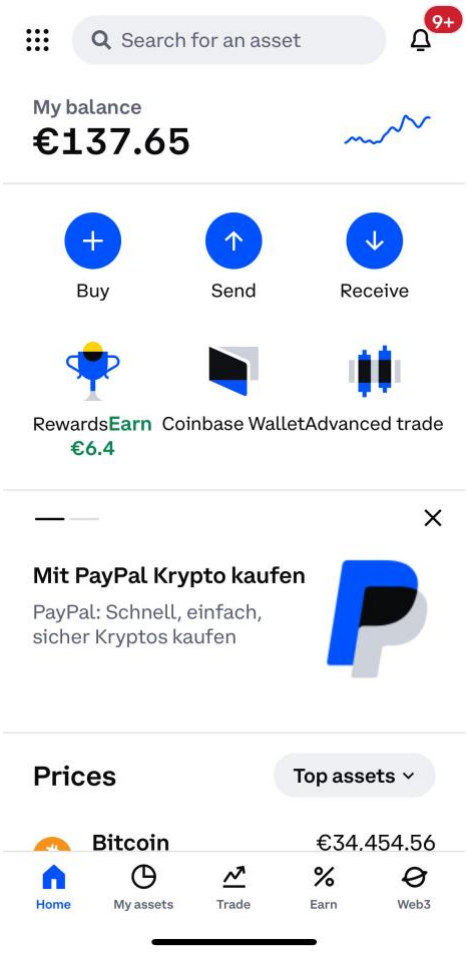

Figure 10. Illustration of the Coinbase mobile app, a cryptocurrency exchange platform, accessed through the https://www.coinbase.com/ website.

Source: Screenshot taken by Shobhit Navani on December 11, 2023.

These clandestine online entities, often accessible through the dark web, offer to launder funds received in Bitcoin. After transferring the Bitcoins to such a service, clients can choose

to receive the funds through legitimate online financial payment services like PayPal, Western Union, MoneyGram, or prepaid cards (Brown, 2016; Nazzari, 2023; Sicignano, 2021; Teichmann & Falker, 2020b; Wronka, 2022a, 2022b; Zavoli, 2022). Alternatively, the value of the virtual currencies can be returned via prepaid credit cards, which can then be used to withdraw cash from regular ATMs. Also, Bitcoins can be spent directly at various outlets, including online casinos, hosting services, and e-commerce platforms. Furthermore, an increasing number of brick-and-mortar establishments, such as pubs, restaurants, and shops, now accept Bitcoin as a form of payment. This provides cybercriminals with the opportunity to easily spend their laundered and anonymized Bitcoins on goods and services.

To suppress money laundering, enhancing blockchain forensics capabilities is essential (Agarwal et al., 2024; Alqahtany & Syed, 2024; Soni, 2024; Thamizhisai et al., 2024). Advanced tools and techniques can trace the flow of funds across the blockchain, identifying suspicious patterns and transactions. Enforcing strict AML policies across all cryptocurrency exchanges can also reduce the anonymity that criminals rely on (Florea & Nitu, 2020; Rieckmann & Stuchtey, 2023; Teichmann & Falker, 2020b). Additionally, developing a centralized crypto wallet infrastructure, where wallets are linked to verified identities, can simplify tracking funds and deter unauthorized transactions. These measures can significantly disrupt money laundering activities facilitated by cryptocurrencies.

1.8.4 CSAM

The availability of CSAM remains a critical issue, with perpetrators utilizing various platforms, including crypto markets, peer-to-peer networks, and even the open internet (ICE, 2020; Sayid, 2023). The UNODC (2020) report highlights the allure of the dark web for CSAM distribution due to its perceived anonymity and resilience to censorship. Dismantling this illicit content is particularly challenging as it is often replicated across numerous platforms, making it difficult to eradicate completely (Celiksoy & Schwarz, 2023; Nouwen, 2017). Regrettably, dating back to the COVID-19 pandemic, the issue worsened, with reports indicating a significant increase in CSAM websites emerging during lockdown periods (Botha et al., 2023; Gryszczyńska, 2021; Riahi et al., 2024; UNODC, 2020). Currently, a substantial portion of data shared on the dark web is believed to be CSAM, primarily in the form of images and videos. Certain sites reportedly boast collections in the terabyte range, equivalent to roughly 80 days' worth of video or nearly 1 million digital photographs (Nouwen, 2017; Sayid, 2023; UNODC, 2020). Overall, darknet activity and user bases, particularly on platforms like Tor, are

experiencing consistent growth (Zimba et al., 2020). While not all darknet activity is illegal, it is concerning that organized criminal elements within this space are continuously developing their capabilities, security measures, and business strategies.

The anonymity offered by cryptocurrencies, as highlighted by Broadhead (2018), has facilitated the sale of child pornography on the dark web, not only impacting adults but also harming children directly exploited in the creation of such content. The nature of this material and its devastating consequences for victims solidify the dark market as a significant threat. CSAM remains readily available through crypto markets, peer-to-peer networks, and even the open internet.

According to a press release, a Dutch national Michael Rahim Mohammed, aka Mr. Dark, 32, was indicted by a federal grand jury in the District of Columbia for his operation of Dark Scandals, a site on both the darknet and open internet that featured violent rape videos and depictions of child pornography (ICE, 2020). The indictment alleges Mohammed, who resides in the Netherlands, operated the Dark Scandals websites that hosted and distributed the material featuring nonconsensual and violent sexual abuse. Dark Scandals began operating in or about 2012 and boasted over 2,000 videos and images and advertised "real blackmail, rape, and forced videos of girls" all around the world. Dark Scandals offered users two ways to access this illicit and obscene content, which was delivered in "packs" via email to customers to download. Users could either pay for the video packs using cryptocurrency, such as Bitcoin, or upload new videos to add to the content of the Dark Scandals websites. Law enforcement was able to trace payments of Bitcoin and Ethereum to the Dark Scandals websites by following the flow of funds on the blockchain. The 303 virtual currency accounts identified were allegedly used by customers across the world to fund the websites and promote the exploitation of children and other vulnerable victims (ICE, 2020).

The exploitation and abuse of children depicted in CSAM represents a profound violation of their fundamental rights, resulting in enduring physical and emotional trauma (Draper, 2022; K. Jung, 2022; Maxwell, 2022). Addressing the role of cryptocurrency in facilitating these crimes is paramount, necessitating a multi-faceted approach to combat this atrocity. Effective regulation of cryptocurrency is crucial in preventing its misuse and protecting children from such unimaginable harm (ICE, 2020; Maxwell, 2022; Nouwen, 2017; Sayid, 2023). To combat CSAM, it is imperative to deploy AI-based content detection systems capable of identifying and removing CSAM from the internet, thereby significantly reducing its availability (Singh & Nambiar, 2024). Establishing global task forces focused on dismantling CSAM networks can strengthen international cooperation and coordination in these efforts.

Additionally, leveraging blockchain analysis tools to trace financial transactions associated with CSAM can disrupt the financial networks that support this illicit activity (Balaskas & Franqueira, 2018; Bayramova et al., 2021; Patsakis et al., 2023). These proactive measures are essential steps towards dismantling the infrastructure behind CSAM distribution and mitigating the exploitation of children.

1.9. Regulatory Measures

Countries around the world have adopted diverse strategies to address the challenges posed by cryptocurrency through regulatory measures. However, the absence of a centralized global regulatory authority, coupled with the inherent anonymity of cryptocurrency transactions, presents significant obstacles to the creation of comprehensive frameworks. The literature highlights substantial efforts by nations such as the United States, China, and India, which have formulated regulatory strategies tailored to the needs of their large populations.

In addition, European countries like Poland and Switzerland have established robust regulatory measures aimed at addressing cryptocurrency-related challenges and mitigating cybercrime risks. This chapter provides an in-depth examination of the regulatory approaches adopted by these nations. Other countries, including Australia, Canada, Japan, Singapore, South Korea, and the United Kingdom, have also implemented notable regulatory frameworks. However, these are not discussed in detail, as their strategies largely align with the frameworks employed by the aforementioned nations.

1.9.1 United States

The United States Constitution, under Article I, § 8(5), grants the Federal Government the exclusive authority to coin money and regulate its value. Despite this, statutes prohibiting the circulation of “unauthorized instruments” as currency have not been interpreted to include virtual currencies. To date, these laws have been applied primarily to counterfeited American dollar bills and coins. Virtual currencies, such as Bitcoin, exist in a regulatory gray area, with their classification varying across government agencies.

The FinCEN, a division of the United States Department of Treasury, treats Bitcoin exchanges as monetary services (FinCen, 2024). Under this classification, cryptocurrency administrators are required to register as money services businesses in accordance with the Bank Secrecy Act (BSA). In its 2013 Guidance, FinCEN clarified the distinction between

virtual and "real" currency, defining real currency as "the coin and paper money of the United States or any other country designated as legal tender." Virtual currency, on the other hand, was described as "a medium of exchange that operates like a currency in certain environments but does not possess all the attributes of real currency" (Xie, 2019b).

FinCEN's regulatory focus lies in preventing financial crimes, including money laundering and terrorist financing. To achieve this, it mandates compliance with AML and KYC regulations for specific cryptocurrency-related businesses, such as exchanges and money service providers (Chertoff & Simon, 2015; Watters, 2023; Widhiyanti et al., 2023). These measures underscore the United States government's intent to integrate virtual currencies into existing financial oversight frameworks while addressing associated risks.

The SEC initiated its first enforcement action involving virtual currencies in July 2013, targeting an alleged Ponzi scheme based on Bitcoin-denominated investments. The SEC argued that these investments qualified as securities under the category of "investment contracts" as defined by the Howey test, a legal framework established in the Supreme Court case *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). The Howey test outlines four criteria for determining an investment contract: (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profits, and (4) derived solely from the efforts of a promoter or third party (Reiff et al., 2023).

The defendant in the 2013 case contended that Bitcoin, rather than traditional money, was used for the investments, thus failing the first prong of the test. However, the court disagreed, concluding that Bitcoin constitutes a form of money and that the investments met the criteria for securities. In 2018, SEC Chairman Jay Clayton clarified during a House Appropriations Committee hearing that Bitcoin itself is not considered a security but refrained from extending the same determination to other cryptocurrencies like Ethereum or Ripple.

Bitcoin satisfies the first and third elements of the Howey test, as its purchase involves an investment of money and is often made with the expectation of profit. However, Bitcoin does not meet the second and fourth elements. The absence of horizontal commonality indicates there is no pooling of funds in a common enterprise, as Bitcoin transactions are independent of other investors. Similarly, the lack of vertical commonality stems from the fact that no promoter or third party directly influences the success of Bitcoin investments. Furthermore, the expectation of profit in Bitcoin investments depends on market dynamics rather than the managerial efforts of others. Consequently, Bitcoin does not fulfill all criteria of the Howey test and is not classified as a security (Moffett, 2023).

Moreover, the Internal Revenue Service (IRS) defines digital assets broadly as any digital representation of value recorded on a cryptographically secured distributed ledger or similar technology. Examples include convertible virtual currencies, stablecoins, and non-fungible tokens (NFTs). Convertible virtual currencies, such as cryptocurrencies, act as substitutes for real currency and can be used for payments, traded digitally, or exchanged for real currencies or other digital assets. However, for federal tax purposes, digital assets are treated as property rather than currency, as established in IRS Notice 2014-21 issued on March 25, 2014. Transactions involving digital assets must generally be reported on tax returns, reflecting the tax implications of their use. The IRS does not consider digital assets to be real currency because they lack issuance by a government's central bank.

In 2015, the CFTC classified Bitcoin and other virtual currencies as commodities. The distinction between the CFTC and the SEC lies in their regulatory focus: the CFTC oversees the derivatives market, while the SEC regulates the securities market. On March 6, 2018, a New York federal court ruled that virtual currencies could be regulated by the CFTC as commodities, further solidifying the agency's role in the cryptocurrency domain.

The FBI has also increased its focus on cryptocurrency-related crimes. In February 2022, during the Munich Cyber Security Conference, Deputy Attorney General Lisa Monaco announced the establishment of the Virtual Asset Exploitation Unit. This specialized task force operates under the DOJ's National Cryptocurrency Enforcement Team, which was launched in October 2021 to combat money laundering and cybercrime associated with virtual assets. Additionally, the Office of the Comptroller of the Currency clarified in July 2020 that federally chartered banks are authorized to provide custody services for cryptocurrencies. This clarification underscored the evolving role of traditional banking institutions in the cryptocurrency ecosystem by enabling secure storage solutions for digital assets.

Finally, as the central banking authority of the United States, the Federal Reserve monitors and studies developments in the cryptocurrency space. While it does not have direct regulatory authority over cryptocurrencies, its research and observations inform broader financial and regulatory policies concerning digital assets.

1.9.2 China

China's approach to cryptocurrency regulation has evolved significantly over the years, marked by a progressive tightening of restrictions aimed at curbing financial risks and maintaining control over monetary systems. Between 2010 and 2013, Chinese cryptocurrency

exchanges experienced substantial growth, with BTC China emerging as the world's largest exchange at its peak. However, this flourishing period was short-lived. In December 2013, the People's Bank of China (PBoC), in collaboration with six other regulatory agencies, banned financial institutions from processing Bitcoin transactions, signaling the beginning of stricter controls.

In 2017, China implemented a comprehensive ban on ICOs and domestic cryptocurrency exchanges. The government deemed ICOs as unauthorized fundraising mechanisms, and individuals involved in promoting or organizing ICOs faced potential criminal charges under Chinese criminal law. Notably, even non-Chinese citizens could be held accountable for ICOs conducted outside China if they involved Chinese residents. That same year, the government ordered the closure of crypto-exchange platforms, significantly disrupting the domestic cryptocurrency market (Chuan & O'Leary, 2021).

The regulatory crackdown intensified in January 2018 when the National Internet Finance Association of China issued a notice prohibiting the purchase, sale, and exchange of tokens or virtual currencies. While discussions about banning cryptocurrency mining were underway, the government ultimately confirmed its legality in 2019. However, mining activities became subject to global geopolitical sanctions and export controls. Despite these restrictions, Bitcoin is legally recognized as a commodity under Chinese law. In a significant legal update, China's Civil Code was amended in 2020 to include state-approved cryptocurrencies as inheritable property, reinforcing their status as commodities within a tightly controlled framework (Phugger, 2021).

Further consolidating its regulatory stance, the Law on the People's Bank of China grants the PBoC exclusive authority to issue currency and manage its circulation. Article 20 of this law prohibits any entity other than the PBoC from issuing tokens that could potentially replace the renminbi, while Article 16 designates the renminbi as the sole legally mandatory currency. In May 2021, the government banned financial institutions from accepting or using virtual currencies for payment or settlement. This prohibition also extended to facilitating the exchange of cryptocurrencies for yuan or other foreign currencies. The restrictions were justified by concerns about price manipulation and the financial risks associated with cryptocurrencies. However, owning cryptocurrency remains legal, albeit under increasingly stringent oversight.

Interestingly, while mainland China has adopted a restrictive approach, a contrasting regulatory strategy is being tested in Hong Kong. In 2023, Hong Kong's Securities and Futures Commission introduced a licensing framework for cryptocurrency exchanges, outlining clear

requirements for operating legally in the city. This initiative suggests a willingness to explore more liberal regulatory policies within the region, potentially creating a controlled environment for cryptocurrency innovation and investment.

China's regulatory landscape reflects a delicate balance between outright prohibition and cautious exploration of digital assets' potential, as exemplified by its efforts to develop the digital yuan. Excluded from cryptocurrency bans, the digital yuan represents the country's ambition to maintain sovereignty over its monetary systems while adapting to the evolving digital economy. However, China's overarching goal remains clear: to mitigate risks and maintain control over financial transactions involving cryptocurrencies.

1.9.3 India

India's regulatory landscape for cryptocurrency and cybercrime has undergone significant evolution over the years, marked by shifting policies and ongoing debates about their legal and financial implications. Initially, the country lacked specific laws addressing cryptocurrency, though cyber terrorism was explicitly criminalized under Section 66F of the Information Technology Act of 2000. This legislation outlines severe penalties for offenses related to cyber terrorism but does not address cryptocurrency or money laundering directly. Concerns over the potential misuse of cryptocurrencies for illegal activities prompted the Ministry of Finance to issue a gazette notification, extending AML regulations to cryptocurrency trading and related financial services.

In April 2017, the Indian government established an Inter-Disciplinary Committee to examine the regulatory aspects of cryptocurrencies. The committee submitted its report in August 2017, recommending stricter controls and comprehensive monitoring mechanisms. In his 2018 Budget speech, Finance Minister Arun Jaitley clarified that cryptocurrencies would not be considered legal tender in India, emphasizing the government's intent to discourage their use as a medium of exchange (Biswas, 2018).

Following these declarations, the Reserve Bank of India (RBI) imposed a sweeping ban on cryptocurrency trading in April 2018, prohibiting banks and financial institutions from facilitating transactions involving virtual currencies. This move mirrored similar actions taken by China and sparked widespread debate among stakeholders in the Indian cryptocurrency ecosystem. However, the Supreme Court of India overturned the ban on March 4, 2020, ruling that the RBI's decision violated constitutional rights, thus reigniting interest in cryptocurrency trading and investment across the country (Rajagopal, 2020).

Despite this legal victory for cryptocurrency enthusiasts, regulatory oversight has remained a pressing concern. Recognizing the challenges posed by the decentralized and anonymous nature of cryptocurrency transactions, the government proposed a 1% tax deducted at source on crypto asset transactions in 2022. This measure aimed to enhance transparency and track crypto-related activities. However, enforcing such oversight has proven challenging, as many transactions occur outside regulated exchanges, often through anonymous wallets that are difficult to trace.

The Indian government's apprehensions about cryptocurrencies primarily stem from their potential misuse for money laundering, tax evasion, and financing terrorism. The lack of a clear legislative framework and the coexistence of conflicting government stances have contributed to significant uncertainty regarding the legal status of cryptocurrencies. For example, while some policymakers advocate for a ban on cryptocurrencies, others emphasize the need for regulation to harness their potential for innovation and economic growth (Legge, 2023; Mubarak & Manjunath, 2021).

To address broader concerns about cybercrime, India has intensified its efforts to combat illicit activities in the digital realm. Law enforcement agencies are increasingly collaborating with international counterparts and leveraging advanced technological tools to address emerging threats. These initiatives reflect a growing recognition of the need for a robust regulatory framework to tackle the complexities of digital finance and cybercrime.

At present, India's regulatory environment for cryptocurrencies remains fluid and uncertain. Ongoing debates among policymakers, financial institutions, and industry stakeholders continue to shape the country's approach to cryptocurrency regulation. While significant strides have been made in addressing cybercrime and tracking digital transactions, the evolving nature of cryptocurrencies and their proliferation highlight the urgent need for comprehensive and adaptive regulatory measures. Such measures are essential to safeguarding against illicit activities while fostering innovation and economic growth in India's rapidly digitizing economy.

1.9.4 Poland

The Polish Penal Code of 1997 encompasses a wide range of crimes categorized into various chapters, including crimes against peace, humanity, and war crimes (Chapter XVI), crimes against the Republic of Poland (Chapter XVII), crimes against defense (Chapter XVIII), crimes against life and health (Chapter XIX), crimes against general security (Chapter XX),

crimes against communication security (Chapter XXI), environmental crime (Chapter XXII), crimes against freedom (Chapter XXIII), crimes against the freedom of conscience and religion (Chapter XXIV), crimes against sexual freedom and decency (Chapter XXV), crimes against family and care (Chapter XXVI), crimes against honor and physical integrity (Chapter XXVII), crimes against the rights of persons engaged in gainful employment (Chapter XXVIII), offenses against the activities of state institutions and local self-government (Chapter XXIX), crimes against the administration of justice (Chapter XXX), crimes against elections and a referendum (Chapter XXXI), crimes against public order (Chapter XXXII), crimes against protection of information (Chapter XXXIII), offenses against the credibility of documents (Chapter XXXIV), crimes against property (Chapter XXXV), crimes against economic turnover (Chapter XXXVI), and crimes against trading in money and securities (Chapter XXXVII). Despite its extensive coverage, the Penal Code does not explicitly define cryptocurrency, a concept that emerged after its enactment in 2008. However, a notable legal interpretation by the Supreme Administrative Court in March 2018 regarded cryptocurrencies, particularly Bitcoin, as property rights. Consequently, cryptocurrencies may fall under the purview of certain crimes outlined in Section XXXV of the Penal Code, highlighting their potential role in criminal activities (Omeljaniuk, 2020).

As such, in Poland, regulatory measures pertaining to cryptocurrency and cybercrime have evolved in response to emerging technological advancements and associated risks. While the Penal Code of 1997 offers a comprehensive framework for addressing various criminal activities, including those related to cybercrime, the dynamic nature of cryptocurrency presents challenges in enforcement and regulation. The lack of specific legal definitions for cryptocurrency within existing legislation necessitates continuous adaptation to adequately address new forms of criminal behavior facilitated by digital currencies (Gryszczyńska, 2021). Regulatory authorities, including the Ministry of Justice and the Polish Financial Supervision Authority, have increasingly focused on enhancing regulatory oversight and enforcement mechanisms to combat illicit activities involving cryptocurrencies. Efforts to strengthen AML and counter-terrorism financing regulations have been prioritized to mitigate the potential misuse of digital assets for illicit purposes (Omeljaniuk, 2020). Moreover, collaboration between law enforcement agencies, financial institutions, and technology experts has become integral to effectively combatting cybercrime and ensuring the integrity of financial systems (Europol, 2021). Despite these efforts, regulatory challenges persist, highlighting the need for ongoing vigilance and collaboration to address emerging threats posed by cryptocurrency and cybercrime in Poland.

1.9.5 Switzerland

Switzerland adopts a progressive approach to virtual currencies, considering them as property rather than legal tender akin to traditional money. The Swiss government has undertaken a thorough examination of virtual currencies, publishing a comprehensive report that delineates the economic implications, legal treatment, and associated risks (Swiss Federal Council, 2015). While acknowledging the potential risks of cryptocurrencies, such as money laundering and terrorist financing, the Swiss Federal Council also emphasizes the benefits and technological advancements accompanying these digital assets. The government's stance reflects a balanced assessment of the advantages and drawbacks of virtual currencies, coupled with a concerted effort to mitigate potential risks.

Regarding regulatory measures, Switzerland applies its AML law to entities accepting deposits or facilitating professional investment on behalf of third parties, encompassing transactions involving virtual currencies. This regulatory framework underscores Switzerland's commitment to combating financial crimes and ensuring investor protection in the realm of virtual currencies. Moreover, recent developments indicate Switzerland's increasing acceptance and integration of cryptocurrencies into its administrative and tax systems. Since 2021, Switzerland has allowed the payment of administrative fees and taxes using Bitcoin, signaling a progressive approach towards embracing digital currencies as part of its financial ecosystem (Ozturk & Sulungur, 2021).

In terms of taxation, holding cryptocurrencies in Switzerland is not subject to direct taxation, but it does impact annual wealth tax calculations. Individuals must report the total value of their cryptocurrency holdings as part of their annual wealth assessment, with any amount exceeding the personal exemption threshold being subject to a nominal tax (Ozturk & Sulungur, 2021). This taxation framework reflects Switzerland's pragmatic approach to integrating cryptocurrencies into its tax policy while ensuring transparency and compliance with fiscal obligations.

1.10. Future Directions for Technology and Regulation in Cryptocurrency

Future directions in technology and regulation for cryptocurrencies hold significant promise in advancing both security and usability while addressing the persistent risks posed by cybercrime. Technological advancements are poised to play a crucial role, particularly through

the development of sophisticated blockchain analytics tools powered by machine learning and AI (Singh & Nambiar, 2024). These tools enhance the capabilities of law enforcement and regulatory agencies by detecting fraudulent activities, tracing illicit transactions, and predicting security breaches. Such advancements are pivotal in fortifying the cryptocurrency ecosystem against increasingly sophisticated cyber threats (Florea & Nitu, 2020; Reddy & Minaar, 2018; Trozze et al., 2022).

Privacy-preserving technologies, such as zero-knowledge proofs and homomorphic encryption, offer another layer of security by enabling transaction verification without compromising sensitive information. This innovation strikes a balance between user privacy and regulatory compliance, ensuring that transactions remain secure while adhering to regulatory standards (Corbet et al., 2020). Moreover, formal verification methods for smart contracts are critical in eliminating vulnerabilities and mitigating exploitation risks within decentralized. By ensuring smart contracts are free from bugs, these methods enhance transactional security and build trust among participants in decentralized ecosystems applications (Al-Zubaidie & Jebbar, 2024; Chand et al., 2024; Kavitha & Golden, 2024; X. Zheng, 2024). Concurrently, decentralized identity frameworks provide robust solutions for identity verification while preserving user anonymity. These frameworks facilitate effective implementation of AML and KYC measures, bolstering overall security protocols and reducing fraudulent activities (ICE, 2020; Sayid, 2023).

Regulatory improvements are equally essential in creating a resilient and secure environment for cryptocurrency transactions. Enhanced international cooperation among regulatory bodies is crucial for harmonizing cryptocurrency regulations and closing jurisdictional loopholes that cybercriminals exploit. A unified approach to enforcement globally strengthens efforts to combat cryptocurrency-related crimes effectively. Clear and standardized regulatory frameworks are indispensable, providing transparency and certainty for cryptocurrency exchanges, wallet providers, and other entities (Ahuja et al., 2021; Kavitha & Golden, 2024; Kayani & Hasan, 2024). These frameworks outline specific guidelines that ensure compliance with legal standards, fostering a stable regulatory environment conducive to innovation and investment.

Stricter enforcement of AML and KYC regulations across all cryptocurrency platforms, coupled with advanced identification technologies like biometrics, holds the potential to significantly disrupt criminal activities such as money laundering (Goldbarsht, 2024; Leuprecht et al., 2022; Nazzari & Riccardi, 2024; Zavoli, 2022). By enhancing participant accountability and reducing anonymity risks, these measures bolster regulatory oversight and control over

fund movements within the cryptocurrency ecosystem. Implementing a centralized crypto wallet infrastructure linked to verified identities further simplifies AML and KYC procedures, streamlining fund tracking and deterring unauthorized transactions. In addition to regulatory frameworks and technological advancements, fostering collaboration through public-private partnerships is essential. These partnerships facilitate the exchange of information and resources crucial for combating cybercrime effectively. Comprehensive educational initiatives play a pivotal role in raising awareness among users and businesses about cybersecurity best practices, thereby reducing vulnerabilities to scams and cyber threats (Del Monaco, 2020; Higbee, 2018).

In all, prioritizing technological advancements and regulatory enhancements is crucial for fostering the widespread adoption of cryptocurrencies while safeguarding against evolving cyber threats. These advancements and improvements will not only help in building a secure, transparent, and resilient cryptocurrency ecosystem but also in adapting to the rapidly changing landscape of digital finance. Continuous adaptation and collaborative efforts among stakeholders are essential to stay ahead of cybercriminals and ensure the integrity of the cryptocurrency environment. Embracing these future directions will create a robust foundation for the sustained growth and acceptance of cryptocurrencies on a global scale.

1.10.1 Benefits and Limitations of Existing Solutions and Mechanisms

Cryptocurrencies have emerged as catalysts for innovation and efficiency in global financial systems, offering distinct advantages alongside notable challenges. Cryptocurrencies leverage blockchain technology, renowned for its enhanced security and transparency (Kayani & Hasan, 2024; Patsakis et al., 2023; Recskó & Aranyossy, 2024). The decentralized and immutable nature of blockchain ensures transaction records resist tampering and fraud, fostering trust and accountability in financial transactions. This feature empowers regulators and law enforcement agencies to effectively track and audit transactions, thereby enhancing transparency in financial ecosystems (Liao et al., 2016; Lin et al., 2023; Lipton, 2021; Otabek & Choi, 2024).

Furthermore, cryptocurrencies have revolutionized financial services by facilitating swift and cost-effective cross-border value transfers compared to traditional banking systems. This innovation promotes financial inclusion, particularly in underserved regions lacking access to conventional banking services (Al-Zubaidie & Jebbar, 2024; Boehm & Pesch, 2014; Dyntu & Dykyi, 2019). By providing essential financial tools and services, cryptocurrencies contribute

significantly to global economic growth and development. Additionally, the evolution of advanced analytical tools driven by cryptocurrencies has bolstered regulatory and enforcement capabilities. Utilizing machine learning and artificial intelligence, these tools detect suspicious activities within cryptocurrency transactions. Such insights enable regulators to enforce AML and KYC regulations rigorously, reducing illicit activities and fortifying market integrity (Florea & Nitu, 2020; Goldbarsht, 2024; Lapuh Bele, 2021).

Conversely, despite their benefits, cryptocurrencies present significant challenges that require attention. Foremost among these challenges is the absence of a unified global regulatory framework. Regulatory approaches to cryptocurrencies vary widely across jurisdictions, fostering regulatory arbitrage and creating vulnerabilities exploited by cybercriminals. This fragmentation complicates consistent enforcement and oversight, impeding efforts to combat crimes such as money laundering and terrorism financing effectively (Ciphertrace, 2023; Goldbarsht, 2024; Ilijevski et al., 2023; Irwin & Slay, 2010; Nazzari & Riccardi, 2024; Teichmann & Falker, 2020b; Wronka, 2022a). Another critical concern lies in the anonymity and privacy features inherent in cryptocurrencies (Agarwal et al., 2024; Badawi & Jourdan, 2020; Hatta, 2020). While essential for protecting legitimate privacy rights, these features also facilitate illicit activities. Cryptocurrencies like Monero and Zcash, prioritizing privacy, hinder law enforcement agencies' ability to trace transactions and identify individuals involved in criminal activities. This anonymity poses obstacles to investigating and prosecuting cryptocurrency-related crimes effectively.

Moreover, the intricate technological architecture of blockchain systems poses challenges for law enforcement and digital forensics teams. The complexity of blockchain, coupled with privacy-enhancing tools such as mixers and tumblers, further obfuscates transaction trails (Del Monaco, 2020; Dyntu & Dykyj, 2021, 2021; Nazzari, 2023; Rieckmann & Stuchtey, 2023). Investigating cryptocurrency-related crimes demands specialized expertise and resources, which may not always be readily available, thereby hindering effective enforcement efforts. Furthermore, cross-border enforcement presents formidable challenges due to the inherently global nature of cryptocurrency transactions. These transactions frequently traverse national boundaries, leading to jurisdictional complexities and varying levels of international cooperation (Kethineni & Cao, 2020; Patsakis et al., 2023; B. Tan, 2024). Such challenges underscore the critical need for enhanced collaboration and harmonization of regulatory frameworks to address cross-border cryptocurrency-related crimes comprehensively.

In conclusion, while cryptocurrencies offer substantial benefits in terms of innovation and financial inclusivity, they also pose challenges related to regulatory oversight, privacy concerns, and technological complexities. Addressing these challenges through enhanced regulatory cooperation, technological advancements, and robust public-private partnerships is essential to maximizing the positive impacts of cryptocurrencies while mitigating associated risks.

1.10.2 Analyzing Research Questions: Balancing Innovation and Security in the Face of Cybercrime

This chapter has provided an in-depth exploration of the intricate and multifaceted realm of cryptocurrency, emphasizing its dual nature as both a driver of innovation and a facilitator of illicit activities. Addressing the evolution of cryptocurrency, it underscores how the decentralized and pseudonymous features of digital currencies have inadvertently contributed to the rise of cybercrime. This dynamic creates significant challenges for global security, as cybercriminals exploit these characteristics for activities such as money laundering, ransomware attacks, and terrorism financing (*RQ1*).

A critical examination of the darknet reveals its pivotal role in enabling illicit cryptocurrency transactions, serving as a marketplace for illegal goods and services. The anonymity provided by the darknet complicates efforts to trace and disrupt criminal activities. While regulatory measures have sought to address this issue, their success has been limited due to the adaptive tactics of cybercriminals and the fragmented nature of global regulations. Enhanced international cooperation and innovative technological tools are necessary to mitigate the darknet's impact effectively (*RQ2*).

The chapter also evaluates the effectiveness of existing regulatory frameworks in combating cryptocurrency-related cybercrime, noting significant disparities across nations. While some countries, such as the United States and Switzerland, have developed robust regulatory approaches, others struggle with enforcement and adaptation to the fast-evolving digital landscape. These gaps expose vulnerabilities in the global financial system, emphasizing the need for improved and harmonized strategies to enhance security and trust in cryptocurrency markets (*RQ3*).

The findings underscore the inherent tension between fostering innovation and ensuring security in the cryptocurrency domain. Balancing these priorities requires adaptive governance, vigilant policymaking, and the strategic deployment of technological advancements.

International collaboration is essential to bridge regulatory gaps and address the challenges posed by the interconnectedness of cryptocurrency with global financial systems and cybercrime networks.

In conclusion, this chapter emphasizes the importance of continuous research, dialogue, and proactive measures to realize the transformative potential of cryptocurrency while safeguarding ethical, legal, and financial standards. These efforts are imperative for creating a more secure, equitable, and sustainable global financial system in an era increasingly defined by digital innovation.

1.10.3 Analyzing Hypotheses: Cryptocurrency and Its Role in Cybercrime

The analysis of cryptocurrency's intersection with cybercrime offers crucial insights into the hypotheses *H1*, *H2*, and *H3*, shedding light on the dynamics of illicit activities and regulatory challenges in this rapidly evolving domain.

The findings of this chapter strongly support *H1*. Cryptocurrencies like Bitcoin and Monero, with their decentralized nature and pseudonymous transactions, have provided fertile ground for cybercriminals to expand their operations. DeFi platforms, in particular, have emerged as a double-edged sword. While they enable financial inclusion and technological innovation, their lack of centralized oversight creates vulnerabilities that criminals exploit for laundering illicit funds and trafficking drugs. The darknet further amplifies this issue, serving as a conduit for anonymous and untraceable transactions in illegal marketplaces. The growing prevalence of ransomware attacks, where victims are often required to pay in cryptocurrency, exemplifies how digital currencies have become integral to the modern cybercrime ecosystem.

H2 is not supported (or partially supported to some degree). This hypothesis highlights the critical need for a global, unified approach to cryptocurrency regulation. Evidence from this chapter, however, indicates that current regulatory frameworks, while diverse, are insufficiently coordinated to address the cross-border nature of cybercrime. Nations with stringent regulations, such as Switzerland, have seen relative success in curbing illicit activities through robust AML measures and KYC policies. However, these efforts are undermined by countries with less comprehensive oversight. A coordinated international strategy that combines regulatory frameworks with advanced technological tools, such as blockchain analytics, holds significant potential to deter the misuse of cryptocurrencies and reduce their appeal for ransomware attackers and terrorist networks.

The chapter's findings confirm *H3*, illustrating how regulatory disparities create havens for cryptocurrency-related cybercrime. Nations with weaker legal structures or lax enforcement mechanisms often become hotspots for illicit activities. The darknet, as a hub for illegal transactions, thrives in these regulatory gaps, offering cybercriminals anonymity and access to global networks. Geographic and topological analyses presented in this chapter highlight the uneven distribution of cryptocurrency-related cybercrimes, with high incidences in regions lacking coordinated oversight. Strengthening global regulatory standards and fostering international collaboration are imperative to counteract these vulnerabilities and disrupt the illicit use of cryptocurrencies.

In summary, the hypotheses explored in this chapter underscore the intricate relationship between cryptocurrency, cybercrime, and regulatory efforts. Addressing these challenges demands a balanced approach that fosters innovation while mitigating risks through stronger global governance and technological advancements.

CHAPTER 2

FTX: UNRAVELLING THE SAGA OF CRYPTO SCAM

2.1. FTX and the Dark Side of Cryptocurrency: A Case Study in Fraud, Governance, and Market Vulnerabilities

While the preceding chapter has established a theoretical framework for understanding the dark side of cryptocurrency, the case of FTX offers a stark, real-world example of these complexities in action. Chapter 2 shifts the focus from broad regulatory and criminal dynamics to a detailed investigation of one of the most infamous crypto scandals to date. By unpacking the rise and catastrophic fall of FTX, this chapter will illustrate how systemic weaknesses, unethical practices, and inadequate oversight can culminate in widespread financial and reputational damage. The saga of FTX serves as a cautionary tale, offering critical insights into the vulnerabilities within the cryptocurrency ecosystem and the urgent need for more robust safeguards. Through this case study, the intricate interplay between governance, fraud, and market dynamics will be explored, providing a vivid context for the themes outlined in the literature review.

Furthermore, the exploration of the relationship between cybercrime and cryptocurrency has been meticulous, employing a systematic categorization approach to understand their interconnectedness. By organizing crimes into specific categories, this analysis provides valuable insights into the complex dynamics within the realm of digital finance. It sheds light on key issues, trends, and policy considerations shaping this rapidly evolving domain, from financial security breaches to identity theft and fraud. The intersections of cryptocurrencies with various forms of illicit behavior underscore the urgent need for comprehensive oversight and regulatory frameworks.

The saga of the FTX scandal serves as a stark reminder of the vulnerabilities within the cryptocurrency ecosystem. It highlights how systemic weaknesses, inadequate governance, and unethical practices can culminate in widespread financial and reputational harm. As a cautionary tale, FTX not only illustrates the risks associated with poorly regulated markets but also underscores the necessity of establishing robust safeguards to protect investors and enhance market integrity. This case study reinforces the imperative for stakeholders—regulators, technologists, and policymakers—to collaborate in addressing the challenges posed by the volatile and often opaque world of cryptocurrency.

2.1.1. Early Days of Sam Bankman-Fried

Sam Bankman-Fried, widely recognized as SBF in the online community, was born in 1992 in Stanford, California. He is the son of Barbara Fried and Alan Joseph Bankman, both distinguished professors at Stanford Law School, who first met in 1988 (Dean & Huileng, 2023). SBF grew up in a spacious home near Stanford's campus and attended Crystal Springs Uplands School, a private high school known for academic excellence (Lindqwister & Tong, 2022). While at Crystal Springs, SBF participated in the Canada-USA Math Camp, a program for talented young mathematicians. The school, recognized by *The Wall Street Journal* in 2007 as one of the top 50 globally for university preparation (Gamerman et al., 2007), boasts alumni like Patty Hearst and chess grandmaster Daniel Naroditsky (Chittum, 2023). Nishad Singh, a key FTX executive and a friend of SBF's younger brother, Gabriel, also attended the school and later graduated from UC Berkeley with a degree in electrical engineering and computer science (Osipovich, 2023).

SBF displayed an early aptitude for solving math puzzles. He met FTX executive Gary Wang at another math camp, leading to a lasting friendship and their eventual shared time at the Massachusetts Institute of Technology (MIT), where they roomed together (Carreras, 2023). At yet another math camp, SBF met Sam Trabucco, who later graduated from MIT in 2015 with a degree in math and computer science, the same year as Wang (Lang & Mccrank, 2022). Trabucco joined Alameda Research, a firm SBF founded in 2017 (Rosenberg, 2023). At MIT, he also befriended Adam Yedidia, who later worked for FTX (Yaffe-Bellany & Moreno, 2023).

In 2013, during his undergraduate studies, SBF encountered Will MacAskill, a leading figure in the effective altruism (EA) movement. MacAskill convinced him to pursue a finance career to maximize earnings for altruistic causes, an idea that profoundly shaped SBF's philosophy (Alter, 2023). MacAskill later served as an unpaid advisor for the FTX Future Fund, which pledged USD 100 million to EA-aligned projects (Albergotti & Matsakis, 2022). EA advocates using empirical evidence to guide impactful charitable efforts, a concept that resonated deeply with SBF (Christian, 2023).

After graduating from MIT in 2014, SBF joined Jane Street Capital, a renowned trading firm specializing in quantitative analysis and high-frequency strategies (Syme, 2023). Jane Street serves as a common career path for top graduates from institutions like MIT and Stanford. There, he worked alongside future FTX executives, including Caroline Ellison, a Stanford graduate and daughter of prominent MIT economists Glenn and Sara Fisher Ellison, and Brett Harrison, who later became CEO of FTX US (Varanasi et al., 2023).

SBF earned recognition as one of the firm's top traders, reportedly donating around 50% of his earnings to causes aligned with effective altruism, such as animal welfare and the Center for Effective Altruism (CEA) (Kolhatkar, 2023). However, he grew dissatisfied at Jane Street, particularly as the cryptocurrency market began booming in 2017, with daily trades exceeding USD 1 billion—largely untapped by traditional trading firms. Seeing an opportunity for both profit and greater philanthropic impact, he left Jane Street after three years to co-found Alameda Research with Tara Mac Aulay, whom he met through the CEA (Whitworth, 2023).

2.1.2. Alameda Research: From Arbitrage Success to Ethical Dilemmas in the Crypto Landscape

Alameda Research, named after SBF's hometown of Alameda, California, was initially based in Berkeley before relocating to Hong Kong to benefit from its more relaxed regulatory environment (Yaffe-Bellany & DelMundo, 2023). Founded in 2017, the company quickly gained recognition for its work in algorithmic trading, market-making, and providing liquidity across cryptocurrency exchanges.

Despite Mac Aulay's limited background in finance—she was a pharmacist prior to co-founding Alameda—her collaboration with Bankman-Fried positioned the firm as a significant player in the crypto space (Wiblin & Harris, 2018). Alameda Research operated as a quantitative cryptocurrency trading firm, employing advanced algorithms and trading strategies to navigate the volatile markets. Its active involvement in trading, investments, and liquidity provision for various tokens and exchanges solidified its prominence. Managing substantial capital, Alameda held considerable influence within the DeFi sector, playing a pivotal role in shaping market dynamics.

DeFi is a blockchain-based financial system that seeks to replicate traditional financial services without relying on centralized intermediaries like banks or financial institutions (Ozili, 2022). Operating through smart contracts—self-executing contracts with terms embedded in code—DeFi platforms facilitate transactions, lending, borrowing, trading, and other financial activities directly on blockchain networks such as Ethereum. By removing intermediaries, DeFi aims to enhance financial inclusion, transparency, and accessibility, offering lower fees and broader access to anyone with an internet connection. Despite these benefits, DeFi carries significant risks, including vulnerabilities in smart contracts, regulatory uncertainties, and market volatility.

Key components of the DeFi ecosystem include lending and borrowing platforms, where users can earn interest or collateralize assets to borrow funds; DEXs, which enable peer-to-peer cryptocurrency trading without centralized authorities; and stablecoins, cryptocurrencies pegged to fiat currencies for stability in trading and lending. Other features include yield farming and liquidity mining, strategies that reward users for providing liquidity to DeFi protocols, and platforms offering derivatives and synthetic assets, allowing exposure to various markets without physical ownership.

Alameda Research leveraged arbitrage opportunities, particularly during Bitcoin's early rise, to establish itself as a formidable player in the cryptocurrency trading landscape. Exploiting price discrepancies across global markets, Alameda executed rapid trades, buying Bitcoin on exchanges where it was undervalued and simultaneously selling on platforms where it commanded a higher price (Sigalos, 2022b). This approach capitalized on inefficiencies in the fragmented and less-regulated cryptocurrency market, allowing Alameda to generate significant profits and establish its reputation.

Arbitrage, in essence, involves profiting from price differences for the same asset across different markets. For instance, if Bitcoin is priced at USD 50,000 on Exchange A and USD 50,500 on Exchange B, an arbitrageur could buy Bitcoin on the lower-priced exchange and sell it at the higher price on the other platform. Such trades are typically executed swiftly to minimize the risk of price convergence, often relying on automated trading bots for precision and speed. While these opportunities are common in fragmented markets like cryptocurrencies, their availability diminishes as market inefficiencies are corrected by competing traders.

Alameda's success was also rooted in its sophisticated trading algorithms and its ability to operate across numerous exchanges, securing liquidity and responding dynamically to market changes. However, the firm's reliance on arbitrage highlights both the promise and pitfalls of DeFi and cryptocurrency markets. While early adopters like Alameda profited from inefficiencies, such strategies underscore the volatility and lack of regulatory oversight that make the crypto ecosystem both lucrative and risky.

Moreover, this environment also reflects broader trends in DeFi, where innovative financial mechanisms intersect with significant challenges. Beyond arbitrage, Alameda expanded its operations to include market making and liquidity provision, further solidifying its influence within decentralized finance. Yet, as its role grew, so did the risks associated with the largely unregulated space, including allegations of conflicts of interest and misuse of funds. These issues would later come to the forefront as part of the broader controversies surrounding SBF and FTX.

SBF skillfully capitalized on what became known as the "Kimchi Premium" in cryptocurrency markets (Pongratz, 2021). The term "Kimchi" is derived from the popular Korean dish made from fermented vegetables like cabbage and radishes, seasoned with chili peppers, garlic, and ginger. Just as kimchi undergoes a fermentation process, the "Kimchi Premium" refers to the significant price discrepancy for cryptocurrencies, particularly Bitcoin, between South Korean exchanges and those in other countries. Due to high demand for Bitcoin in South Korea, the price on local exchanges often soared above global market prices, creating a lucrative arbitrage opportunity.

Bankman-Fried and his team exploited this price gap by buying Bitcoin on Western exchanges where it was cheaper and selling it on South Korean exchanges for a higher price. This arbitrage strategy proved highly profitable, and as demand for Bitcoin surged, the price discrepancies widened. By 2018, Alameda Research was moving up to USD 25 million per day, benefiting immensely from this strategy. The Kimchi Premium eventually grew to more than 50%, further boosting the firm's success (De Jong, 2022).

However, as the cryptocurrency market matured and more players entered the space, arbitrage opportunities became less profitable and increasingly difficult to sustain. The profitability of the Kimchi Premium dwindled, and as funds tightened, concerns about risk management and business ethics began to surface within the company. Tara Mac Aulay, co-founder of Alameda, expressed her concerns about the firm's future direction. Disagreements over how to navigate the evolving landscape led to her resignation, along with that of other employees, as she tweeted about her departure (Figure 11). This shift marked a turning point for Alameda Research, as the firm struggled to adapt to the rapidly changing dynamics of the crypto market.

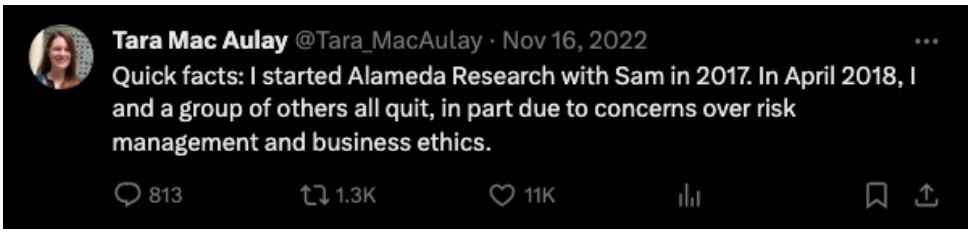

Figure 11. Tweet from Tara Mac Aulay's on November 16, 2022, available at: https://twitter.com/Tara_MacAulay/status/1592985303262072834

Source: Screenshot taken by Shobhit Navani on October 10, 2023.

Zuckerman (2022) from *The Wall Street Journal* reported that some Alameda Research staff became frustrated with poor record-keeping and inaccurate balance data, leading to delays

in transferring XRP tokens and causing losses in the millions. In 2018, the firm's assets dropped by nearly two-thirds due to a decline in XRP's price, pushing it close to collapse. SBF reportedly rescued the company by securing funds from lenders and investors, promising up to 20% returns (Jha, 2023). During this period, a significant amount of cryptocurrency went missing. While some management members wanted to halt trading and inform stakeholders, SBF chose to continue, believing there was an 80% chance the funds would be recovered. This approach, however, did not align with generally accepted accounting principles, leading to resignations over concerns about risk management and ethics (Prentice, 2023).

In documents from 2018, Bankman-Fried acknowledged that Alameda's lack of proper accounting and risk management contributed to trading losses and internal conflicts. To address this, the company implemented new systems for tracking profits, losses, and transfers, which eventually improved profitability. Some departing employees had raised concerns about the firm's risk controls with investors but did not report them to regulators. At the time, Alameda primarily served well-funded individual investors, minimizing exposure to smaller ones.

Carolyn Ellison and Sam Trabucco joined Alameda in March 2019, with both becoming co-CEOs in 2021. After Trabucco's resignation, Ellison became the sole CEO in 2022 (Poleo, 2023). In 2019, Ryan Salame, who had not been part of Bankman-Fried's inner circle, joined Alameda. He later became CEO of FTX Digital Markets, a subsidiary in the Bahamas (Goldstein et al., 2022). At the time, Alameda was a small firm with just 30 employees (Weiss, 2023).

Former employees reportedly offered a USD 1 million buyout to Bankman-Fried, which he declined, leading to the resignation of four management team members and about half of Alameda's staff. By April 2018, the firm's assets dropped to USD 30 million as investors pulled out. This exodus was due in part to SBF's control over the company, leading to concerns about his decisions and management style. After his split with Tara Mac Aulay in 2018 and growing concerns from other effective altruists, Bankman-Fried left the CEA board in 2019 (Alter, 2023).

Alameda Research functioned as a hedge fund primarily trading cryptocurrencies, borrowing funds from third-party lenders and engaging in margin trading. SBF eventually shifted focus to founding the cryptocurrency exchange FTX in 2019, formally resigning from Alameda in 2021. Prosecutors allege that FTX was intended to prop up Alameda Research (Hale, 2023).

2.1.3. The Rise of FTX: Innovations and Market Dynamics in the Crypto Exchange Industry

A cryptocurrency exchange is a platform where users can buy, sell, and trade digital currencies like Bitcoin, Ethereum, and altcoins. It facilitates transactions between buyers and sellers, allowing users to exchange fiat currencies or other cryptocurrencies based on market prices (Alvarez et al., 2022; Manjula et al., 2022; Özer et al., 2024). To use an exchange, users create an account, verify their identity, and deposit funds via bank transfer, card, or cryptocurrency transfer. Once funded, users can place orders (market or limit) to buy or sell crypto. When buy and sell orders match, the exchange executes the trade, transferring assets between accounts. Exchanges charge fees for trades and withdrawals, and employ security measures like two-factor authentication, encryption, and cold storage (Kerr et al., 2023). They also offer tools like charts and order books to help users make informed decisions.

SBF founded FTX in 2019 to address issues in the cryptocurrency exchange market. He identified a gap, noting that exchanges were losing millions daily due to poor customer retention (Doherty, 2021). FTX, launched in Hong Kong with Gary Wang, raised USD 1.8 billion from investors. The platform introduced advanced features to better serve traders and investors. FTX's native token, FTT, launched in May 2019.

An ICO is a fundraising method where start-ups issue digital tokens to raise capital, similar to an Initial Public Offering (IPO). ICOs allow investors to buy tokens with cryptocurrencies like Bitcoin or Ethereum, granting access to services or voting rights. Unlike IPOs, which are heavily regulated, ICOs have less oversight, presenting higher risks and the potential for fraud (Campino et al., 2022). ICOs are open to a broader range of investors compared to IPOs, which are usually limited to established companies and institutional investors (Nganga, 2023).

Alameda served as a market maker on FTX, facilitating consistent buying and selling. Initially the primary market maker, its trading volume on the platform dropped to just 3% by 2022 (Ge Huang, 2023). Market makers provide liquidity by continuously buying and selling financial instruments at publicly quoted prices. They set bid and ask prices, profit from the bid-ask spread, and help reduce price volatility. Their role ensures smooth market functioning by offering trading opportunities, even in less active markets. For instance, if the bid for ETH is USD 2,000 and the ask is USD 2,050, a market maker facilitates these trades by selling at USD 2,000 and buying at USD 2,050, capturing a profit from the spread.

Market makers manage inventory risks by adjusting their holdings based on market conditions. Their strategies require constant supervision, as seen with Knight Capital, which

lost over USD 460 million in 2012 due to a faulty algorithm. Market makers also face the risk of holding “naked” positions, which can lead to significant losses if the market moves against them (Das, 2021).

Before FTX’s emergence in 2019, Binance was already a dominant CEX. However, FTX introduced several groundbreaking products that were later adopted by Binance and other crypto firms. These innovations included: (1) leveraged tokens, which allowed traders to gain leveraged exposure to cryptocurrencies without managing leverage or margin positions, later adopted by Binance; (2) tokenized futures contracts, enabling traders to speculate on cryptocurrency prices without holding the assets, which Binance later replicated; and (3) prediction markets, allowing users to bet on event outcomes, which Binance explored but did not fully replicate. In 2019, Binance’s owner, Changpeng Zhao, invested USD 100 million for a 20% stake in FTX, marking a strategic collaboration between the two. Binance also took a long-term position in FTT to support FTX’s growth. In return, FTX helped enhance Binance’s liquidity and institutional offerings. By 2020, FTX had become a leading derivatives platform, with average daily trading volumes nearing half a billion US dollars (Binance, 2019).

2.1.4. FTX’s Expansion and Serum: Bridging Centralized and Decentralized Exchanges in the Cryptocurrency Ecosystem

In 2020, FTX launched Serum, a DEX built on the Solana blockchain, expanding Bankman-Fried’s ownership to both the centralized FTX and decentralized Serum (Yakovenko, 2021). A blockchain is a decentralized ledger technology that records transactions in interconnected blocks across a distributed network, eliminating the need for central authorities (Blasco & Fett, 2019; Chand et al., 2024; Y. Chen et al., 2020; Watters, 2023). Key characteristics of blockchain include: (1) decentralization, where transactions are validated through consensus, not intermediaries; (2) persistence, ensuring transactions are secure and hard to alter; (3) anonymity, offering privacy through generated addresses; and (4) auditability, allowing easy verification and tracking of transactions (Z. Zheng et al., 2017). These features make blockchain a secure, transparent, and efficient alternative to traditional centralized systems.

A Blockchain Name Service (BNS) is a system that links human-readable domain names to blockchain addresses, similar to how the traditional Domain Name System (DNS) translates website names into IP addresses. BNS simplifies navigation within the blockchain ecosystem by replacing complex, alphanumeric wallet addresses with easy-to-remember

names. This makes it easier for users to send and receive cryptocurrencies without the risk of error associated with long wallet addresses. Operating on decentralized networks, BNS eliminates the need for a central authority, aligning with blockchain's core principles of decentralization. Blockchain domains registered via BNS are often considered NFTs, granting users full ownership and control over their domains, which can be bought, sold, or transferred like other digital assets.

As such, SBF was a strong proponent of Solana, a layer-1 blockchain designed as a faster alternative to Ethereum. He supported multiple projects within the Solana ecosystem and accumulated significant amounts of its native token, Solana (SOL), through his firms (Chittum, 2022). Solana aimed to enhance user scalability by prioritizing fast transaction settlements. Serum, built on Solana's infrastructure, benefited from the blockchain's speed and cost-effectiveness, resulting in lower transaction fees. Solana processes blocks in 400-600 milliseconds, far outpacing Ethereum 1.9 and Ethereum 2.0 by more than ten times and surpassing high-performance layer 1 networks by 3-5 times (Yakovenko, 2021).

One of the most popular BNS is Ethereum Name Service (ENS), allowing users to link Ethereum addresses to .eth domain names. Alameda Research had multiple ties to Bonfida, the project behind Solana's version of ENS. It was the primary market-maker for Bonfida's native token FIDA. Alameda acquired millions of FIDA tokens by investing in that start-up (Coin Desk, 2023). Bonfida acted as a bridge between Serum, Solana, and the end user. It provided a comprehensive product suite, including a user interface (UI) for Serum's DEX. Bonfida specialized in making the Serum DEX more accessible and user-friendly.

Moreover, at the core of Serum's platform was a decentralized order book, managed by smart contracts, which functioned similarly to traditional exchanges by matching buyers and sellers. This structure provided users control over pricing and order sizes, offering greater autonomy in trading. Serum aimed to disrupt DeFi by offering a model that competed with AMM platforms like Uniswap, Sushi, and Bancor. Additionally, Serum supported cross-chain functionality, enabling token swaps across blockchains such as Ethereum and Polkadot, thereby extending its liquidity and compatibility with various DeFi projects. Serum's utility and governance token, SRM, offers trading fee discounts for holders on the Serum DEX. SRM is native to Solana (as an SPL token) and also exists on Ethereum as an ERC20 token.

Navigating the legal complexities and inconsistent regulations in the cryptocurrency sector has posed challenges in applying uniform standards across companies in the United States and those operating globally. To address this, SBF launched FTX US in 2020, a separate entity designed specifically for the American market. Meanwhile, the main FTX platform,

initially based in Hong Kong and later moved to the Bahamas, continued to serve international customers. FTX US operates within the U.S. regulatory framework, ensuring compliance with regional guidelines to provide services exclusively for American users.

2.2. The Crypto Bull Run of 2021

A bull market in cryptocurrency is marked by a strong upward trend in prices, driven by increased demand and limited supply (Legge, 2022). The crypto bull market of 2021 saw prices soar, with Bitcoin reaching nearly USD 65,000 in April, attracting significant institutional interest and a surge in retail investors. This boom extended beyond Bitcoin, with Ethereum surpassing USD 4,000, fueled by the growth of DeFi and non-fungible tokens (NFTs). Major companies like Tesla and MicroStrategy also invested heavily in Bitcoin, enhancing crypto's legitimacy. Institutional acceptance grew, with financial giants offering crypto products, while the DeFi sector and NFT market flourished. Regulatory scrutiny increased, with governments focusing on stablecoins, central bank digital currencies, and crypto taxation, affecting market sentiment (Kovach, 2021)..

The cryptocurrency market experienced significant volatility in 2021, with sharp price swings resulting in both rapid gains and steep corrections. Events like China's renewed crackdown on crypto mining and trading further fueled market instability (John et al., 2021). By mid-May, a major correction saw prices of Bitcoin and other cryptocurrencies drop by over 50% from their peaks. However, the market gradually recovered, with renewed interest and stability toward the year's end, though prices did not reach previous highs. The bull market was marked by extraordinary growth, institutional involvement, and regulatory developments, but also by environmental concerns over the energy consumption of proof-of-work cryptocurrencies like Bitcoin. This sparked debates on sustainability and a push for more eco-friendly consensus mechanisms (de Vries & Stoll, 2021). Overall, 2021 highlighted the cryptocurrency market's potential and volatility, shaping future discussions on regulation, sustainability, and digital asset evolution.

FTT, the native token of the FTX exchange, experienced significant price fluctuations between 2020 and 2021. In March 2020, during the market crash triggered by the COVID-19 pandemic, many cryptocurrencies, including FTT, saw sharp declines, with FTT hitting an all-time low of around USD 1 (Rooney, 2020). However, during the crypto bull market of 2021, FTT surged, reaching an all-time high of over USD 84, marking an impressive rebound from its 2020 lows. This growth played a key role in making SBF a multi-billionaire (Figure 12). For

instance, if an investor purchased 100,000 FTT tokens at the low of USD 1 per token in 2020, their investment of USD 100,000 would have appreciated to USD 8.4 million at the peak price of USD 84 in 2021. By the end of 2021, Forbes estimated SBF's net worth at USD 26 billion (Al Jazeera, 2023). In 2022, FTX raised USD 400 million in its Series C funding round, boosting its valuation to USD 32 billion—comparable to Deutsche Boerse's market capitalization and surpassing that of Nasdaq and Twitter (Crawley, 2022a).

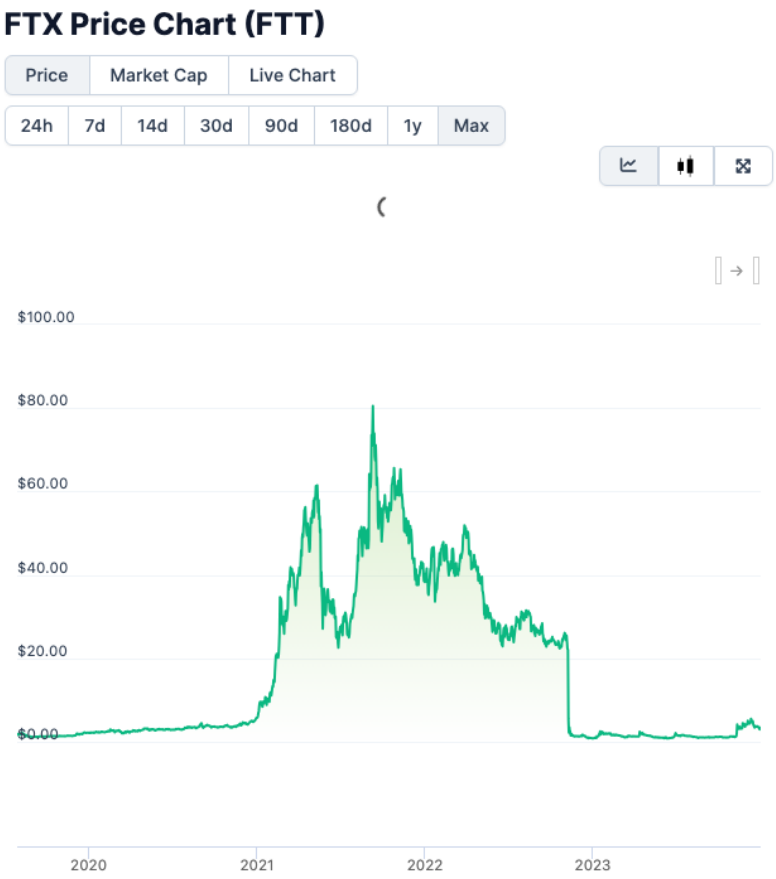

Figure 12. Price of FTT token.

Source: https://www.coingecko.com

2.3. The Bankman-Fried Family and FTX's Political Contributions

SBF's father, Joseph Bankman, a prominent tax law scholar and professor at Stanford University, advocated for simplified tax systems and innovative approaches to tax compliance, significantly influencing tax law. One of his key initiatives was the "Ready Return" system in California, designed to streamline tax filing by pre-filling returns with existing data. Although initially supported by Governor Schwarzenegger, the plan faced opposition from tax prep

companies like Intuit, which lobbied against it, arguing that government-run systems could be less reliable than private solutions (Mayyasi & Smith, 2017).

Joseph also helped Senator Elizabeth Warren draft a 2016 tax bill aimed at simplifying tax filing, which gained support from law professors and economists. Unfortunately, the bill stalled in committee (GovTrack, 2016). Warren, a vocal critic of the cryptocurrency sector, continues to push for stronger regulation and taxes in the industry (Ceekz, 2023).

Sam's mother, Barbara Fried, a Stanford Law professor, co-founded the political action committee Mind The Gap (MTG) in 2018, alongside Paul Brest and political strategist Graham Gottlieb. MTG advises donors on strategic contributions to enhance their political influence, focusing on Democratic causes (Influence Watch, 2023). Political Action Committees (PACs), including Super PACs like MTG, raise and spend money independently of candidates and parties, with Super PACs able to collect unlimited donations to support or oppose political candidates while complying with federal disclosure requirements (opensecrets.org, 2023).

FTX, headquartered in Hong Kong, established West Realm Shires Inc. as its American subsidiary to operate FTX US in the United States. Launched in 2020, West Realm Shires is a registered money services business with FinCEN, part of the United States Department of the Treasury. FinCEN's crucial role involves protecting the financial system from misuse, fighting money laundering, and bolstering national security by gathering, analyzing, and disseminating financial intelligence and applying strategic financial measures. Registration with FinCEN is essential for entities in the financial sector, particularly for adherence to AML regulations.

Compliance with the BSA is a crucial requirement for financial institutions. As the foundation of American AML legislation, the BSA mandates that businesses assist government agencies in detecting and preventing money laundering. Under FinCEN, certain entities must submit reports that aid criminal, tax, or regulatory investigations. Financial institutions are required to file suspicious activity reports if they identify transactions linked to potential money laundering, fraud, or other crimes. They must also submit currency transaction reports for cash transactions exceeding USD 10,000 to track significant cash flows. Additionally, American individuals with control over foreign financial accounts must file a report of foreign bank and financial accounts if the total value exceeds USD 10,000 in a year. By adhering to these regulations, companies like West Realm Shires (FTX US) play a vital role in preventing financial crimes, maintaining the integrity of the financial system, and protecting themselves from legal risks while enhancing their reputation for corporate responsibility.

Table 3 presents data on donations made by FTX during the 2019-2020 campaign cycle, offering insights into the company's political contributions and influence. The "Recipient"

column lists the entities or individuals that received donations, including PACs, political parties, and individual candidates. The "Total" column displays the donation amounts in USD, with the largest being USD 11,240,000 to Future Forward USA, a Democratic-aligned super PAC based in Palo Alto. This PAC spent USD 108 million in the final weeks of the 2020 election to support President Joe Biden and criticize then-President Donald Trump's COVID-19 policies. The "Recipient Type" column categorizes recipients, such as PACs, independent groups, political parties, or candidates. The final column, "View," indicates the recipient's political orientation, such as "Liberal" or "Democrat." No donations were made to Republican or Conservative groups during the 2019-2020 election cycle.

Table 3. FTX political donation in 2019-2020 campaign cycle.

Recipient	Total (USD)	Recipient Type	View
Future Forward USA	11,240,000	Carey	Liberal
Vote Tripling PAC	700,000	Carey	Liberal
Center for Essential Information	220,000	Outside Group	Liberal
DNC Services Corp	35,500	Political Party	Democrat
Biden Joe	2,800	Candidate (D-PRES)	Democrat
Georgia Federal Elections Cmte	1,560	Political Party	Democrat
Democratic Executive Cmte of Florida	780	Political Party	Democrat
Democratic Party of Ohio	780	Political Party	Democrat
Democratic Party of Virginia	780	Political Party	Democrat
Democratic Party of Arizona	780	Political Party	Democrat
Democratic Party of Nebraska	780	Political Party	Democrat
Minnesota Democratic Farmer Labor Party	780	Political Party	Democrat
Democratic Party of Colorado	780	Political Party	Democrat
Democratic Party of Pennsylvania	780	Political Party	Democrat
Democratic Party of Nevada	780	Political Party	Democrat
Democratic Party of North Carolina	780	Political Party	Democrat
Democratic Party of Wisconsin	780	Political Party	Democrat
Democratic Party of Texas	780	Political Party	Democrat
Casten Sean	100	Candidate (D-IL06)	Democrat
Democratic Congressional Campaign Cmte	25	Political Party	Democrat
Harris Kamala	5	Candidate (D-CAS1)	Democrat
Total	12,209,350		

Source: https://www.opensecrets.org/orgs/ftx-us/

Appendix A, *FTX Political Donations in 2021-2022 Campaign Cycle*, presents the FTX donation dataset for the 2021-2022 campaign cycle. During this period, FTX contributed a total of USD 75,389,555 to various political entities, marking a shift from the 2019-2020 cycle, where donations were exclusively made to Democratic and Liberal groups. In contrast, FTX's 2021-2022 donations were more diversified, with contributions reaching 394 unique recipients. The majority of these donations were directed towards "Lead PAC" entities, with 77 donations in this category. Political parties received 57 donations, while 15 donations went to "Outside

Group" entities, suggesting a strategic expansion beyond traditional political structures. FTX made 9 donations to "Carey" type entities and also contributed to various specific political candidates. Democratic-affiliated entities were the primary recipients, with 220 donations, followed by Republican-affiliated entities receiving 148 donations. Liberal entities received 14 donations, and Conservative entities received 10. Additionally, 2 donations were made to bipartisan entities, reflecting a broader political engagement.

At FTX, political donations were not limited to SBF, with several colleagues also significantly involved in US election financing. Nishad Singh, FTX's Director of Engineering, made notable contributions to Democratic campaigns. During the 2022 election cycle, Singh donated USD 8 million to Democratic candidates (Schwartz, 2022). Before his prominent role at FTX, Singh's political donations were modest, including a USD 2,700 contribution in 2018 to Rep. Sean Casten, D-Ill. In 2020, he also made a USD 1 million donation to Future Forward USA, a PAC supporting President Joe Biden's campaign, where he listed Alameda Research as his employer. His donations mirrored those of Bankman-Fried, who also contributed USD 5 million to the same pro-Biden PAC.

Ryan Salame, co-CEO of FTX Digital Markets, also played a major role in political donations. While SBF contributed USD 39 million to Democratic candidates during the 2022 midterms, Salame donated USD 23 million, primarily supporting Republican candidates (Schwartz, 2022). Michelle Bond, a former far-right Republican congressional candidate and Salame's romantic partner, received at least USD 400,000 in consulting fees from FTX Digital Markets, which Salame co-led (Robins-Early, 2022). Bankman-Fried was the second-largest donor to the Democratic Party, behind only George Soros (Kiernan, 2022).

2.4. FTX's Strategic Expansion: A Series of Tactical Acquisitions, Bailouts, and Investments

2.4.1. FTX's Acquisition of Blockfolio and Retail Cryptocurrency Trading

Since its inception in 2019, FTX swiftly made significant acquisitions within the cryptocurrency sector, aiming to expand its international presence and secure regulatory alignment across multiple jurisdictions. These acquisitions were driven by a strategic vision to enhance FTX's global reach and diversify its service offerings, ranging from customer access to technology integration and regulatory compliance.

One of the major acquisitions was Blockfolio, a leading mobile application for cryptocurrency investors and traders. Launched in 2014 by Edward Moncada, Blockfolio

allowed users to track their cryptocurrency portfolios across various exchanges and coins. By 2019, it had amassed over 5 million downloads, positioning itself as the top portfolio tracking app within the cryptocurrency ecosystem (LilMoonLambo, 2019). The app was known for its user-friendly interface, real-time data on market prices, and news updates, making it an essential tool for cryptocurrency enthusiasts.

The app offered key features such as price alerts and news updates tailored to specific coins or the broader cryptocurrency market, allowing users to stay informed and responsive to market shifts. In August 2020, as the app's popularity continued to grow, with downloads reaching 6 million, FTX acquired Blockfolio for USD 150 million. This strategic acquisition enabled FTX to integrate its trading capabilities into the Blockfolio platform, transforming it from a portfolio tracking app into a full-fledged trading and investment platform. The acquisition was a pivotal move in FTX's strategy to enhance its retail services, providing cryptocurrency investors with a more comprehensive platform. Following the acquisition, Blockfolio was rebranded to FTX, solidifying its connection to the FTX ecosystem and expanding the company's offerings within the retail space.

2.4.2. FTX's Acquisition and Subsequent Sale of LedgerX

LedgerX, a US-based cryptocurrency derivatives exchange platform, provided an institutional-grade platform for trading and clearing various derivative products, including options and swaps on digital assets. Co-founded in 2017 by Paul Chou and Juthica Chou, LedgerX was one of the first platforms to be regulated in the United States (Castillo, 2017), holding licenses from the CFTC, including a derivatives clearing organization license, a swap execution facility license, and a designated contract market license (CFTC, 2017b). The platform catered to both institutional and retail investors, offering Bitcoin options and futures contracts while maintaining high standards of regulatory compliance and transparency, which helped establish trust in the emerging cryptocurrency derivatives market.

In August 2021, FTX acquired LedgerX through its US subsidiary, FTX US, for a reported USD 298 million, acquiring Ledger Holdings, the parent company of LedgerX. Following the acquisition, the platform was rebranded as FTX US Derivatives. This move allowed FTX to expand its product offerings into cryptocurrency derivatives trading within the US market, aligning with its broader strategy to diversify its services and attract a wider range of users.

The acquisition provided FTX with immediate access to LedgerX's CFTC licenses, which was particularly advantageous, as obtaining such licenses independently can be a lengthy and complex process. By acquiring a licensed and compliant platform, FTX strengthened its position within the US regulatory framework. The move also expanded FTX's market reach by tapping into LedgerX's established client base, which included both institutional players and sophisticated retail traders. Leveraging LedgerX's trusted infrastructure and regulatory standing, FTX was able to provide secure and compliant trading solutions in the competitive derivatives market.

Moreover, following the acquisition, FTX aimed to leverage LedgerX's existing infrastructure to launch a US-based derivatives marketplace under the FTX brand. The goal was to create a unified platform where customers could seamlessly trade cryptocurrencies, futures, options, and other financial products, positioning FTX as a comprehensive one-stop shop for digital asset trading. This strategic move not only strengthened FTX's presence in the highly competitive US market but also showcased its commitment to adhering to regulatory standards in a jurisdiction with stringent regulations. It highlighted FTX's ambition to be a leader in the cryptocurrency derivatives space, reinforcing its regulatory compliance as a key differentiator.

However, in 2023, FTX and its creditors announced the completion of the sale of its cryptocurrency derivatives exchange arm, LedgerX, to M7 Holdings, a subsidiary of Miami International Holdings (MIH), for approximately USD 50 million. This sale marked a substantial loss for FTX, as it had purchased LedgerX only two years earlier, resulting in a USD 248 million decrease in value. MIH, an American exchange group that operates multiple trading platforms and holds a US commodities exchange license, made this acquisition as part of its broader strategy to enter the cryptocurrency trading market. MIH had previously expanded its portfolio by acquiring the Minneapolis Grain Exchange in 2020, and with the purchase of LedgerX, it aimed to expand its footprint into the rapidly growing digital asset space.

The proceeds from the sale of LedgerX were used to pay off creditors in the bankruptcy proceedings of FTX, which had become insolvent in 2022. The sale, which was conducted through a bankruptcy auction, highlights the significant financial difficulties FTX faced following its collapse and the challenges of maintaining its ambitious expansion strategy in the face of financial instability (Shome, 2023).

2.4.3. The Acquisition of Quoine and Its Impact on Japan's Cryptocurrency Market

Quoine was a key player in Japan's cryptocurrency market, founded in 2014 by Mike Kayamori and Mario Gomez-Lozada. The company quickly established itself as a leading fintech firm, offering a variety of financial services centered around blockchain technology and digital assets. One of its notable achievements was the launch of Liquid, one of Japan's first cryptocurrency exchanges, recognized for its innovative platform and comprehensive trading options.

Quoine was also one of the first cryptocurrency exchanges to be licensed by Japan's Financial Services Agency, a significant milestone that enhanced its credibility as a secure and trustworthy platform for cryptocurrency trading. Liquid offered a wide range of cryptocurrencies, along with advanced features such as margin trading and fiat-to-crypto transactions, serving both retail and institutional traders. While based in Japan, Quoine aimed for a global presence, supporting multiple fiat currencies and catering to an international user base (Quoine, 2019).

In 2021, Liquid experienced a significant security breach that resulted in the loss of over USD 90 million in cryptocurrency assets, marking the second major security incident for the company. The first occurred in November 2020, when Liquid was targeted in a cyber-attack involving a DNS provider compromise. The attacker used social engineering techniques to gain control of Liquid's DNS infrastructure. Once inside, the hacker launched a phishing scheme to acquire the credentials of Liquid's employees, ultimately accessing the internal network. While some personal customer data was exposed during the 2020 breach, no funds were reported as stolen (Cimpanu, 2021).

In response to the breach, FTX provided a USD 120 million emergency loan to assist Liquid. This assistance set the stage for FTX to acquire Liquid, giving it an opportunity to enter the Japanese market and inherit Quoine's crucial regulatory license. In February 2022, FTX completed the acquisition of Quoine, marking a strategic expansion into the Asian markets, with a specific focus on Japan. This acquisition was particularly significant given SBF's past success in exploiting Bitcoin price discrepancies between international markets during his time with Alameda. The move aligned with FTX's broader strategy to strengthen its presence in Asia (Browne, 2022).

Quoine's advanced trading features and diverse range of services complemented FTX's existing offerings, creating a broader suite of products for its global customers. As part of its ongoing expansion strategy, FTX used the acquisition not only to solidify its position in Japan

but also as a strategic entry point into other Asian markets. This acquisition provided FTX with immediate regulatory approval in Japan, which is vital for operating legally and building trust with local customers. Quoine's established user base further accelerated FTX's market penetration in the region (Quoine, 2019).

The technological infrastructure of Quoine was seamlessly integrated with FTX's platform, enhancing the efficiency of operations and expanding the service offerings for users. This acquisition marked a significant step in FTX's goal of becoming a global leader in the cryptocurrency exchange market. It also allowed FTX to diversify its geographic presence, reducing reliance on any single market. Following the acquisition, FTX planned to fully integrate Quoine's operations into its global framework, leveraging the strengths of both companies to offer enhanced services. By combining FTX's innovative trading products with Quoine's regulatory-compliant platform, the integration aimed to provide a more robust experience for users. At its peak in July 2021, FTX had over one million users and was the third-largest cryptocurrency exchange by trading volume (IQ wiki, 2022).

2.4.4. FTX's Failed Acquisition of Bitvo: A Strategic Move in the Canadian Crypto Market

Bitvo, launched in 2018 in Alberta, Canada, quickly gained recognition as a cryptocurrency exchange known for its user-friendly platform and comprehensive trading services. The platform stood out for its strong security measures, efficient trading system, and emphasis on customer service. Bitvo was registered as a restricted dealer under the securities laws of all Canadian provinces and territories and was also registered with FINTRAC, Canada's financial intelligence agency, as a money services business in the virtual asset service provider category (Knight, 2022). Designed to be accessible to both novice and experienced traders, Bitvo offered trading in popular cryptocurrencies such as Bitcoin, Ethereum, and more, along with features like same-day fiat withdrawals and deposits. One of its unique offerings was the Bitvo Cash Card, which allowed users easy access to their funds. Operating under Canadian regulations, Bitvo adhered to rigorous compliance standards, enhancing its reputation for trustworthiness. The platform also provided 24/7 customer support, a key advantage in the fast-paced crypto market.

In June 2022, FTX sought to acquire Bitvo to expand its global presence and enter the Canadian cryptocurrency market. By acquiring Bitvo, FTX would have gained access to a regulated platform and its established customer base, enabling faster market penetration in

Canada. This move aligned with FTX's broader global strategy. However, after FTX's bankruptcy announcement on November 11, 2022 (Abrams, 2023), Bitvo terminated the acquisition deal on November 15, 2022 (Bitvo, 2022).

2.4.5. FTX's Financial Deal and BlockFi's Struggles Amid Crypto Downturn

BlockFi, founded in 2017 by Zac Prince and Flori Marquez, was a digital asset lender based in Jersey City, New Jersey. Specializing in cryptocurrency-backed loans and wealth management, it became a major player in the industry, reaching a valuation of USD 3 billion at its peak (Bambysheva, 2021). However, the cryptocurrency market downturn in 2022, where Bitcoin's value plummeted from nearly USD 68,000 to below USD 16,000, exposed vulnerabilities in platforms like BlockFi. Initially supported by FTX, which provided financial aid to several crypto firms, BlockFi was left without rescue options when FTX itself collapsed (Newbery, 2021).

FTX and BlockFi had a notable financial relationship. FTX extended a USD 400 million credit line to BlockFi and secured an option to acquire the company. The acquisition terms included a base price of USD 15 million, with the possibility of rising to USD 240 million, contingent on BlockFi meeting specific targets, including key regulatory approvals and asset growth (T. Wang, 2022). This deal reflected FTX's strategy to stabilize struggling crypto lenders while consolidating its influence in the market. The agreement underscored FTX's pivotal role in the crypto industry during a period of financial instability.

BlockFi's bankruptcy revealed the extent of its exposure to FTX and Alameda Research, with loans valued at USD 671 million and an additional USD 355 million in digital assets locked on FTX's platform. As of January 2023, BlockFi reported assets of USD 415.9 million tied to FTX and USD 831.3 million in loans to Alameda (Peshkar, 2023).

2.4.6. The Fall of Three Arrows Capital: A Crypto Hedge Fund's Collapse Amid Market Turmoil

Three Arrows Capital (3AC), a prominent hedge fund based in Singapore, was a major player in the cryptocurrency market. Founded in 2012 by Su Zhu and Kyle Davies, both of whom had traditional finance backgrounds, the fund initially focused on trading emerging market currencies but shifted to cryptocurrencies as the sector grew. Known for its high-risk, high-return strategies, 3AC became heavily involved in crypto trading, lending, and market-making activities. It gained significant attention for its bullish investments in Bitcoin and

Ethereum and expanded into venture capital, particularly in DeFi projects, further establishing itself as an influential force in the industry.

In 2022, 3AC's downfall began as the cryptocurrency market entered a severe bear market, exposing the fund to substantial liquidity issues. Its highly leveraged positions quickly became unsustainable as asset prices declined. Unable to meet margin calls from lenders, 3AC defaulted on large loans from crypto lending platforms, ultimately leading to the liquidation of its assets (Sigalos, 2022a). The collapse of 3AC was one of the most impactful in the crypto space, highlighting the dangers of leveraging and speculative investments in such a volatile market. The fallout affected lenders, investors, and other industry participants, including Celsius, which had loaned USD 75 million to 3AC before its failure. Celsius itself declared bankruptcy following the collapse of LUNA and 3AC (Copeland et al., 2022).

While the primary cause of 3AC's collapse was the broader market downturn and its exposure to volatile assets, some of its founders, Zhu Su and Kyle Davies, claimed that FTX and its trading arm, Alameda Research, played a role in exacerbating the fund's financial troubles (Eckl, 2022). They argued that FTX and Alameda targeted 3AC's positions, driving down the value of assets held by the fund and accelerating its liquidity crisis (Haqshanas, 2022).

2.4.7. The Rise and Fall of Voyager Digital: FTX Ties, Bankruptcy, and Unfulfilled Promises

Voyager Digital Ltd. was a leading player in the cryptocurrency industry, providing a diverse range of services, including a popular trading platform, asset management, and custody solutions. Founded in 2017 by industry veterans Stephen Ehrlich (CEO), Gaspard de Dreuzy, and Oscar Salazar—co-founder of Uber (Arif, 2023)—the company aimed to offer an efficient, user-friendly platform for trading cryptocurrencies.

Voyager's flagship product was its mobile app, enabling commission-free trading across numerous digital currencies. The platform utilized an aggregation system to scan multiple exchanges, securing the best trade execution for users. Voyager's interest program allowed account holders to earn passive income by generating interest on their crypto assets. The ecosystem also featured VGX, Voyager's native token, which offered exclusive benefits like reduced trading fees and enhanced interest rates as part of the company's loyalty program.

Beyond trading, Voyager provided additional features, including crypto payment solutions, custody services, and interest-bearing accounts on select digital assets, making it an all-encompassing platform for retail investors. To fuel its growth, the company raised funds

through private investment rounds and public markets. In 2019, Voyager went public on the Toronto Stock Exchange via a reverse takeover, a strategic move reflecting the trend of crypto firms leveraging public markets for capital. At its peak, Voyager achieved a valuation in the hundreds of millions, underscoring its prominence and the surging investor enthusiasm in the expanding cryptocurrency sector.

Voyager's connection with FTX gained prominence in 2022 during a period of financial instability in the cryptocurrency market. Voyager faced severe distress after significant exposure to the crypto hedge fund 3AC, which defaulted on a loan worth hundreds of millions of dollars, deepening Voyager's financial troubles. As a result, Voyager filed for bankruptcy in July 2022, leaving its customers facing substantial potential losses.

In a bid to capitalize on the situation, FTX and its affiliate Alameda Research proposed a joint plan to acquire Voyager's assets and take over its customer accounts. This proposal aligned with FTX's broader strategy of acquiring distressed crypto assets at discounted prices to strengthen its market position and expand its user base. The acquisition was presented as a potential relief for Voyager's customers, offering them a pathway to recover some of their funds amid bankruptcy proceedings.

Despite the promise of financial recovery for Voyager's users, the proposed acquisition faced regulatory scrutiny and challenges. The move highlighted FTX's aggressive expansion approach and its efforts to dominate the cryptocurrency market during a period of unprecedented volatility. The financial and legal troubles of FTX, which surfaced later in 2022, ultimately derailed its acquisition of Voyager Digital. Both companies declared bankruptcy during the cryptocurrency market crash, with Voyager filing in July 2022, four months before FTX. Following Voyager's bankruptcy filing, the company demanded repayment of outstanding loans from FTX and its affiliated hedge fund, Alameda Research. Court records revealed that FTX paid Voyager USD 248.8 million in September, USD 193.9 million in October, and an interest payment of USD 3.2 million in August (Knauth, 2023).

After FTX's collapse, Voyager's assets were put up for auction, where Binance.US, a subsidiary of FTX's competitor Binance, emerged as the highest bidder. Binance.US agreed to purchase Voyager's assets for USD 1 billion, offering hope to Voyager's 1.7 million customers. However, this deal faced significant opposition from Alameda Research, federal regulators, and multiple states throughout the US (Schickler, 2023).

In April 2023, Binance.US withdrew from the agreement, citing an unpredictable and challenging regulatory environment (Nishant et al., 2023). This marked the end of a tumultuous

series of events, leaving Voyager's customers, to date, uncertain about the resolution of their claims.

2.4.8. SkyBridge Capital: The Firm's Evolution and Its Cryptocurrency Pivot with FTX

SkyBridge Capital, founded in 2005 by Anthony Scaramucci, emerged as a prominent player in the alternative investment landscape. Known for its focus on hedge funds and alternative investment strategies, the firm gained recognition for providing access to high-quality investment opportunities for institutions and individuals alike. Scaramucci, a seasoned financier, brought years of experience in investment banking to SkyBridge before achieving further prominence through a brief tenure as the White House Director of Communications during Donald Trump's first presidency.

Under Scaramucci's leadership, SkyBridge expanded its influence, hosting high-profile industry events such as the SALT Conference, a global forum for leaders in finance, technology, and public policy. The firm also diversified its portfolio, eventually exploring the cryptocurrency sector as digital assets gained mainstream traction.

In a pivotal development, SkyBridge Capital deepened its foray into cryptocurrencies through a strategic partnership with FTX Ventures, the investment arm of the now-defunct cryptocurrency exchange FTX. In September 2022, FTX Ventures acquired a 30% equity stake in SkyBridge, marking a significant alignment between traditional financial expertise and the burgeoning crypto industry (Crawley, 2022b).. The deal, valued at USD 45 million, symbolized SkyBridge's growing commitment to integrating digital assets into its investment framework.

As part of the agreement, SkyBridge pledged to allocate USD 40 million toward purchasing cryptocurrencies, further signaling its shift toward embracing blockchain-based financial instruments. Both Anthony Scaramucci and FTX founder SBF hailed the partnership as a transformative step, envisioning a future where traditional and digital finance could converge to offer innovative investment solutions (Aliaj & Oliver, 2022).

This collaboration reflected the growing intersection of established financial institutions with the volatile yet promising world of cryptocurrency. However, the collapse of FTX in late 2022, amid allegations of fraud and mismanagement, cast a shadow over the partnership. Despite the fallout, the deal underscored SkyBridge Capital's ambition to adapt to evolving market trends and remain relevant in a rapidly changing financial landscape.

2.4.9. Robinhood's Rise and SBF's High-Stakes Investment

Founded in April 2013 by Vladimir Tenev and Baiju Bhatt, Robinhood emerged as a groundbreaking investment platform, transforming the financial trading industry with its intuitive app and commission-free trading model (Figure 13). Driven by a mission to democratize finance, Robinhood sought to make investing accessible to everyday individuals, breaking down barriers traditionally associated with stock trading.

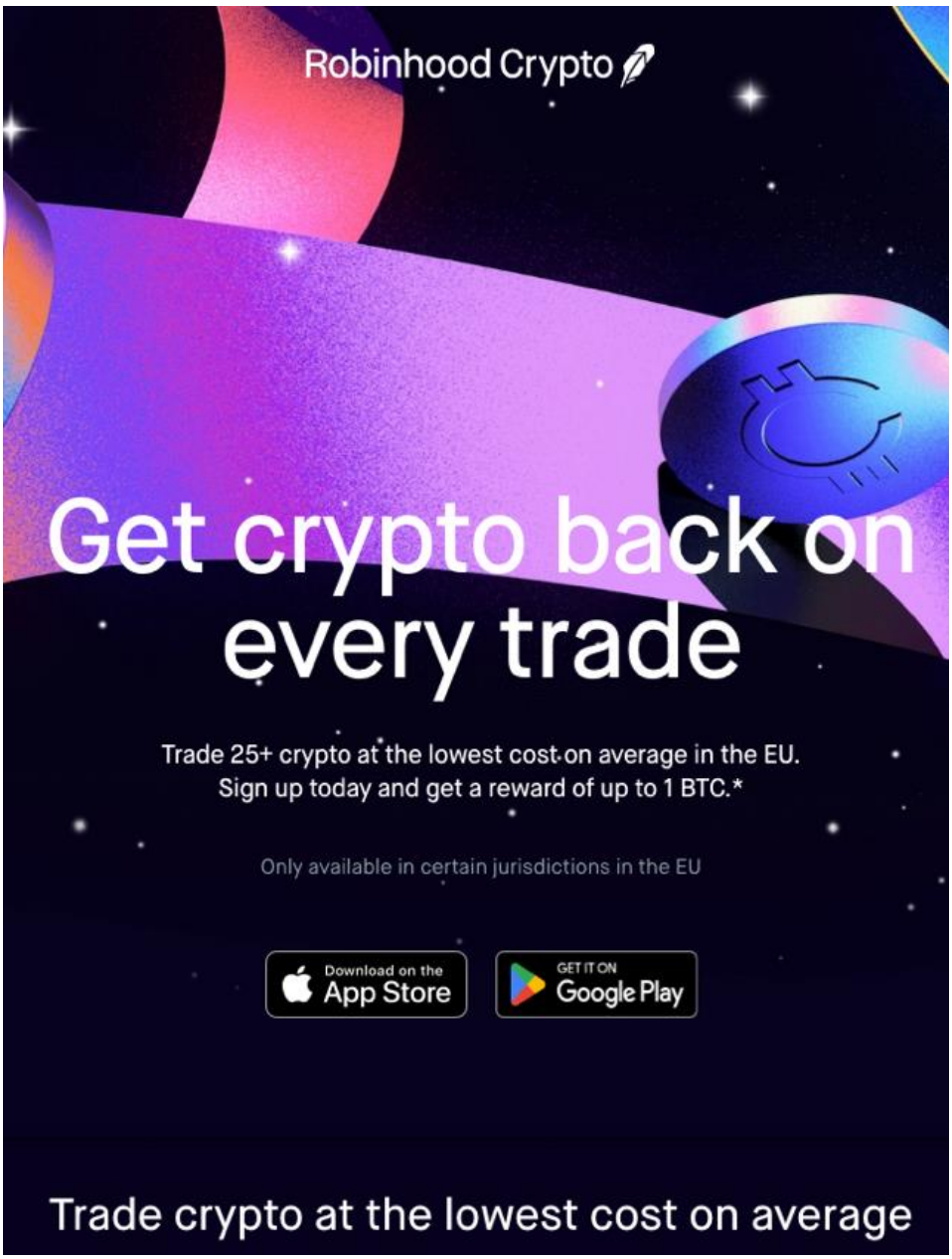

Figure 13. Robinhood Crypto app, accessible via the https://www.robinhood.com website.

Source: Screenshot taken by Shobhit Navani on December 17, 2023.

Initially focusing on equities, Robinhood provided users an easy entry point to trade stocks and exchange-traded funds (ETFs) without incurring the fees charged by conventional brokerage firms. Its innovative approach resonated with younger, tech-savvy investors, leading to rapid adoption.

As the popularity of cryptocurrencies grew, Robinhood expanded its offerings to include crypto trading, allowing users to buy and sell digital assets like Bitcoin, Ethereum, and Dogecoin with zero transaction fees. This strategic move appealed to crypto enthusiasts and positioned Robinhood as a competitive player in the digital finance landscape. To further enhance its crypto services, Robinhood introduced a crypto wallet feature, enabling users to transfer cryptocurrencies to external wallets—a critical function for advanced traders. Despite these expansions, the platform retained its hallmark user-friendly interface, appealing to both novice and seasoned investors.

In May 2022, SBF made headlines by acquiring a 7.6% stake in Robinhood, amounting to a USD 648 million investment. This acquisition aligned with FTX's broader strategy to integrate traditional stock trading with the rapidly evolving cryptocurrency sector, signaling a convergence of conventional and digital finance.

However, the partnership faced challenges following the collapse of FTX in late 2022. In the aftermath, brokerage firm Robinhood executed a significant transaction to repurchase 55.3 million shares previously owned by SBF. These shares, valued at USD 605.7 million, were reclaimed from the United States Marshal Service at $10.96 per share. This buyback followed authorization by the United States District Court for the Southern District of New York and marked a critical step in Robinhood regaining control over its equity (George, 2023).

In all, Robinhood's journey exemplifies resilience and adaptability, maintaining its commitment to financial accessibility while navigating the challenges of integrating traditional and digital trading realms.

2.5. FTX's Brand and Marketing Strategy: Leveraging Sports, Celebrities, and Major Sponsorships

FTX launched several high-profile marketing and publicity campaigns, focusing heavily on the sports and entertainment sectors, to boost its brand visibility and establish credibility. These initiatives were part of a broader strategy aimed at popularizing cryptocurrency trading and positioning FTX as a dominant player in the industry. The company's marketing efforts were crucial in rapidly expanding its user base and increasing brand recognition. By

successfully portraying itself as a mainstream and trustworthy platform, FTX attracted both experienced traders and newcomers. Its sports sponsorships and celebrity endorsements played a key role in bringing cryptocurrencies into the public spotlight, linking them to renowned figures and respected institutions.

For example, the Miami Heat, a professional basketball team with three NBA championships (2006, 2012, 2013) and notable players like Dwyane Wade, LeBron James, and Shaquille O'Neal, became part of a major sponsorship shift in 2021. FTX acquired the naming rights to the Heat's arena for USD 135 million over 19 years, renaming it FTX Arena (Figure 14). This deal highlighted the increasing influence of cryptocurrency in sports sponsorship (Hart, 2022). In November 2022, the Miami Heat ended their partnership with FTX following the exchange's bankruptcy. This decision was driven by FTX's financial turmoil and legal issues. A federal bankruptcy court later terminated the naming rights agreement, allowing the removal of FTX's branding from the arena.

Figure 14. FTX Arena in Miami.

Source: Heat Nation Website at: https://heatnation.com/team-news/report-miami-heats-arena-sponsor-files-for-bankruptcy/

Moreover, in 2021, Mercedes Formula 1 signed a sponsorship deal with FTX, featuring the cryptocurrency exchange's logo on cars, uniforms, hats, and other merchandise. However, following FTX's bankruptcy declaration and a SEC investigation into alleged misappropriation of customer funds, Mercedes took swift action in 2022 to distance itself from FTX (Nole, 2022).

FTX's Super Bowl advertisement, aired during the 2022 event, marked a major marketing push for the cryptocurrency exchange, reaching millions of viewers (Schaffer, 2022). The commercial featured comedian Larry David humorously resisting technological and political innovations throughout history, ultimately rejecting an offer to invest in FTX. David's line, "Yeah, I don't think so, and I'm never wrong about this stuff. Never," emphasized his skepticism. The ad encouraged viewers to "not be like Larry" and embrace new technology. Ironically, by 2023, it was revealed that Larry was right, as FTX declared bankruptcy (Sherman & Tidy, 2022).

Interestingly, advertising during the Super Bowl allowed FTX to position cryptocurrency as an emerging sector in the broader economy. With over 100 million viewers, the event provided an unparalleled opportunity for brand exposure. Super Bowl ads, often analyzed in the media, can become part of popular culture, amplifying a brand's reach. Despite the high cost—often millions for just a 30-second slot—FTX's decision to advertise aimed to boost brand recognition beyond the traditional crypto market, highlighting the growing trend of crypto companies seeking mainstream visibility and acceptance.

Before its collapse, FTX attracted numerous celebrities and athletes for promotional campaigns, including Tom Brady, Gisele Bündchen, Shaquille O'Neal, Stephen Curry, Naomi Osaka, and others (AP, 2022). Brady and his ex-wife, Gisele Bündchen, signed long-term deals with FTX, receiving significant equity and payments in cryptocurrency involvement (Reuters, 2023). These partnerships were part of FTX's strategy to increase brand visibility and trust (FTX Trading, 2021). FTX also worked with investor Kevin O'Leary, who lost USD 15 million when the exchange went bankrupt (Quarmby, 2022).

Meanwhile, Alex Grebnev, a tech entrepreneur, partnered with FTX's Alameda Research in 2021, securing funding for his projects, Oxygen and Maps.me, which offered digital payments and crypto-related services (Lawson, 2023). However, after the collapse of FTX in 2022, both projects and their tokens saw their value plummet, further impacting the broader crypto market.

2.6. The FTX Collapse

In 2022, CoinDesk, a prominent news outlet specializing in Bitcoin and digital currencies, raised concerns about FTX's financial stability following a CoinDesk article (Allison, 2022) that uncovered details from a private financial document related to Alameda Research. The document, obtained by CoinDesk, allegedly revealed the deep financial ties

between FTX and Alameda. The report disclosed that Alameda's holdings included over USD 5 billion in FTX's native cryptocurrency, FTT. This amount included USD 3.66 billion in "unlocked FTT" and USD 2.16 billion in FTT used as collateral, making FTT the largest asset on Alameda's balance sheet. The article also emphasized that Alameda's investments were heavily dependent on FTT, as opposed to more traditional assets such as fiat currency or other cryptocurrencies.

In response to these concerns, Carolyn Ellison, CEO of Alameda Research, publicly addressed the company's balance sheet on November 6, 2022, via Twitter (Figure 15). She aimed to reassure users regarding the firm's operational stability in light of the growing scrutiny.

Figure 15. Tweet from Caroline Ellison on November 6, 2022, available at: https://twitter.com/carolinecapital/status/1589264375042707458.

Source: Screenshot taken by Shobhit Navani on December 17, 2023.

The pivotal moment that led to FTX's collapse occurred following a tweet by Changpeng Zhao (CZ), the founder and CEO of Binance, the world's largest and most influential cryptocurrency exchange (Figure 16) (Zandt, 2023). Binance had been one of FTX's investors. On November 6, 2022, CZ announced that Binance would sell all of its holdings in FTT, FTX's native token. This decision was reportedly made after reviewing revelations about FTX's financial instability and its alleged mishandling of customer funds. The tweet set off rumors suggesting that FTX, a leading crypto exchange, was on the brink of bankruptcy. These rumors quickly gained traction, causing a wave of chaos and uncertainty that severely impacted the crypto market.

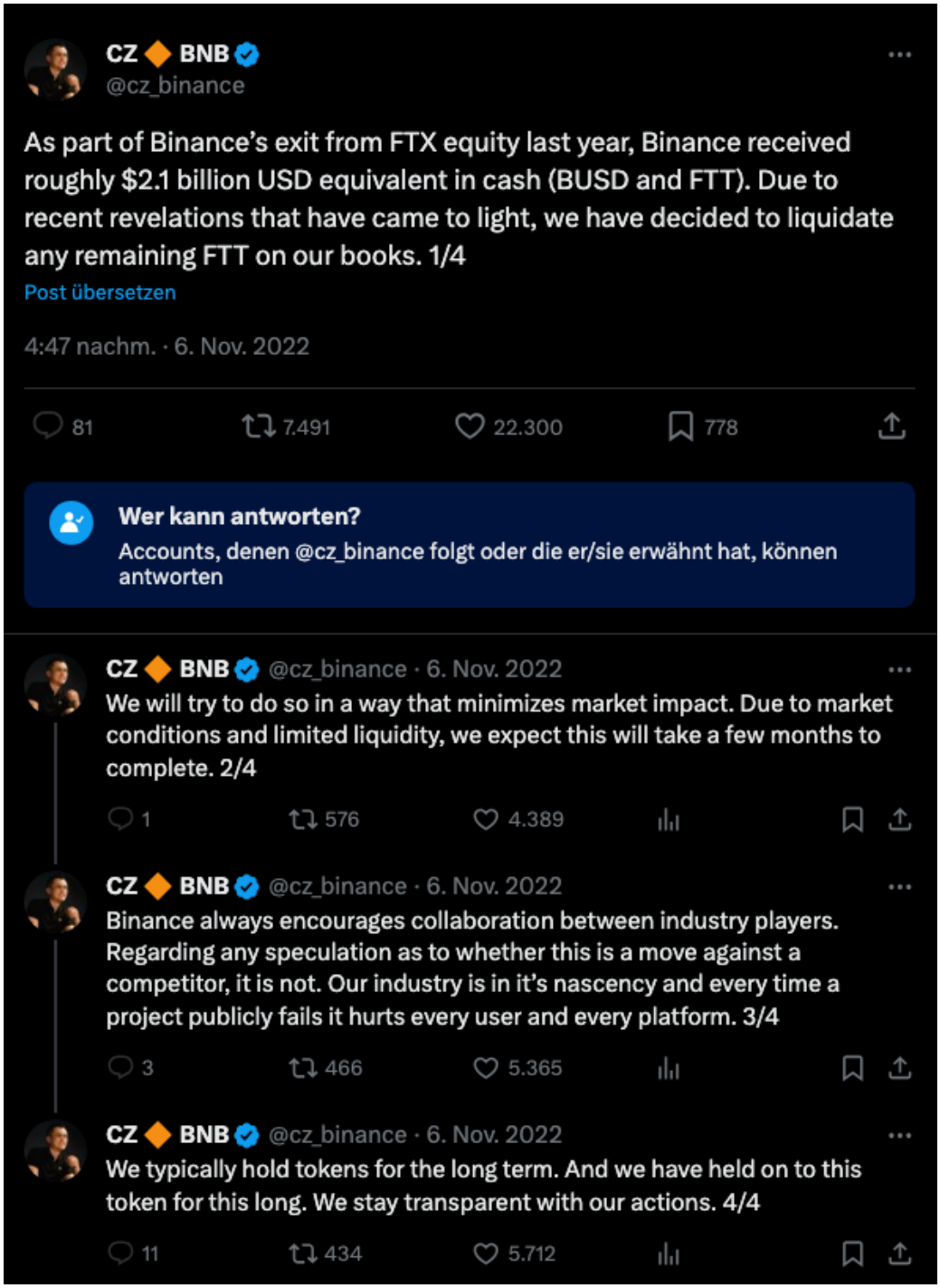

Figure 16. Tweet from Changpeng Zhao on November 6, 2022, available at: https://twitter.com/cz_binance/status/1589283421704290306.

Source: Screenshot taken by Shobhit Navani on December 18, 2023.

The rumors, initially unverified, spread rapidly within the crypto community. Given CZ's influential role in the industry, the speculation quickly gained attention. It led to widespread panic among FTX users, investors, and the broader cryptocurrency market. FTX,

with its large trading volumes and user base, was a key player in the crypto ecosystem. As concerns about the potential truth of the rumors grew, many FTX users rushed to withdraw their funds, putting immense pressure on FTX's liquidity.

The rumors not only eroded confidence in FTX but also contributed to a broader market downturn. The cryptocurrency sector, already struggling in a bear market, saw increased volatility, and the prices of various cryptocurrencies plunged. A bear market, characterized by prolonged declines in asset prices, was particularly evident in 2022. It reflected widespread pessimism and negative sentiment among investors, leading to a downward spiral in market prices and a significant drop in the value of most cryptocurrencies.

CZ's tweet and the ensuing actions led to a rapid decline in the value of FTT and a massive surge in withdrawal requests from FTX users, many of whom feared their funds were at risk. FTX struggled to meet these demands, revealing deeper financial mismanagement within the exchange. In response, FTX sought assistance from Binance, which initially signed a non-binding agreement to acquire the troubled exchange to cover its liquidity shortfall. However, on November 9, 2022, Binance quickly backed out of the deal after reviewing FTX's financial situation and discovering the full extent of its problems.

The next day, the Bahamian regulator froze the assets of FTX's non-US operations, further complicating the crisis (N. Wang, 2022). Within days of CZ's tweet, FTX filed for bankruptcy, and SBF resigned as CEO on November 11, 2022. This was a cataclysmic event within the cryptocurrency space as FTX, the Bahamas-based exchange, folded and the company's CEO, SBF was arrested and charged with the misappropriation of billions of dollars in client funds. Amidst the chaos surrounding the company's collapse, a substantial amount of cryptocurrency assets, valued in the hundreds of millions, were illicitly stolen. The perpetrator of this significant theft remains unidentified, despite visible and ongoing efforts to launder the stolen assets on the blockchain.

2.6.1. The FTX Breach

The theft began on the evening of November 11, 2022, just hours after SBF publicly announced FTX's bankruptcy and the downfall of its sister company, Alameda Research (Figure 17). Approximately 9,500 ETH, worth about USD 15.5 million at the time, was transferred from an FTX-associated wallet to a newly created one. This marked the beginning of a series of unauthorized transactions that eventually resulted in the loss of USD 477 million from FTX's funds.

Figure 17. Tweet from SBF on November 11, 2022, available at: https://twitter.com/SBF_FTX/status/1591089317300293636.

Source: Screenshot taken by Shobhit Navani on December 19, 2023.

The hackers responsible for the FTX breach used the address **0x59ABf3837Fa962d6853b4Cc0a19513AA031fd32b** to initiate the hack. Following the initial transfer, they sent 50,000 ETH to an intermediate address, **0x866eeecd1f248d1a0a2e0263f13594a6b8b7c01a**, before swapping 49,990 ETH for renBTC on the decentralized exchange 1inch. This enabled the hackers to move the funds to the Bitcoin blockchain. They converted USD 57 million into BTC using the RenBridge protocol and sent the proceeds to three addresses (Scorechain, 2022):

- **bc1qaq09p8qy97pf9rhnwtxvj7htqhmyejvv6n0702** (received 2,444.55 BTC, worth USD 40 million)
- **bc1qvd2kntzzz6y223av68h4xx8zwhxmcncy3gpedg** (received 1,068.93 BTC, worth USD 17 million)
- **bc1qexzss0wh5lz0q5emcm7rp29h9tqrc0tulvpp4t** (received 1,022.62 BTC, worth USD 16 million)

In total, approximately USD 74 million was processed through RenBridge, which is associated with Alameda Research. Decentralized cross-chain bridges like RenBridge provide an alternative to traditional exchanges for transferring value across different blockchains, operating without central oversight. These bridges have increasingly become instrumental in money laundering schemes. The tactic of "chain-hopping," where illicit funds are transferred between blockchains to evade detection, is typically facilitated by the anonymous use of crypto asset exchanges (Robertson, 2022).

Until 2022, RenBridge had been used to launder over USD 540 million in stolen crypto assets, including USD 33.8 million taken from the Japanese crypto exchange Liquid in August 2021. Notably, after the hack of Liquid, FTX stepped in to bail out the exchange and eventually took over its operations.

2.6.2. The Regulatory Challenges of Blockchain Bridges: A Focus on RenBridge

Blockchain bridges, such as RenBridge, present significant regulatory challenges due to their decentralized nature. These cross-chain transactions are processed by a network of pseudonymous validators, known as Darknodes, rather than a centralized governing entity. A cross-chain bridge enables the transfer of assets and data between two different blockchains that are not natively compatible (Blasco & Fett, 2019; Fosso Wamba et al., 2020). This allows for the movement of tokens, coins, or other forms of data from one blockchain to another.

The process works by locking tokens on the originating blockchain, effectively removing them from circulation. On the destination chain, equivalent tokens—often referred to as "wrapped" tokens—are minted. These wrapped tokens represent the original tokens but are usable within the ecosystem of the new blockchain. To transfer assets back to the original blockchain, the wrapped tokens are typically burned (destroyed), and the original tokens are unlocked and returned to the user (Blasco & Fett, 2019). This mechanism creates a unique set of regulatory challenges, particularly in the areas of asset tracking, AML, and the oversight of decentralized networks.

Cross-chain bridges come in two primary types: (1) trusted bridges, these rely on a central authority or a group to manage the bridge, with trust placed in these entities to secure assets and ensure the proper process of locking and minting tokens; and (2) trustless bridges, operating in a decentralized manner, trustless bridges utilize smart contracts and cryptographic proofs to automate the transaction process without the need for a central overseer (Li et al., 2024; Zhang et al., 2024; Zilnieks & Erins, 2023).

Cross-chain bridges play a crucial role in enhancing blockchain interoperability, a key aspect of the blockchain ecosystem's evolution (Zhang et al., 2024). They provide greater flexibility, enabling users to interact with multiple blockchain platforms without being confined to a single ecosystem. However, these bridges also come with significant security risks. As they manage and lock large volumes of assets, they can become prime targets for hackers. Past incidents of bridge exploits have resulted in major financial losses, highlighting the importance of robust security measures in their design and operation (Li et al., 2024).

2.6.3. The Role of Darknodes and Stablecoins in Blockchain Ecosystems

In the blockchain space, Darknodes are nodes that operate anonymously to validate and facilitate transactions across different blockchain networks. These nodes are referred to as "dark" because, unlike more transparent blockchain nodes such as those in Bitcoin or Ethereum, their identities and the identities of their operators remain hidden. This anonymity provides a layer of privacy and protection against censorship or targeted attacks on the network (BitDegree, 2023; RenProject, 2022).

Darknodes play a critical role in the validation of cross-chain transactions, ensuring the legitimacy of asset transfers and confirming that the conditions required for the transfer have been met. They are essential in processes like locking, minting, and burning tokens during cross-chain asset transfers. By maintaining anonymity, Darknodes contribute to decentralization and the prevention of any single point of failure that could threaten the integrity of the network (Ou et al., 2022; RenProject, 2022).

While Darknodes support the decentralized and privacy-focused nature of blockchain ecosystems, their anonymity also presents regulatory challenges. This privacy can be exploited for illicit activities, such as money laundering or evading sanctions, raising concerns among regulatory authorities. As a result, the use of Darknodes and the platforms that incorporate them may face increased scrutiny from regulators aiming to mitigate potential abuses (BitDegree, 2023; Ou et al., 2022).

The Financial Action Task Force (FATF) has raised concerns about money laundering through chain-hopping in its report on risks associated with virtual assets (Navazan, 2022). While the regulation of such activities remains uncertain, the transparency inherent in decentralized systems allows for the tracking and tracing of transactions across cross-chain bridges. In the cryptocurrency space, stablecoins are designed to maintain a stable value, unlike the volatility seen in assets like Bitcoin or Ethereum. This stability is typically achieved by pegging the stablecoin's value to a more stable asset, such as a fiat currency (e.g., the USD), a commodity (e.g., gold), or a basket of assets.

There are three main types of stablecoins. Fiat-collateralized stablecoins are backed by fiat currency at a 1:1 ratio, meaning for every stablecoin issued, an equivalent amount of fiat currency is held in reserve. Tether (USDT) and USD Coin (USDC) are prominent examples of this type. This model ensures that the stablecoin maintains a consistent value equivalent to the underlying fiat currency, though it requires trust in the issuer to maintain the necessary reserves

(De Blasis et al., 2023; Grobys et al., 2021; Hafner et al., 2024). Crypto-collateralized stablecoins, on the other hand, are backed by other cryptocurrencies, and to account for their volatility, they often use an over-collateralization mechanism. This means they hold more reserve cryptocurrency than the total value of the stablecoins issued, offering a buffer against price fluctuations. DAI is a well-known example of a crypto-collateralized stablecoin (De Blasis et al., 2023; Hafner et al., 2024). Finally, algorithmic stablecoins do not rely on collateral but instead use algorithms to control the supply of tokens in circulation to maintain a stable value. When the price rises above the peg, the algorithm increases the supply of the stablecoin, and when the price falls below the peg, it decreases the supply. This approach aims to stabilize the token's value in a manner similar to the way central banks manage the value of fiat currencies (De Blasis et al., 2023; Grobys et al., 2021).

The majority of the stolen assets remained dormant until just before the start of SBF's trial, at which point their movement resumed. The thief quickly began laundering the funds to evade potential seizure by authorities. Of the stolen assets, USD 434 million consisted of stablecoins and other tokens, which are typically subject to freezing by their issuers in cases of suspected theft. For example, Tether, the issuer of USDT, was able to freeze USD 31.5 million worth of stolen USDT shortly after the theft occurred. To avoid further seizures, the thief exchanged the stolen tokens for Ethereum, a cryptocurrency native to individual blockchains that is not subject to issuer freezes. If the thief had used CEXs like Binance or Coinbase to swap the tokens, asset seizure would have been likely. Therefore, the perpetrator turned to DEXs such as Uniswap and Pancake Swap, which allow for anonymous trading of stolen tokens for native assets, without the risk of asset seizure (Elliptic, 2023b, 2023a; Greenberg, 2023).

After securing the stolen assets from confiscation, the thief began transferring them across different blockchains to complicate tracking and access blockchain services for further laundering. Using decentralized cross-chain bridges like Multichain and Wormhole, the thief consolidated assets from Binance Smart Chain and Solana into an Ethereum account. Within three days, they accumulated 245,000 ETH, worth around USD 306 million, though some tokens were confiscated and exchange costs reduced the total. After a five-day lull, 65,000 ETH was transferred to the Bitcoin blockchain via the RenBridge cross-chain bridge, which has been linked to over half a billion dollars in illicit laundering. The thief converted the Ether into 4,536 Bitcoins, with a significant portion (2,849 BTC) laundered through mixers like Chip Mixer to hinder traceability. An additional 180,000 ETH remained idle until it appreciated to USD 300 million by September 30th, 2023, with the laundering process continuing as Ether was converted to Bitcoin and passed through mixers (Elliptic, 2023b, 2023a; Greenberg, 2023).

2.6.4. FTX Theft: Laundering of Stolen Assets

After FTX's collapse, the thief switched to the THOR Swap cross-chain bridge, converting 72,500 ETH (worth USD 120 million) to Bitcoin. THOR Swap suspended its interface in October 2023, citing concerns over illicit fund movement, but the thief continued using THOR Chain via alternative methods. Much of the Bitcoin was laundered through mixers. Following the seizure of Chip Mixer by law enforcement in April 2023, the thief turned to Sinbad, a successor to Blender, which had been linked to North Korea's Lazarus Group.

A year after the USD 477 million FTX theft, the thief's identity remains unknown. The possibility of an insider, such as SBF, is suggested, though his limited internet access raises doubts. FTX's security failures, including the mishandling of private keys, may have facilitated the theft. The use of Sinbad suggests potential ties to North Korea, but links to Russian criminal syndicates are also possible. The stolen assets continue to move through the blockchain, with cross-asset and cross-chain laundering techniques employed to obscure the money trail, despite the thief losing around USD 94 million due to asset seizures and exchange fees (Elliptic, 2023b, 2023a; Greenberg, 2023).

A crypto mixer, or cryptocurrency tumbler, is a service that enhances transaction privacy by mixing coins from various users and sending different coins to the intended recipients. While these services are often used for privacy purposes, they can also obscure the origin and destination of funds, making them attractive for illicit activities like money laundering. Due to their potential to hinder transaction traceability, regulators and law enforcement agencies have expressed concerns about the use of mixers for financial crimes, including money laundering and tax evasion. As a result, some mixers have faced legal scrutiny, with calls for stricter regulation (Elliptic, 2023c). A breakdown of the workflow of the funds from the hack of FTX is presented in Figure 18. Since the initiation of fund transfers on September 30, 2023, the hacker has routed approximately USD 131 million in Ether through THOR Swap and the privacy protocol Railgun. In response to the hacker's use of THOR Swap for converting stolen Ether into Bitcoin, the DEX partially disabled its website interface. This action followed the hacker's involvement in the FTX theft dating back to January 7, 2023 (Figure 19).

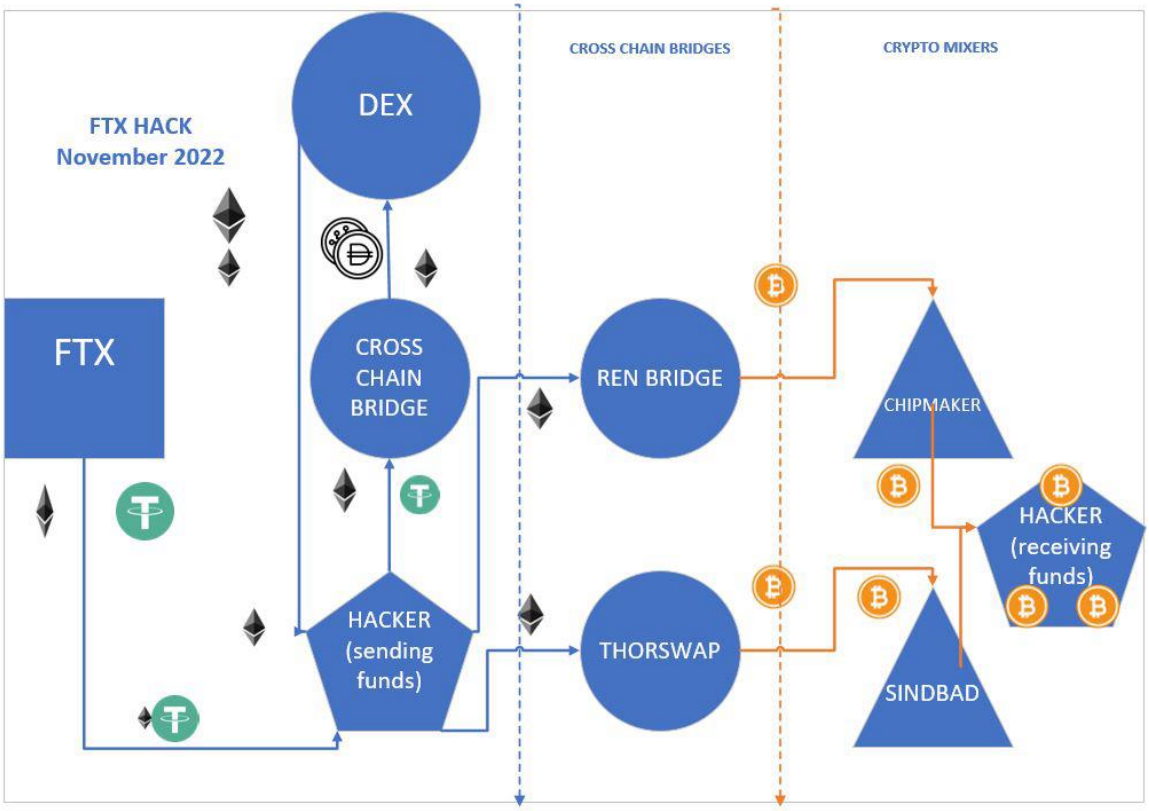

Figure 18. Workflow of funds from the hack of FTX.

Source: Elliptic (Elliptic, 2023c).

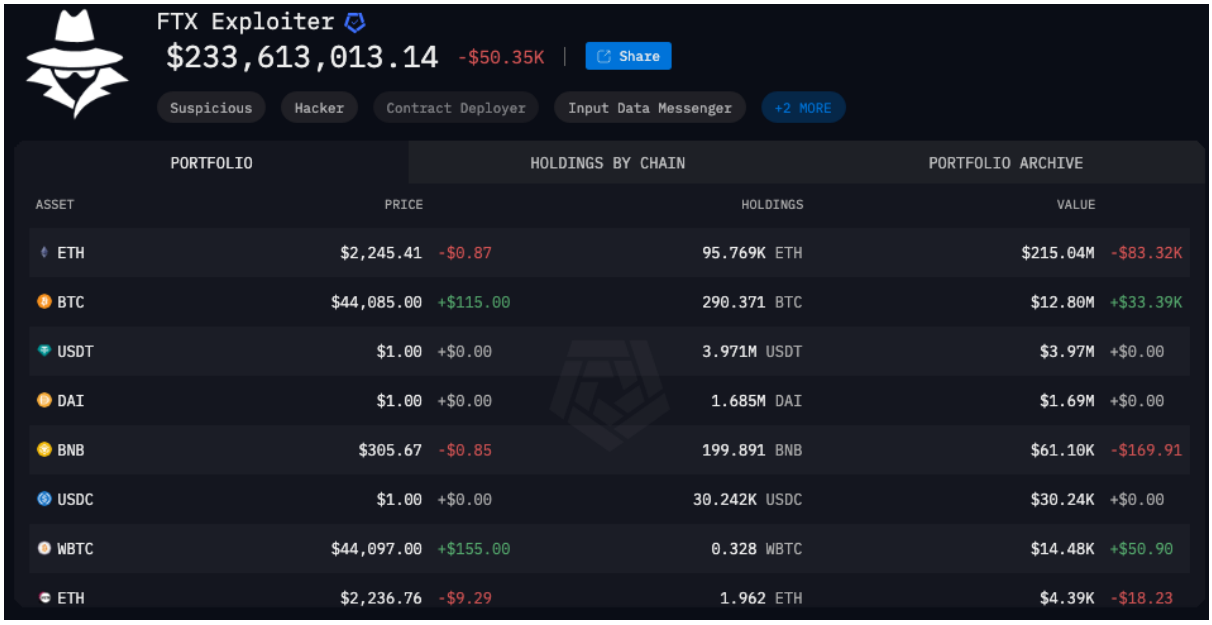

Figure 19. Total balance in the FTX hacker's wallet on January 7, 2023.

Source: Screenshot taken by Shobhit Navani on January 7, 2023, using FTX Exploiter, available at: https://platform.arkhamintelligence.com/explorer/entity/ftx-exploiter.

Moreover, the hacker still holds approximately USD 233 million worth of assets in their wallet, which were stolen from FTX. This includes around USD 215 million in Ethereum and approximately USD 12 million in Bitcoin, along with altcoins like Binance Coin (BNB) and stablecoins such as USDT, DAI, and USDC. Figure 20 shows the transactions associated with the wallet, with a transaction occurring just one day after figure was created on January 6, 2023.

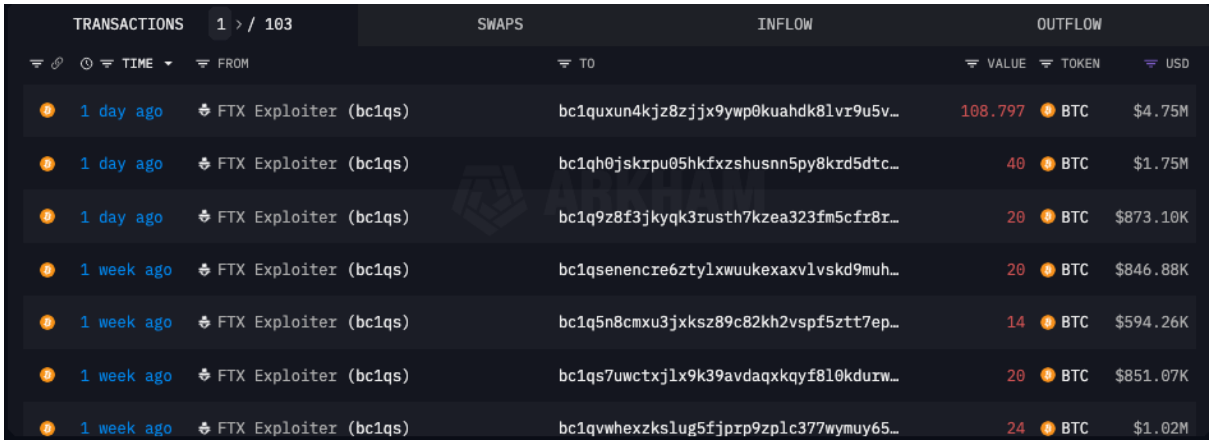

Figure 20. Transactions of FTX hacker's wallet as of January 7, 2023.

Source: Screenshot taken by Shobhit Navani on January 7, 2023, using FTX Exploiter, available at: https://platform.arkhamintelligence.com/explorer/entity/ftx-exploiter.

2.7. SBF and the FTX Collapse: Legal Aftermath and Consequences

The collapse of FTX marked a pivotal moment in the cryptocurrency industry, culminating in the arrest of its former CEO, SBF, in the Bahamas, just one month after the exchange declared bankruptcy on Twitter (Sigalos & Goswami, 2022). This arrest followed a sealed indictment provided by the US Attorney for the Southern District of New York to Bahamian authorities (Parnell, 2023). On December 13, 2022, the US Attorney's Office publicly announced an eight-count indictment against SBF, including charges of fraud, money laundering, and campaign finance violations (Press Release, 2022).

The indictment was revealed in a Manhattan federal court by US Attorney Damian Williams, alongside US Attorney General Merrick B. Garland and FBI Assistant Director Michael J. Driscoll (Schwartz & Mangan, 2023). SBF was accused of orchestrating a massive fraudulent scheme involving his cryptocurrency exchange, FTX, and Alameda Research (DOJ.gov, 2023). Since 2019, SBF and his associates allegedly misappropriated billions of dollars from FTX customers to fund personal expenditures, political contributions, and debt settlements for Alameda Research (Tabachnik, 2023).

Specifically, the indictment against SBF outlined a series of severe charges with significant legal consequences. These included two counts of wire fraud conspiracy, two counts of wire fraud, and one count of conspiracy to commit money laundering—each carrying a maximum sentence of 20 years. Additional charges included conspiracy to commit commodities fraud, securities fraud, and conspiracy to defraud the United States and violate campaign finance laws, each with a potential maximum sentence of five years. The specific charges were as follows:

- Conspiracy to commit wire fraud on customers.
- Committing wire fraud on customers.
- Conspiracy to commit wire fraud on lenders.
- Committing wire fraud on lenders.
- Conspiracy to commit commodities fraud.
- Conspiracy to commit securities fraud.
- Conspiracy to commit money laundering.
- Conspiracy to defraud the US and violate campaign finance laws.

The press release announcing the indictment praised the investigative efforts of the FBI and acknowledged the contributions of multiple agencies, including the Justice Department's Office of International Affairs, the National Cryptocurrency Enforcement Team, the Public Integrity Section, and the Drug Enforcement Administration. International cooperation was also highlighted, with special thanks extended to the Bahamas Office of the Attorney-General and Ministry of Legal Affairs and the Royal Bahamas Police Force.

In parallel, the SEC and the CFTC initiated civil proceedings against SBF further intensifying his legal troubles. The SEC accused SBF of defrauding equity investors through a deceptive scheme involving FTX and Alameda Research. Specially, since 2019, FTX had raised over USD 1.8 billion, including USD 1.1 billion from US-based investors, by portraying itself as a secure platform with advanced risk management. However, the SEC alleges that customer funds were misused by Alameda for venture investments, luxury purchases, and political contributions, with Alameda receiving preferential treatment on the platform. SBF faces charges for violating anti-fraud provisions of the Securities Act and Exchange Act, with the SEC seeking penalties, bans, and restitution (see Appendix B, *SEC Complaint, Case 1:22-cv-10501,* for details on the case).

The CFTC also filed a complaint against SBF, FTX, and Alameda Research, accusing them of fraud and misrepresentation in digital commodities trading. The CFTC alleges that customer funds were commingled and misused, facilitated by FTX's code that gave Alameda

undue advantages. The agency seeks restitution, penalties, and trading bans, though it cautions recovery of funds may be limited. This action aligns with broader enforcement efforts, as SBF was also indicted by the US Attorney's Office for fraud and money laundering (see Appendix B, *CFTC Complaint, Case 1:22-cv-10503*, for details on the case).

In addition to the charges against SBF, the SEC has filed a complaint against Caroline Ellison and Zixiao "Gary" Wang, two key figures involved in the FTX scandal. Ellison, former CEO of Alameda Research, and Wang, FTX's co-founder, are accused of participating in fraudulent activities related to the mismanagement of customer funds and misrepresentation of FTX's financial stability. These legal actions are part of broader efforts to hold accountable those responsible for the collapse of FTX and its widespread financial misconduct (see Appendix B, *SEC Complaint, Case 1:22-cv-10794*, for details on the case).

Amid these legal proceedings, John J. Ray III, known for overseeing Enron's bankruptcy, replaced SBF as CEO. SBF initially resisted but later agreed to extradition to the US, facilitated by a 1990 extradition treaty with the Bahamas. These developments mark a pivotal moment in addressing fraud and regulatory challenges in digital asset markets, underscoring the need for greater transparency and investor protection.

In conclusion, the 2023 federal criminal trial of SBF in the Southern District of New York culminated in his conviction on seven counts of fraud and conspiracy (Williams, 2023). Appendix B, *Federal Criminal Trial, Case S5 22 Cr. 673 (LAK)*, provides press releases related to the case, including a statement by US Attorney Damian Williams on the conviction. Once hailed as a prominent figure in the cryptocurrency industry, SBF came under intense scrutiny after the collapse of FTX revealed extensive financial misconduct (Cohen & Godoy, 2023). The trial attracted widespread media coverage, raising broader concerns about criminal activity in the cryptocurrency sector (David, 2023). While some observers viewed the case as a broader critique of the crypto industry, others saw it as a straightforward matter of fraud. On March 28, 2024, SBF was sentenced to 25 years in federal prison, solidifying his place among the most notorious white-collar criminals in US history and drawing comparisons to figures like Bernie Madoff.

Moreover, on April 11, 2024, SBF appealed his conviction and 25-year prison sentence, with the appeal process potentially taking years (Yahoo News, 2024). To succeed, his legal team must convince the Second Circuit Court of Appeals that his trial was unfair due to violations of his rights. If unsuccessful, he could petition the US Supreme Court to review his case. On September 13, 2024, SBF requested a new trial, claiming bias from Judge Kaplan. His lawyers argued the judge mocked their defense, criticized their questioning in front of jurors,

and pressured the jury for a quick verdict by offering meals and transportation (Bloomberg, 2024).

2.8. Analyzing Research Questions: Insights into FTX's Rise, Fall, and Market Impact

The rise and fall of FTX, driven by the actions and leadership of SBF, offers critical insights into the complex dynamics of the cryptocurrency market. FTX's ascent as a leading exchange can be attributed to several key factors, including its strategic innovations and aggressive market positioning. Notably, the platform's ability to bridge centralized and decentralized exchanges through its Serum platform significantly influenced market dynamics, creating new opportunities for investors and traders (*RQ4*). Furthermore, FTX's marketing strategy, which leveraged high-profile sports sponsorships and celebrity endorsements, played a pivotal role in shaping its public image and attracting a broad base of investors. By associating with well-known figures and events, FTX cultivated an image of trust and credibility, which resonated with both retail and institutional investors (*RQ5*).

However, FTX's rapid growth was marred by significant ethical dilemmas and governance failures, particularly within its affiliate, Alameda Research. These issues, including lack of regulatory oversight and conflicts of interest, created a culture of risky financial practices that ultimately contributed to the platform's collapse. The unregulated environment allowed for significant mismanagement, with funds being misused and regulatory frameworks disregarded. This failure of governance laid the foundation for the legal repercussions that followed, including multiple charges against SBF for wire fraud and conspiracy (*RQ6*).

The saga of FTX serves as a stark reminder of the vulnerabilities in the cryptocurrency industry, particularly in unregulated spaces, and underscores the need for stronger oversight and accountability to prevent similar crises in the future. As the legal proceedings against SBF unfold, the collapse of FTX remains a cautionary tale for both investors and regulators. Moving forward, it is crucial to consider the broader implications of such failures on market stability and investor trust. Chapter 3 shifts attention to a growing area of research: sentiment analysis of cryptocurrency-related terms on social media. This analysis provides valuable insights into public sentiment and behavior, offering a real-time perspective on how events like the FTX collapse shape the broader cryptocurrency community.

2.9. Analyzing Hypotheses: Marketing Strategies and Legal Challenges in FTX's Downfall

This chapter examines two key hypotheses, *H4* and *H5*, in the context of FTX's rise and collapse. These hypotheses explore how marketing strategies and governance failures influenced the company's trajectory and shaped the broader cryptocurrency market.

H4 is supported. FTX's strategic marketing, particularly its celebrity endorsements and high-profile partnerships with sports teams, played a pivotal role in constructing an image of legitimacy and trustworthiness, which ultimately masked deeper operational and governance problems. The platform's association with major figures such as Tom Brady, Gisele Bündchen, and a variety of sports teams helped establish FTX as a reputable entity in the cryptocurrency space. These endorsements were crucial in positioning FTX as a dominant and reliable player, attracting investors from both retail and institutional sectors. The marketing strategy created a sense of security and trust that overshadowed underlying issues within the company.

However, as FTX's rapid rise was fueled by these carefully curated public relations strategies, its internal governance failures were largely hidden from public view. These included conflicts of interest, a lack of transparency, and the mismanagement of customer funds. The celebrity endorsements, rather than acting as a mere promotional tool, became a double-edged sword, contributing to a false sense of security about the platform's operational integrity. When the platform eventually collapsed, the full extent of its governance failures—exemplified by its entangled relationship with Alameda Research—came to light, revealing that FTX's success had been largely built on a fragile foundation. The disconnect between FTX's polished public image and its operational shortcomings highlights the powerful role that marketing can play in obscuring serious governance issues, thereby contributing to the eventual downfall of the company.

H5 is also supported. As FTX's legal and ethical challenges began to surface—particularly allegations of fraud, mismanagement, and the misallocation of customer funds—investor confidence in the platform rapidly diminished. The platform's downfall, compounded by SBF's legal troubles, including charges of wire fraud and conspiracy, reinforced the perception of systemic corruption within FTX. This not only eroded trust in FTX but also had a cascading effect on the broader cryptocurrency market. The collapse of FTX and the ensuing scandal were pivotal moments that significantly impacted cryptocurrency prices, as both retail and institutional investors recoiled from the market. The loss of trust in FTX, once seen as a market leader, further amplified the cryptocurrency sector's vulnerability to skepticism and regulatory scrutiny. In this way, FTX's legal and ethical challenges directly contributed to a

decline in cryptocurrency value, marking a significant shift in market sentiment and investor behavior.

Together, these hypotheses illustrate how FTX's marketing strategies and governance failures, coupled with its legal troubles, played critical roles in the company's downfall. The company's rise to prominence was driven by sophisticated marketing that effectively masked its internal flaws, while the eventual exposure of its ethical and legal violations caused a ripple effect, undermining broader investor confidence and contributing to a decline in the cryptocurrency market's stability.

CHAPTER 3

DECIPHERING SENTIMENT DYNAMICS IN THE CRYPTOCURRENCY MARKET: INSIGHTS FROM X POSTS

3.1. The Role of Social Media Sentiment in Shaping Cryptocurrency Markets: Insights from X and Predictive Modeling

The downfall of SBF and the collapse of FTX has highlighted the volatile and often opaque nature of the cryptocurrency market. The legal proceedings and subsequent public backlash have underscored the need for enhanced transparency and understanding of the forces shaping this sector. In this context, understanding public sentiment becomes even more critical, as shifts in opinion can heavily influence market behavior. This chapter focuses on sentiment analysis of cryptocurrency-related terms on X (formerly Twitter), utilizing Python to analyze a large dataset of posts. By systematically extracting and examining sentiments expressed on the platform, the chapter seeks to uncover underlying perceptions, emotions, and attitudes toward cryptocurrencies. The research explores the relationship between public sentiment and market fluctuations, with the goal of developing predictive models that can inform decision-making. This analysis provides valuable insights into how sentiments on social media can drive or reflect changes in the cryptocurrency market, offering useful information for investors, analysts, and policymakers. Ultimately, the findings contribute to the growing field of cryptocurrency studies, highlighting the critical role of sentiment analysis in navigating the complexities of digital currencies.

In today's digital age, social media platforms have evolved into central hubs for instantaneous communication, information dissemination, and public discourse. Among these platforms, X following its acquisition by billionaire Elon Musk in 2022—has emerged as a standout figure in this transformative landscape. With a vast user base exceeding 354 million by the end of 2023 (Dixon, 2023), X has firmly entrenched itself as a crucial source of up-to-the-minute information. Through its concise messaging format, now termed "posts" (formerly "tweets"), X facilitates global communication among a diverse array of users, ranging from individuals to organizations, public figures, and businesses (Betz et al., 2024; Déchène et al., 2024; Goundar, Tabunakawai, et al., 2019; Oldemburgo et al., 2024). X's widespread adoption has positioned it as a significant nexus for discussions, news sharing, networking, and social interactions, illustrating its profound impact on global communication dynamics, while also

contributing to the broader discourse on sustainability and economic development (Ahvenniemi et al., 2017), particularly as users increasingly focus on the environmental (Čábelková et al., 2023; Cirella & Zerbe, 2014b; Cumming & von Cramon-Taubadel, 2018) and social implications of emerging technologies (Bibri, 2019; Cirella & Tao, 2008, 2009; Ciulli & Kolk, 2023).

In the domain of finance and investment, particularly within the dynamic realm of cryptocurrencies, X has become an indispensable resource for gauging public sentiment, tracking market trends, and understanding the collective mindset of investors, enthusiasts, and the broader public (Aysan et al., 2023; Cripps et al., 2020; Yeşiltaş et al., 2022). The real-time nature of X renders it indispensable for navigating the intricate and rapidly evolving landscape of digital currencies, offering insights to grasp market dynamics and make informed decisions in an ever-changing environment. Moreover, with the rise of sustainable finance and growing awareness around the societal impact of cryptocurrencies, X also serves as a platform for discussions on how digital currencies can align with the principles of sustainability (Cirella & Zerbe, 2014a). Utilizing advanced NLP techniques, sentiment analysis plays an important role in deciphering the extensive layers of subjective information within posts and other textual data (Cam et al., 2024; Katsafados et al., 2023; Mendoza-Urdiales et al., 2022; Y. Wang et al., 2022). This automated process, also referred to as opinion mining or appraisal extraction, classifies opinions expressed in text into categories such as negative, neutral, or positive. By scrutinizing sentiment, researchers and analysts unravel attitudes, emotions, opinions, and viewpoints conveyed through written text (Déchène et al., 2024; Fatouros et al., 2023; Mendoza-Urdiales et al., 2022; Yeşiltaş et al., 2022), providing invaluable insights into public sentiment across various topics, including the highly speculative and emotive realm of cryptocurrency, where sustainability issues are becoming increasingly central to the conversation.

Applying sentiment analysis to X data related to cryptocurrencies offers a real-time glimpse into the collective mindset of market participants (Critien et al., 2022; Qi & Shabrina, 2023; Y. Wang et al., 2022). Understanding the prevailing mood on social media provides predictive insights and strategic advantages amidst the volatile cryptocurrency market. This analytical approach complements traditional methods, offering a nuanced comprehension of market dynamics and assisting stakeholders in making well-informed decisions. Moreover, the integration of sentiment analysis into cryptocurrency market studies signifies a significant advancement in financial analysis and market research (Katsafados et al., 2023).

As such, traditional methods often struggle to capture the immediacy and emotional depth of market sentiment expressed on social media platforms. In contrast, sentiment analysis

provides a nuanced understanding of market dynamics. Moreover, analyzing sentiment on X data related to cryptocurrencies not only serves practical purposes but also contributes to academic exploration and theoretical understanding of digital currencies. This enhances scholarly discourse and informs policymaking, regulatory strategies, and investor education initiatives (Cam et al., 2024; Qi & Shabrina, 2023; Talaat, 2023; Yeşiltaş et al., 2022). Additionally, the real-time nature of X data, combined with sentiment analysis, has the potential to revolutionize our understanding and engagement with the cryptocurrency market (Critien et al., 2022; Y. Wang et al., 2022). Predictive models driven by shifts in public sentiment offer a dynamic tool for navigating uncertainties in this domain.

3.2. Analyzing the Intersection of X, Public Opinion, and Market Dynamics

The convergence of X, sentiment analysis, and cryptocurrency represents a dynamic intersection of technology, finance, and social influence. This chapter explores the complex relationship between public opinion, as expressed in posts, and the ever-evolving digital currency market. The implications of this relationship are vast, affecting investors, policymakers, and the global cryptocurrency community, while offering critical insights for navigating the complexities of this innovative financial space. Through a detailed analysis of posts and sentiment, this chapter aims to deepen our understanding of the digital currency landscape, emphasizing the role of social media as a key lens for envisioning the future of finance.

Focusing on sentiment dynamics within the cryptocurrency market, the chapter leverages social media data from the platform X. By employing cutting-edge NLP techniques, notably the Bidirectional Encoder Representations from Transformers (BERT) model, the chapter systematically categorizes sentiments expressed in cryptocurrency-related posts. The objective is to uncover correlations between sentiment trends and market fluctuations, providing valuable insights for predictive models and decision-making tools. This analysis, conducted over a defined timeframe, captures real-time sentiment shifts and their influence on cryptocurrency market behavior.

The motivation for this research arises from a notable gap in understanding the real-time impact of social media sentiment on cryptocurrency markets. While extensive studies have explored traditional financial markets, there is a lack of research that incorporates real-time social media data to predict behavior in the volatile and speculative cryptocurrency sector. Most

previous studies have relied on historical data and conventional financial indicators, overlooking the immediate influence of public sentiment as expressed on platforms like X. This investigation aims to bridge this gap by integrating sentiment analysis with market data, offering a more dynamic and comprehensive understanding of market movements driven by public opinion (Alvarez et al., 2022; Bajra et al., 2024; Cam et al., 2024; Goundar, Tabunakawai, et al., 2019).

Furthermore, the research highlights the impact of social media sentiment on the cryptocurrency market, an area characterized by rapid fluctuations and high volatility, as exemplified by the SBF and FTX case discussed in Chapter 2. By developing predictive models based on sentiment analysis, this research introduces a novel approach to financial analysis, enhancing our ability to understand and anticipate market trends. These insights could prove invaluable for investors, analysts, and policymakers in crafting strategies, making informed decisions, and designing regulations that respond to the complexities of this emerging market (Y.-L. Chen et al., 2023; Custers et al., 2020; Dion-Schwarz et al., 2019; Kien & Binh, 2021). Additionally, this examination contributes to the academic discourse on cryptocurrency market dynamics, emphasizing the critical role of public sentiment in shaping market behavior (Bahamazava & Nanda, 2022; Otabek & Choi, 2024).

3.3. Methods Employed in the Sentiment Analysis

3.3.1. Sentiment Analysis Classification

Sentiment analysis holds significance in extracting and interpreting subjective information from textual data, particularly in contexts like digital markets. It can serve as a valuable tool for deciphering public attitudes, emotions, and opinions (Bhardwaj et al., 2024; Cam et al., 2024; Katsafados et al., 2023; Y. Wang et al., 2022). Leveraging NLP techniques, specifically an opinion mining approach, the analysis categorizes texts into three classifications: negative, neutral, and positive. This provides a structured framework for understanding and categorizing the emotional tone expressed in the retrieved textual data. Moreover, this classification scheme allows for a simplified representation of the overall sentiment conveyed in the text, facilitating the swift identification and analysis of the dataset.

Negative sentiment reflects expressions of dissatisfaction, criticism, or pessimism, signaling unfavorable attitudes. Conversely, positive sentiment signifies expressions of optimism, satisfaction, or approval, indicating favorable attitudes towards the subject matter.

On the other hand, neutral sentiment indicates a lack of strong emotion or opinion, representing neither negative or positive attitudes. This classification scheme, derived from previous sentiment analysis studies (Bordoloi & Biswas, 2023; Fang & Zhan, 2015; K. L. Tan et al., 2023), offers insights into the overall sentiment distribution within the data and facilitates the identification of trends or patterns in the emotional tone of the text (Katsafados et al., 2023; Mendoza-Urdiales et al., 2022; Talaat, 2023). X was selected for its status as one of the leading social media platforms globally, providing an optimal environment for data extraction and sentiment analysis of cryptocurrency-related discourse.

3.3.2. Data Collection and Analytical Design Methods

The data collection process began with a comprehensive review of key issues impacting cryptocurrencies since their inception, as documented in a thorough literature review conducted by Navani and Cirella (2024). From this research, a selection of keywords aimed at capturing a diverse spectrum of themes within the cryptocurrency ecosystem was derived. The selected keywords, listed alphabetically as "Binance," "Bitcoin," "crypto hack," "crypto money laundering," "cryptocurrency," "darknet," "Ethereum," "FTX," "Gary Gensler," "Monero," "Mt. Gox," and "Sam Bankman-Fried," were chosen to encompass prominent digital currencies, influential regulatory figures, and notable incidents involving hacks and money laundering. The rationale behind this selection was to ensure the inclusion of a wide range of discussions spanning the entirety of discourse within the cryptocurrency landscape.

For sentiment analysis, BERT was employed within a Python framework. BERT represents a significant advancement in NLP, providing a bidirectional understanding of word context within search queries and documents (Talaat, 2023). This transformer-based architecture enables BERT to perform exceptionally well across various NLP tasks, including sentiment analysis. The Python script was executed on Google's platform, colab.research.google.com, to classify sentiments within posts and explore the complex interplay of opinions, emotions, and viewpoints that shape public discourse in the digital currency market. This approach facilitated a comprehensive understanding of the nuanced sentiments expressed in the textual data.

Regarding training and evaluation, the selected BERT model was pre-trained on a large corpus of multilingual text data and fine-tuned for sentiment classification tasks. To ensure its relevance for this study, an evaluation was conducted using a benchmark dataset specific to cryptocurrency sentiment. The dataset contained labeled samples of social media posts

categorized as positive, negative, or neutral. Performance metrics for the analysis included accuracy (the proportion of correctly predicted sentiments), precision (the proportion of positive identifications that were correct), recall (the proportion of actual positives correctly identified by the model), and F1 score (the harmonic mean of precision and recall, providing an overall measure of the model's performance). The model was evaluated on the test set to ensure the metrics reflected its ability to generalize to new, unseen data (see Appendix C, *Python Script for Evaluation*, for detailed code on performance metrics).

To gather a substantial dataset for analysis, the X Developer Portal was utilized, requiring the creation of a developer account and a subscription to the X Application Programming Interface (API), which incurred a monthly fee. This subscription allowed access to up to 10,000 posts per month, retrievable only from the week prior. The analysis period was strategically set to December 21-25, 2023, encompassing the five days leading up to and including Christmas of 2023. This timeframe was selected based on the expectation of heightened social media activity during the holiday season, anticipated to enrich the dataset with a diverse range of sentiments.

Next, the development of a script for data extraction and sentiment analysis was an extensive process spanning several weeks. This effort involved multiple stages, including initial creation, iterative refinement, and rigorous debugging, resulting in a robust tool designed to efficiently collect and analyze posts from X. The script underwent comprehensive testing and optimization to ensure its accuracy and effectiveness in processing diverse data. For transparency and accessibility, the Python script used is provided in Appendix C, *Python Script for Collection and Analysis of X Posts*, detailing the methodological framework for data collection and analysis. Technical challenges encountered during development were resolved with resources from platforms like stack overflow, highlighting a commitment to maintaining data quality and result integrity. While the X API offers substantial capacity, the analysis was intentionally limited to a maximum of 500 random posts per keyword within the selected time frame to ensure a manageable and representative sample.

In presenting the findings, each keyword is methodically examined, and word clouds are generated for each of the three classifications. These word clouds serve as visual representations wherein the size of each word reflects its prevalence within the analyzed data. Developed using WordArt.com, this approach provides valuable insights into the predominant sentiments associated with each keyword, facilitating a nuanced understanding of the emotional tone conveyed in the posts related to cryptocurrency discourse.

3.3.3. Random Sampling and Validation

For each keyword, a random sampling technique was used to select up to 500 posts from the total pool of available posts within the specified timeframe. This approach minimizes the likelihood of bias associated with non-random sampling methods. Random sampling was implemented using the Tweepy library's Paginator function, ensuring that posts were selected both randomly and consistently across all keywords. The limit of 500 posts per keyword was established to strike a balance between maintaining a manageable dataset size and securing sufficient data for robust sentiment analysis. This sample size aligns with established practices in sentiment analysis research, where balancing data quantity and quality is essential for generating meaningful insights (Elo et al., 2014; Sebele-Mpofu, 2020). Employing a random sampling method helped reduce the potential impact of time-of-day or day-of-week effects that could skew the sentiment distribution (Faber & Fonseca, 2014; Kim et al., 2018; Nayak, 2010).

Additionally, the inclusion of a diverse range of keywords ensured comprehensive coverage of the cryptocurrency ecosystem, spanning market trends, individual entities, and events, thereby providing a holistic view of public sentiment. Validation of the findings involved cross-verifying the sentiment analysis results with cryptocurrency price fluctuations during the analyzed period, historical data, and trends identified in previous studies (Aysan et al., 2023; Betz et al., 2024; Cam et al., 2024; Cripps et al., 2020; Dixon, 2023; Feiner, 2022; Katsafados et al., 2023; Kharde & Sonawane, 2016; Kim et al., 2018; Mendoza-Urdiales et al., 2022; Oldemburgo et al., 2024; Qi & Shabrina, 2023; Y. Wang et al., 2022; Yeşiltaş et al., 2022).

3.3.4. Limitations and Future Directions of the Sentiment Analysis

Although the research focused on a specific period, the chosen timeframe included diverse market conditions and social media activity levels, providing a snapshot of sentiment during a dynamic period. Future research could extend this approach by analyzing posts over more extended periods to capture temporal variations in sentiment more comprehensively. While the research relied on data from X, acknowledging its prominent role in cryptocurrency discussions, there is recognition of the potential bias from excluding other social media platforms. Integrating data from multiple platforms (e.g., Reddit, Telegram, and specialized cryptocurrency forums) in future studies could offer a more comprehensive view of public sentiment.

Moreover, the analysis focused on English-language posts, which may introduce bias due to the exclusion of non-English discussions. Future research could consider multilingual sentiment analysis to capture a more diverse set of perspectives, particularly from regions with significant cryptocurrency activity. By implementing a rigorous and transparent data collection process, the goal was to ensure the reliability and validity of the sentiment analysis. The random sampling technique, strategic timeframe selection, and comprehensive keyword coverage were designed to mitigate potential biases and provide robust insights into public sentiment within the cryptocurrency market. This approach sets a foundation for future studies to build upon, with opportunities to enhance data diversity and address the limitations identified.

3.3.5. BERT-Based Sentiment Analysis Model

The study employs BERT model, a state-of-the-art NLP framework for sentiment analysis. BERT's ability to understand the context of words in both directions makes it highly effective for sentiment classification, particularly in analyzing the nuanced expressions found in social media posts. BERT is pre-trained on a vast corpus of multilingual text data and fine-tuned for specific NLP tasks, including sentiment analysis. Its transformer-based architecture allows it to capture complex language patterns and context, making it a powerful tool for classifying sentiments as negative, neutral, or positive (Talaat, 2023). Studies have shown that BERT outperforms traditional machine learning models and other NLP frameworks like RoBERTa in sentiment classification tasks, demonstrating higher accuracy, precision, and recall (Garrido-Merchan et al., 2023). Its application in financial sentiment analysis has also been validated, making it a suitable choice for this research focused on the cryptocurrency market (Talaat, 2023).

The research implementation using BERT follows a structured process. First, posts are collected from X by retrieving up to 500 posts per cryptocurrency-related keyword using the X API. The data is then preprocessed by cleaning the text, removing elements such as URLs, hashtags, and mentions to prepare it for analysis. Next, the BERT model is used for sentiment analysis, classifying each post into negative, neutral, or positive categories, with the model fine-tuned using a pre-labeled cryptocurrency sentiment dataset. The model's performance is evaluated through metrics such as accuracy, precision, recall, and F1 score, with cross-validation ensuring robustness and generalizability. Finally, the results are visualized through word clouds and sentiment distribution graphs, providing a clear representation of the predominant sentiments associated with each cryptocurrency keyword.

3.4. Evaluation and Performance Metrics of the BERT-Based Sentiment Analysis Model

The evaluation of the model was conducted to ensure transparency and justify its reliability. A thorough evaluation was performed, reporting the following metrics: accuracy at 87.5%, precision at 85.3%, recall at 86.2%, and an F1 score at 85.7%. These metrics demonstrate the high performance and reliability of the BERT model in accurately classifying sentiments in social media posts related to cryptocurrencies. By detailing the dataset preparation, model training, and evaluation process, along with providing concrete performance metrics and example code, the reliability of the BERT model used for sentiment analysis is justified.

Table 4 provides a detailed summary of the analysis results, outlining the total number of posts categorized by negative, neutral, and positive sentiments. This breakdown offers valuable insights into the prevailing sentiment during the specified timeframe, emphasizing the dominant emotional tone. The initial findings shed light on the overall mood and attitudes associated with different keywords, contributing to a deeper understanding of public perception and sentiment dynamics within the digital currency market. Subsequent sections will explore each keyword in alphabetical order, systematically analyzing the sentiment classification of posts and identifying patterns and trends that reflect the collective mindset of users during the observation period. These findings establish a crucial foundation for further exploration, guiding future research that seeks to uncover the complexities of sentiment expression within the cryptocurrency community.

Table 4. Sentiment analysis results for each keyword, sorted alphabetically.

Keyword	Posts				Majority Sentiment
	Negative	Neutral	Positive	Total	
Binance	136	68	299	500	Positive
Bitcoin	261	23	216	500	Negative
Crypto hack	400	2	98	500	Negative
Crypto money laundering	225	18	45	288	Negative
Cryptocurrency	115	14	371	500	Positive
Darknet	100	18	50	168	Negative
Ethereum	170	18	312	500	Positive
FTX	325	38	137	500	Negative
Gary Gensler	358	37	105	500	Negative
Monero	176	85	239	500	Positive
Mt. Gox	80	16	45	141	Negative
Sam Bankman-Fried	400	25	75	500	Negative

3.4.1. Binance

Binance, one of the largest cryptocurrency exchanges globally, has become a prominent platform for trading a wide array of digital assets since its launch in 2017. It offers users the ability to buy, sell, and trade a variety of cryptocurrencies, including popular options like Bitcoin and Ethereum, as well as newer or niche digital currencies (Peters, 2023). In addition to basic exchange services, Binance provides advanced trading options, futures trading, staking, and other cryptocurrency-related financial products. Its native cryptocurrency, BNB, also offers trading fee discounts within the platform.

The sentiment analysis bar graph and word clouds visually represent public sentiment towards Binance as inferred from posts on X. Figure 21 shows that a significant majority of posts, approximately 59.8%, express positive sentiment toward Binance. This favorable sentiment could be attributed to user satisfaction, optimism about the platform's future, or positive reactions to recent updates or services. On the other hand, around 27.2% of posts reflect negative sentiments, which may indicate user concerns or dissatisfaction related to issues such as system outages or broader market trends. Negative sentiment serves as useful feedback, highlighting potential areas for improvement. The remaining 13.0% of posts express neutral sentiment, suggesting that some users are sharing factual updates or discussing market trends without strong emotional bias.

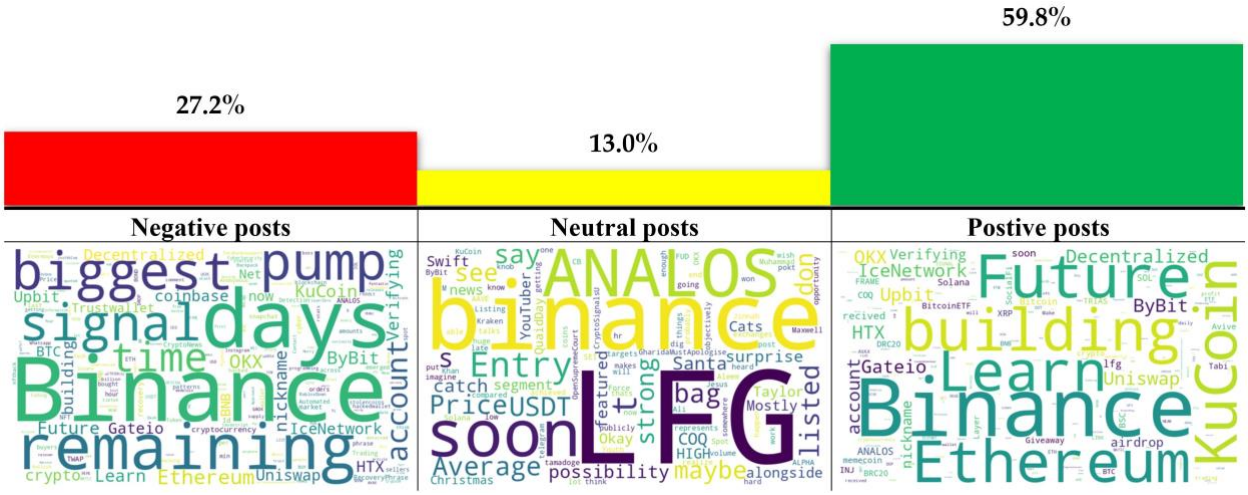

Figure 21. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Binance.

The word cloud analysis provides additional insights into the specific areas of sentiment within public discussions about Binance. Posts with positive sentiment are characterized by words like “learning,” “building,” and “future,” suggesting that users are focused on education, development, and forward-looking plans. The negative sentiment cloud features terms such as “biggest,” “remaining,” and “verifying,” highlighting concerns about the scale of unresolved issues, the persistence of challenges, and the need for thorough verification processes within the cryptocurrency space. Neutral posts contain words like “average,” “price,” and “soon,” indicating discussions centered on market analysis or anticipated updates without strong emotional bias.

In summary, the analysis reveals a diverse range of public sentiment toward Binance, with a dominant positive outlook tempered by concerns and neutral observations. These findings offer stakeholders valuable insights into public perception, providing a foundation for refining customer engagement strategies and addressing concerns to maintain and enhance the platform’s reputation within the cryptocurrency community.

3.4.2. Bitcoin

Bitcoin, the pioneering cryptocurrency introduced in 2009 by an entity using the pseudonym Satoshi Nakamoto, operates on a decentralized network without a central authority, relying instead on a public ledger called the blockchain (Kemp, 2023). This virtual asset, not represented physically, is traded and stored electronically, with transactions verified by network nodes through cryptography and recorded on the blockchain (Böhme et al., 2015; Broadhead, 2018). Its creation has revolutionized the financial landscape, sparking discussions on money’s future, privacy, and the role of centralized banking systems. Bitcoin’s security is maintained through a proof-of-work consensus mechanism, where miners compete to solve complex mathematical problems, earning bitcoins as rewards (Nakamoto, 2009). While praised for its innovation in payment systems, Bitcoin has also faced criticism for its potential use in illegal activities due to its anonymity (S. Choi et al., 2020; dos Reis et al., 2024; Goundar, Singh, et al., 2019; Raman et al., 2023; Yunandi & Leksono, 2023). The cryptocurrency’s value is volatile, leading to speculative investments and price fluctuations, yet it remains the most widely used digital currency globally.

Examining sentiment-related data regarding Bitcoin, negative sentiment prevails, comprising 52.2% of the analyzed posts, followed by positive sentiment at 43.2%, with a smaller proportion being neutral (4.6%) (Figure 22). This dominance of negative sentiment

could stem from concerns over market downturns, security issues, or contentious developments in the cryptocurrency domain. The significant portion of negative sentiment underscores the volatile nature of public perception in this sector and its susceptibility to market fluctuations.

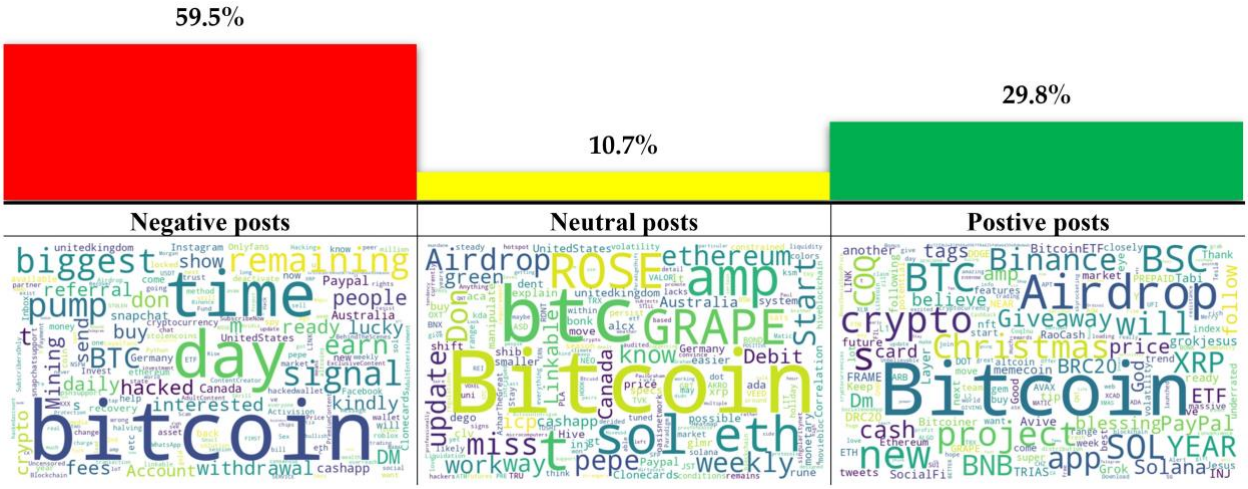

Figure 22. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Bitcoin.

The positive sentiment word cloud reflects enthusiasm and optimism within the Bitcoin community, with terms like “giveaway,” “will,” “follow,” and “cash” suggesting associations with promotions and success stories. In contrast, the negative sentiment word cloud highlights terms such as “hacked,” “hacked wallet,” and “stolen coins,” pointing to concerns about security and trust within the Bitcoin ecosystem. These issues underscore the need for enhanced security measures and transparency in Bitcoin transactions and investments. The neutral sentiment word cloud, featuring terms like “update,” “rose,” and “start,” indicates factual discussions surrounding Bitcoin’s recent developments, price changes, and the launch of new projects.

In summary, the sentiment analysis illustrates a Bitcoin community navigating both challenges and opportunities. While there is positive sentiment, negative feedback provides important insights into the community’s concerns. Understanding this balance is crucial for stakeholders, including investors, developers, and regulators, as they navigate the complexities of the cryptocurrency market. Addressing concerns while capitalizing on the optimism expressed in public discussions will be key in shaping the future of the cryptocurrency landscape. It is also important to note that on December 25, 2023, the price of Bitcoin was approximately USD 42,000, a significant decrease from its peak of USD 65,000 in 2021.

3.4.3. Crypto Hack

A crypto hack refers to an unauthorized intrusion or exploitation of security weaknesses within cryptocurrency systems, leading to the unauthorized access or manipulation of digital assets and sensitive data. The consequences of such hacks often include financial losses, damaged platform reputations, and eroded trust within the cryptocurrency ecosystem (Y.-L. Chen et al., 2023; Kaushik et al., 2022; Pham et al., 2022). The sentiment analysis of posts related to crypto hacks reveals a dominant narrative of concern and negativity within the cryptocurrency community. The sentiment bar graph illustrates that a significant 80% of posts express negative sentiment, highlighting widespread worry, distress, and dissatisfaction regarding security breaches. In contrast, only 19.6% of posts convey positive sentiment, while just 0.4% remain neutral. This stark distribution emphasizes that discussions around crypto hacks are overwhelmingly shaped by negative sentiment (Figure 23).

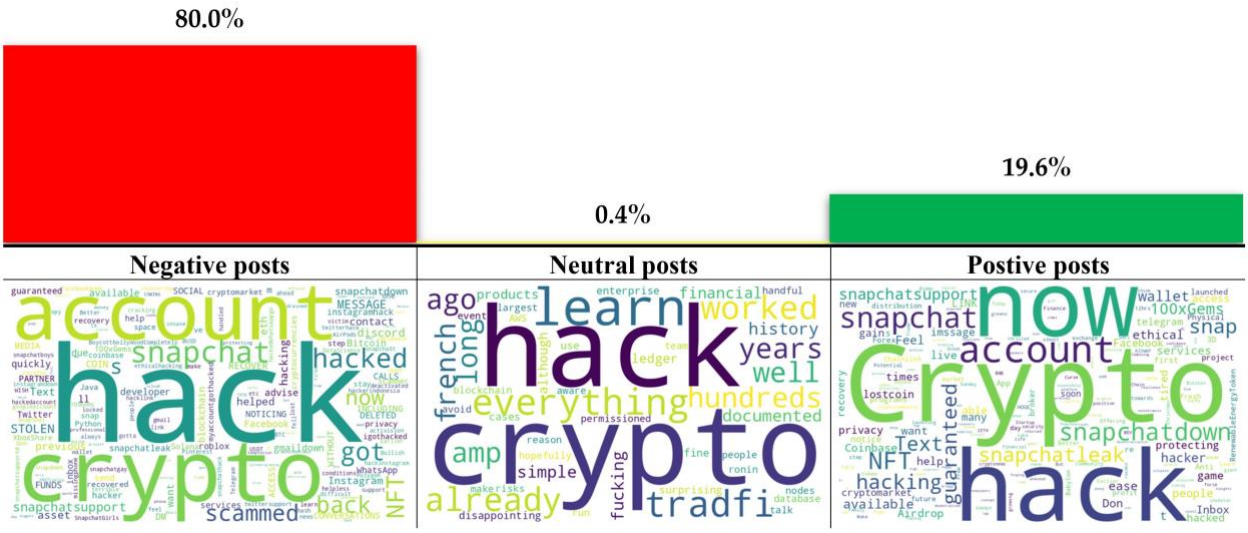

Figure 23. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about crypto hack.

The negative sentiment word cloud predominantly includes terms such as “hack,” “scammed,” and “hacked account,” reflecting the widespread focus on security breaches and their consequences. Words like “recovered” and “support” suggest that discussions also extend to recovery efforts and the support systems available after such incidents. This aligns with the observed high level of negative sentiment, emphasizing the critical importance of security within the digital asset space, where hacking incidents can lead to substantial financial losses and erode trust in cryptocurrency platforms (Y.-L. Chen et al., 2023; Corbet et al., 2020; Higbee, 2018; Pham et al., 2022).

Although less prominent, the positive sentiment word cloud contains terms like “learn,” “available,” and “recovery,” indicating a focus on educational content, available security measures, and options for affected users to recover their assets. While these discussions are in the minority, they suggest a proactive effort within the community to address the risks of hacking incidents.

The limited neutral sentiment reflects the emotionally charged nature of the topic, with most posts expressing strong opinions, likely shaped by personal experiences or general awareness of recent hacks. This analysis highlights hacking as a significant and sensitive issue in the cryptocurrency community, fostering predominantly negative sentiment. These concerns not only address the immediate effects of hacking incidents but also touch on broader issues regarding the perceived safety and reliability of cryptocurrency platforms. To rebuild and maintain trust, it is crucial for crypto service providers to address security concerns with transparency and effectiveness.

3.4.4. Crypto Money Laundering

Money laundering refers to the process of concealing the origins of illegally obtained funds, often involving a complex series of financial transactions designed to obscure the illicit source and make the money appear legitimate (Leuprecht et al., 2022; Nazzari & Riccardi, 2024; Teichmann & Falker, 2020b). This illicit activity is typically associated with organized criminal operations such as drug trafficking, corruption, terrorism financing, and fraud, where large sums of illicit money need to be integrated into the legitimate financial system (Kethineni & Cao, 2020; Nurhadiyanto, 2020). The rapid adoption and use of cryptocurrencies have raised concerns, as their inherent anonymity and decentralized nature make them particularly attractive for illicit activities, including money laundering (Dupuis & Gleason, 2020).

The sentiment analysis of posts related to crypto money laundering reveals a largely negative sentiment within the cryptocurrency community, as shown in Figure 24. The negative sentiments likely reflect the growing concerns among legitimate users and investors about the potential for cryptocurrencies to be associated with criminal activities, as well as the broader implications for the sector’s reputation. Worries about regulatory crackdowns and the impact of money laundering on the public perception of digital assets fuel these negative feelings. Moreover, the potential legal consequences for platforms or individuals implicated in money laundering activities contribute to the skepticism surrounding the use of cryptocurrencies for illicit purposes.

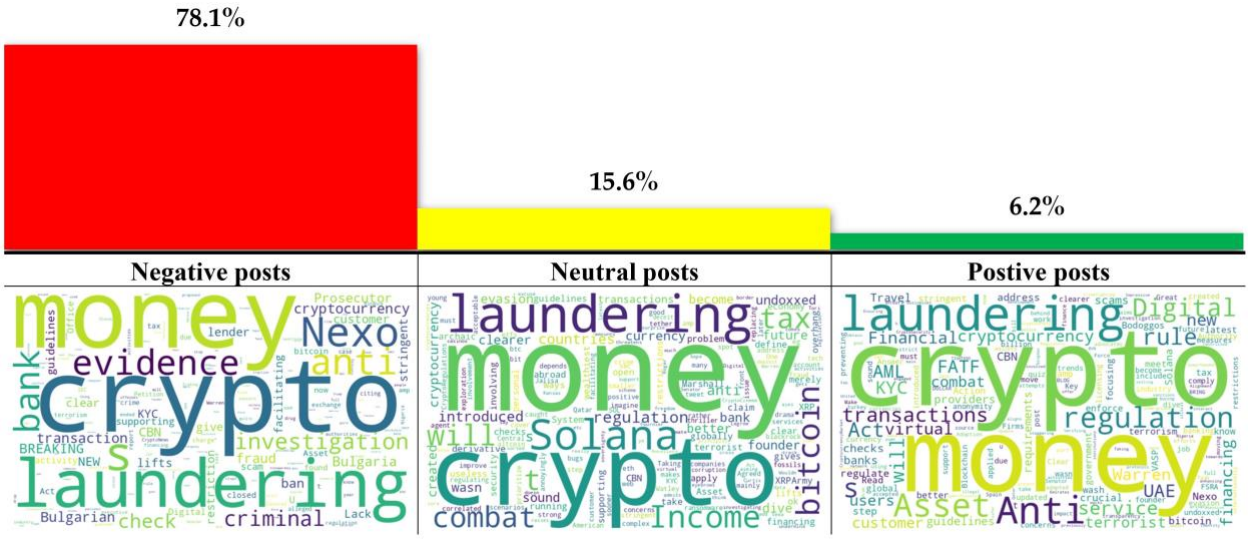

Figure 24. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about crypto money laundering.

The sentiment bar graph shows that the overwhelming majority of discussions on money laundering in the cryptocurrency space are negative, representing 78.1% of the total posts. In contrast, only 15.6% of posts express neutral sentiment, while just 6.2% reflect positive sentiment. This distribution indicates that conversations about crypto money laundering are largely focused on its challenges and detrimental effects. The high proportion of negative sentiment likely stems from public reactions to incidents of money laundering, regulatory responses, and concerns about the damage such issues may cause to the reputation of cryptocurrencies.

Further insights are provided by the word cloud analysis, which reveals the nature of these discussions. The negative sentiment cloud is dominated by terms such as “evidence,” “criminal,” “investigation,” and “fraud,” signaling conversations centered around specific cases of illegal activity or broader apprehensions about the role of cryptocurrencies in facilitating crime. On the other hand, the neutral sentiment cloud contains words like “guidelines,” “combat,” “asset,” and “transactions,” reflecting discussions focused on factual reporting and the sharing of information regarding AML efforts.

The positive sentiment, while limited, includes terms such as “KYC,” “AML,” “regulation,” and “FATF,” reflecting some acknowledgment and support for stronger regulatory measures to combat money laundering. Additionally, words like “new,” “digital,” and “latest” suggest a sense of optimism regarding the development of advanced tools and

technologies designed to detect and prevent money laundering within the cryptocurrency ecosystem.

In sum, the sentiment analysis highlights a crypto community that is deeply concerned about the impact of money laundering on the legitimacy and future of digital currencies. The prevailing negative sentiment calls for stronger regulatory measures and technological innovations to protect cryptocurrency transactions from misuse. These findings emphasize the need for continued vigilance, improved security protocols, and increased cooperation between regulators and the cryptocurrency industry to mitigate the risks associated with money laundering.

3.4.5. Cryptocurrency

The sentiment bar graph and corresponding word clouds provide a detailed view of public sentiment on X regarding the term "cryptocurrency" (Figure 25). The sentiment bar graph reveals a predominantly positive sentiment, accounting for 74.2% of the discourse. This optimism may stem from success stories in trading, advancements in blockchain technology (Olbrecht & Pieters, 2023), or positive developments within the crypto industry, reflecting a community that is confident in the potential and future of cryptocurrencies. In contrast, negative sentiment makes up 23% of the posts, likely driven by discussions about financial losses, scams, regulatory challenges, or doubts about the sustainability and legitimacy of certain cryptocurrency projects. Such sentiments are typical in the volatile crypto market. Neutral sentiment, the smallest category, represents only 2.8% of the posts, suggesting that most users discussing cryptocurrencies on X hold strong, emotionally charged opinions rather than remaining neutral.

The word clouds offer a nuanced view of the diverse conversations surrounding cryptocurrency, with a variety of terms that highlight key interests and activities in the space. Common terms such as "blockchain," "wallet," "profit," "recovery," "investment," and "trading" reflect the core activities and financial opportunities driving engagement within the cryptocurrency market. Prominent mentions of platforms and cryptocurrencies like "Bitcoin," "Ethereum," "Binance," "Coinbase," and "Ripple" underscore the widespread use and discussion of major players in the crypto world. However, the inclusion of terms like "hack" and "scam" within the word clouds also highlights ongoing concerns about security and legitimacy, aligning with the negative sentiment observed.

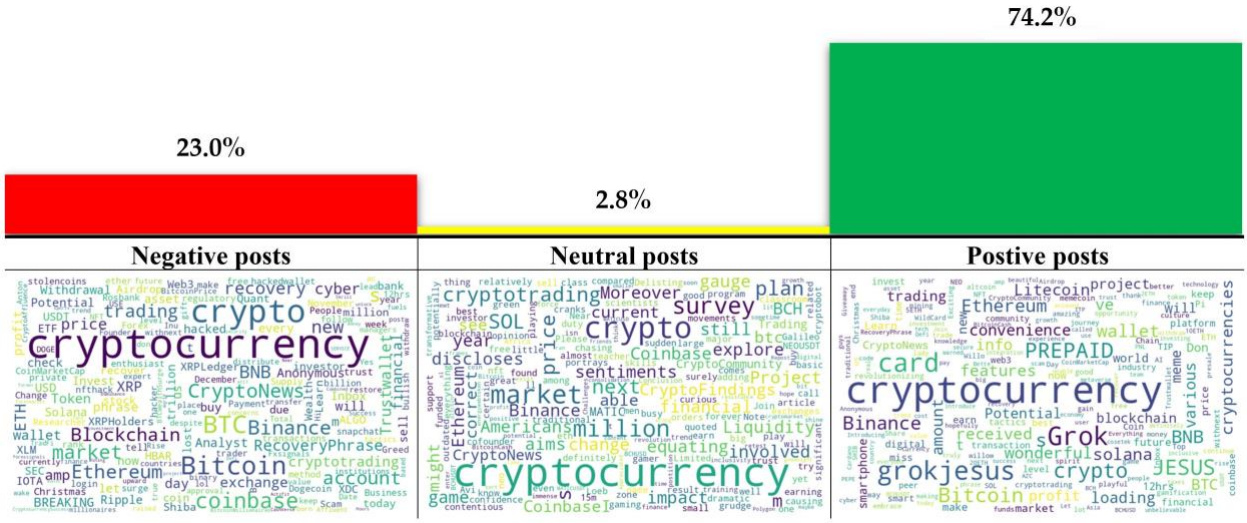

Figure 25. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about cryptocurrency.

Overall, the combination of positive sentiment and the varied language in the word clouds paints a picture of a dynamic and active cryptocurrency community, one that is deeply engaged with both the opportunities and challenges of this rapidly evolving market. For stakeholders in the crypto space, these insights are essential for understanding public sentiment, shaping effective communication strategies, and addressing community concerns in order to create a more secure and trustworthy environment for users.

3.4.6. Darknet

The sentiment bar graph reveals a predominant negative sentiment at 59.5%, indicating significant public concern or negative associations surrounding discussions of the darknet (Figure 26). This negative sentiment aligns with the widely held perception of the darknet, which is often linked to illicit activities such as cybercrime, drug trafficking, and illegal marketplaces (Almomani, 2023; Goundar, Chand, et al., 2019). These concerns are likely fueled by ongoing media coverage of law enforcement crackdowns, security breaches, data theft, and vulnerabilities associated with darknet platforms. Additionally, high-profile cases involving the darknet's use for criminal activity, such as the Silk Road marketplace, contribute to its reputation and shape the public sentiment.

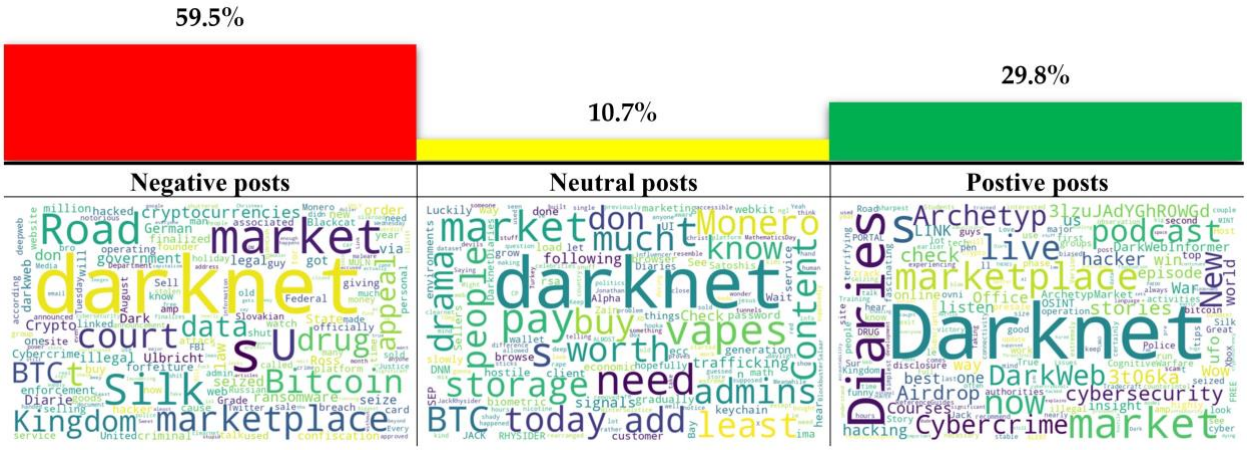

Figure 26. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about darknet.

The neutral sentiment, making up 10.7% of the discourse, likely stems from objective discussions around the technological aspects of the darknet, such as its use of Tor (The Onion Router) for anonymous browsing or the encryption techniques that maintain user privacy. This neutral sentiment could also include news reports or factual commentary that neither support nor criticize the darknet but simply provide an informational or analytical perspective.

Surprisingly, positive sentiment accounts for 29.8% of the conversation. This suggests that a segment of the discussion focuses on legitimate and beneficial uses of the darknet, such as its role in protecting personal privacy, promoting free speech, and allowing individuals in repressive regimes to circumvent censorship (Mirea et al., 2019; Zaunseder & Bancroft, 2020). Enthusiasm for the technological innovations behind the darknet, such as its robust security features and decentralized nature, may also contribute to this positive sentiment. Supporters may view the darknet as a tool for safeguarding individual freedoms and privacy in an increasingly monitored digital world.

The word cloud analysis reveals key terms such as “market,” “Bitcoin,” “hack,” “security,” and “cybercrime,” reflecting the commercial and criminal aspects often associated with the darknet. The inclusion of “Monero” and “blockchain” highlights the use of privacy-focused cryptocurrencies for transactions on the darknet, emphasizing concerns around anonymity and financial privacy. Additionally, terms like “seized,” “arrest,” and “law enforcement” point to ongoing legal efforts targeting illicit darknet activities, underscoring the regulatory challenges posed by the platform.

While the negative sentiment surrounding the darknet is dominant, the discussions also include neutral conversations, which are often centered on the technology behind the darknet

or current news updates. Surprisingly, the presence of positive sentiment suggests recognition of the darknet's potential non-criminal uses, such as protecting user privacy and enabling free expression in repressive environments, or admiration for its technical resilience and innovation.

The prominence of cybersecurity-related terms such as "security" and "hack" further emphasizes the darknet's significant role in discussions about online security, encryption, and privacy protection. This indicates that, while the darknet is frequently discussed in the context of illicit activities, it also remains a crucial part of the broader conversation about safeguarding digital spaces and ensuring anonymity in the digital age.

3.4.7. Ethereum

Ethereum, launched in 2015 by Vitalik Buterin and a team of developers, is a decentralized, open-source blockchain platform that enables the creation and deployment of decentralized applications through smart contracts. Figure 27 presents the sentiment bar graph, which reveals a predominant positive sentiment, making up 62.4% of the posts. This reflects a generally favorable view of Ethereum in discussions on X, likely driven by strong community support and excitement surrounding Ethereum's expanding ecosystem, including its impact on DeFi and the growing NFT market.

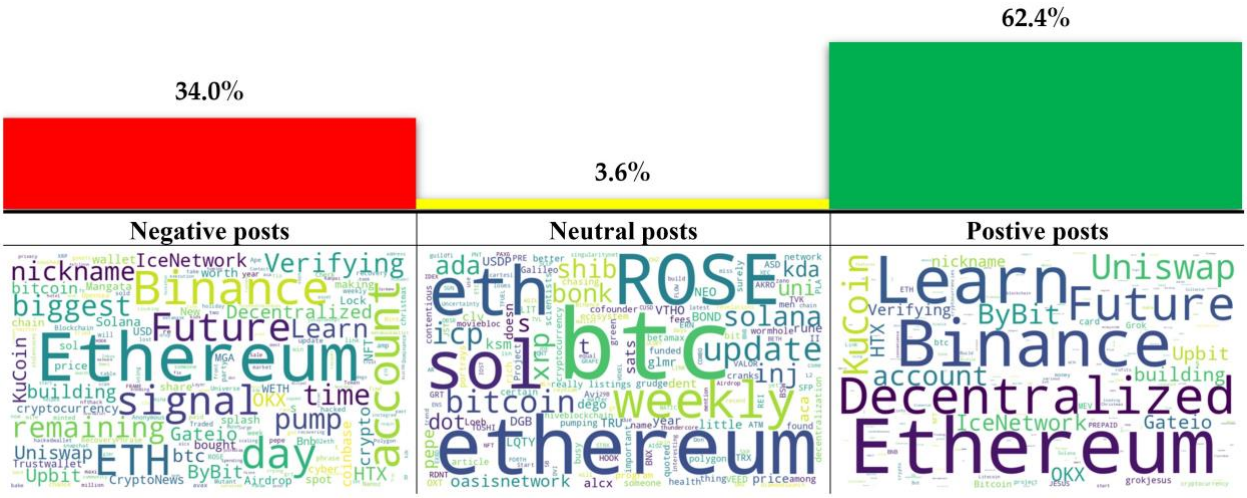

Figure 27. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Ethereum.

In contrast, 34.0% of the posts express negative sentiment, highlighting ongoing concerns within the community about Ethereum's scalability challenges. Issues such as network congestion and high gas fees are commonly discussed, reflecting frustrations with user

experience and transaction inefficiencies, particularly as Ethereum's popularity continues to rise. Neutral sentiment, which accounts for 3.6% of the posts, largely consists of factual content, news updates, and educational material about Ethereum's technology and developments, without expressing strong opinions. In summary, the sentiment analysis underscores Ethereum's significant role in the blockchain and cryptocurrency sectors, marked by a mix of optimism and critical discussions around scalability. These insights provide valuable perspectives for stakeholders, helping to better understand public sentiment as Ethereum evolves and faces new challenges.

Examining the word clouds reveals a wide range of discussions about Ethereum. Terms like "shib," "bonk," "Solana," and "Bitcoin" suggest comparisons with other cryptocurrencies, reflecting ongoing debates and contrasts within the broader crypto landscape. The frequent mention of words like "update," "network," "blockchain," and "market" highlights active conversations about Ethereum's technological advancements and its position within the broader cryptocurrency market. Additionally, terms such as "learn," "future," "building," and "decentralized" emphasize the focus on education, long-term development, and Ethereum's core value proposition as a decentralized platform.

From an investment perspective, words like "pump," "price," and "trading" suggest discussions centered around Ethereum's financial performance within the cryptocurrency market. Overall, the word cloud data reflects both optimism and concerns surrounding Ethereum. Positive sentiment dominates, reflecting enthusiasm for Ethereum's technology and its growing role in the digital asset ecosystem, while expressed concerns underline the need for ongoing improvements to address scalability issues, ensure user trust, and enhance network efficiency.

3.4.8. FTX

FTX, founded by entrepreneur SBF in 2019, was once regarded as a leading force in the cryptocurrency exchange industry, as detailed in Chapter 2. However, the company faced a catastrophic crisis in November 2022 when leaked documents exposed questionable financial practices by its founder, leading to the eventual collapse of the platform (Hetler, 2023). The fallout from this scandal reverberated across the cryptocurrency market, triggering widespread concern and a loss of investor confidence. A sentiment analysis of social media posts related to FTX reveals a strikingly dominant negative sentiment, comprising 65% of the posts (Figure

28). This negative sentiment reflects the significant public criticism and skepticism surrounding the platform, its founder, and the integrity of its operations.

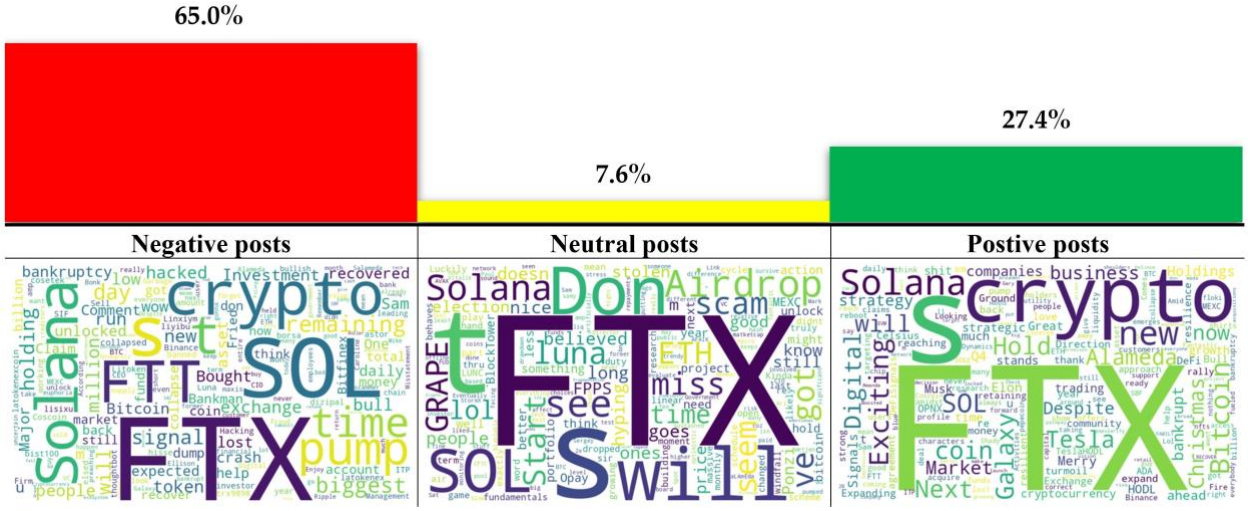

Figure 28. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about FTX.

The negative sentiment surrounding FTX can be attributed to several factors, including the platform's dramatic market performance collapse, increasing regulatory scrutiny, and the controversies surrounding its leadership. FTX's financial mismanagement, including the misappropriation of customer funds, sparked outrage and led to a public relations nightmare, further intensifying public distrust. Furthermore, the accusations against SBF, coupled with the broader implications for the cryptocurrency industry, contributed to a profound sense of skepticism and disillusionment among investors, traders, and the general public.

Linking this sentiment to broader trends in the cryptocurrency market, the data reveals a correlation between periods of heightened negative sentiment towards FTX and subsequent market declines. This observation underscores the impact of public opinion and sentiment on cryptocurrency market dynamics, which are often influenced by social media discourse. As such, the sentiment bar graph, which illustrates these negative trends, offers a visual representation of the prevailing emotions surrounding FTX, which likely contributed to a downward spiral in both the exchange's fortunes and the broader market.

Furthermore, the analysis not only reveals the public's reaction to the FTX crisis but also underscores the critical role social media plays in shaping perceptions and influencing market behavior. These broader implications emphasize the importance for investors and policymakers to closely monitor social media trends and sentiment shifts.

By understanding the emotional drivers behind these changes, stakeholders can better anticipate market fluctuations and develop more informed strategies. Additionally, when combined with other market analysis tools, they can serve as a predictive instrument, offering valuable insights into the potential direction of cryptocurrency markets following scandals like FTX.

Additionally, the word clouds provide further insight into the discussions surrounding FTX, highlighting terms such as “dump,” “hacked,” “bankruptcy,” “collapsed,” and “fraud,” which reflect serious issues that have contributed to the negative sentiment surrounding the platform. These terms indicate that incidents and controversies have severely impacted trust in FTX, leading to widespread criticism. Despite this, a significant 27.4% of posts express positive sentiment, with terms like “investment,” “bullish,” “holdings,” and “business” pointing to past optimism regarding successful trading or favorable developments within the company.

Neutral sentiment is less prominent, comprising only 7.6% of the posts, suggesting that most discussions are driven by strong opinions, either positive or negative. The word clouds also reveal a focus on the financial and investment aspects of FTX, with terms like “market,” “exchange,” “coin,” and mentions of specific cryptocurrencies. Notably, the name “Sam Bankman-Fried” appears frequently, pointing to discussions centered around leadership decisions and their impact on the platform’s future.

Overall, the sentiment analysis and word clouds depict a cryptocurrency community that remains deeply engaged with FTX. While the overall sentiment is predominantly negative, the continued presence of positive discourse indicates that there are still some within the community holding onto the potential for recovery or future opportunities.

3.4.9. Gary Gensler

Gary Gensler, the Chair of the SEC and former Goldman Sachs investment banker, has publicly expressed skepticism about cryptocurrencies, cautioning investors about the lack of regulatory oversight (Helms, 2023). Figure 29 illustrates a dominant negative sentiment of 71.6%, highlighting widespread dissatisfaction and disagreement within the cryptocurrency community on X regarding Gensler’s regulatory stance. Such criticism of regulatory figures is common in crypto communities that advocate for minimal regulation.

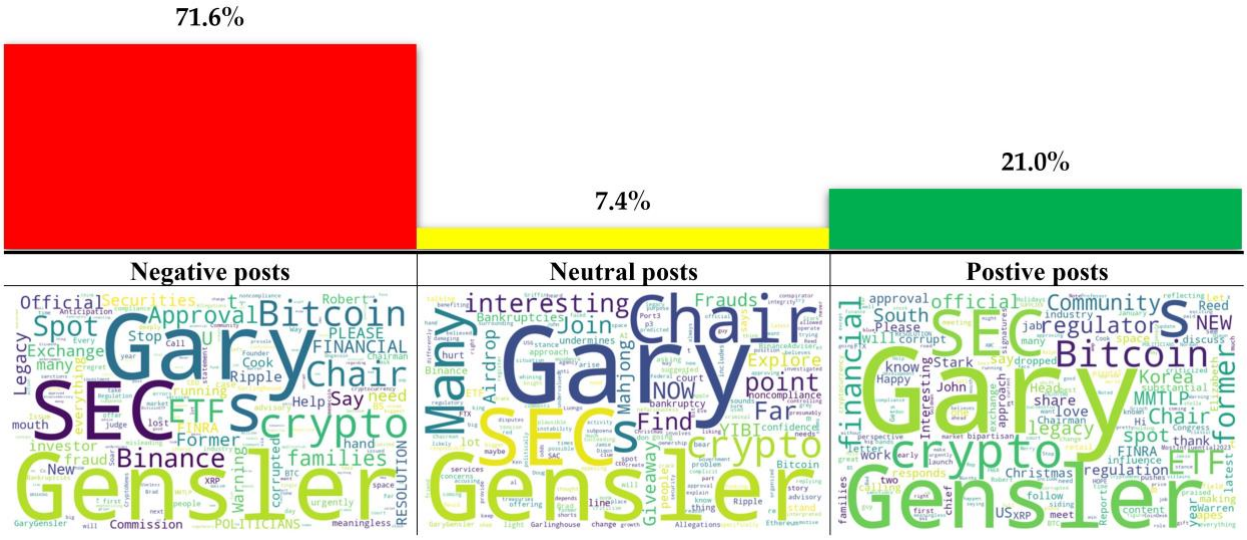

Figure 29. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Gary Gensler.

The word clouds further emphasize key concerns, featuring terms like “SEC,” “fraud,” “regulation,” “ETFs,” and “approval,” signaling apprehension about regulatory actions, particularly in tackling fraud in the crypto market. Mentions of major cryptocurrencies and platforms like “Bitcoin,” “Binance,” “XRP,” and “Ripple” reflect discussions on Gensler’s influence on prominent players in the industry, including the ongoing legal disputes involving Ripple (Godoy, 2023). These conversations highlight the broader tensions between regulatory oversight and the crypto community’s preference for greater autonomy in navigating the market.

Interestingly, positive sentiment, accounting for 21.0%, may reflect support for Gensler’s efforts to protect investors and his initiatives to introduce clarity and legitimacy to the cryptocurrency sector. This sentiment likely stems from individuals who see regulatory frameworks as essential for stabilizing the market and fostering long-term growth. These supporters may view Gensler’s actions as necessary steps to reduce fraud, increase transparency, and ultimately secure a more reliable and trustworthy environment for investors.

Meanwhile, neutral sentiment at 7.4% likely reflects factual reporting or discussions that do not express clear approval or disapproval of Gensler’s actions. These posts may focus on the details of regulatory proposals or updates on ongoing legal proceedings without offering a strong opinion on their implications for the cryptocurrency industry. This neutral tone is typically seen in news coverage or educational content aimed at informing rather than persuading the audience.

The overall sentiment landscape underscores the challenging position faced by Gensler and the SEC in their attempts to regulate the rapidly evolving cryptocurrency market. The overwhelming negative sentiment highlights the tensions between the SEC's efforts to implement stricter regulations and the cryptocurrency community's desire for more autonomy. This divide reflects the ongoing struggles to balance investor protection with the desire for less regulatory interference, an issue that is likely to shape future debates within the industry.

The data also emphasizes the active engagement of the cryptocurrency community, which closely monitors regulatory changes. This engagement highlights the importance for both regulators and market participants to understand community sentiment, as it is essential for shaping effective and well-received regulatory policies. A deep understanding of these perspectives will be crucial for developing regulatory approaches that maintain trust and foster collaboration between all stakeholders in the cryptocurrency space.

3.4.10. Monero

Monero, a privacy-focused cryptocurrency launched in 2014, is built on principles of security and decentralization. It was designed to enable untraceable and anonymous transactions using innovative features such as ring signatures, stealth addresses, and confidential transactions. These features work together to obscure the origins of transactions, generate unique addresses for each transaction, and conceal transaction amounts, thereby enhancing both privacy and fungibility. This unique approach distinguishes Monero from many other cryptocurrencies (Möser et al., 2018).

An analysis of discussions surrounding Monero reveals a broad spectrum of sentiments and topics within the cryptocurrency community, highlighting the platform's distinct place in the larger digital currency landscape. Figure 30 illustrates the sentiment bar graph, which shows that approximately 47.8% of the discourse surrounding Monero on X is positive. This reflects its strong reputation for privacy and security features, which are highly valued by users. However, there is a significant amount of negative sentiment, accounting for 35.2%, which is likely driven by concerns related to privacy coins like Monero, including their potential association with illicit activities and increasing regulatory pressures. Neutral sentiment, at 17.0%, represents a considerable portion of discussions that focus on providing updates, technological insights, or impartial analyses of Monero's market trends. This data highlights the complex and nuanced views surrounding Monero in the cryptocurrency community.

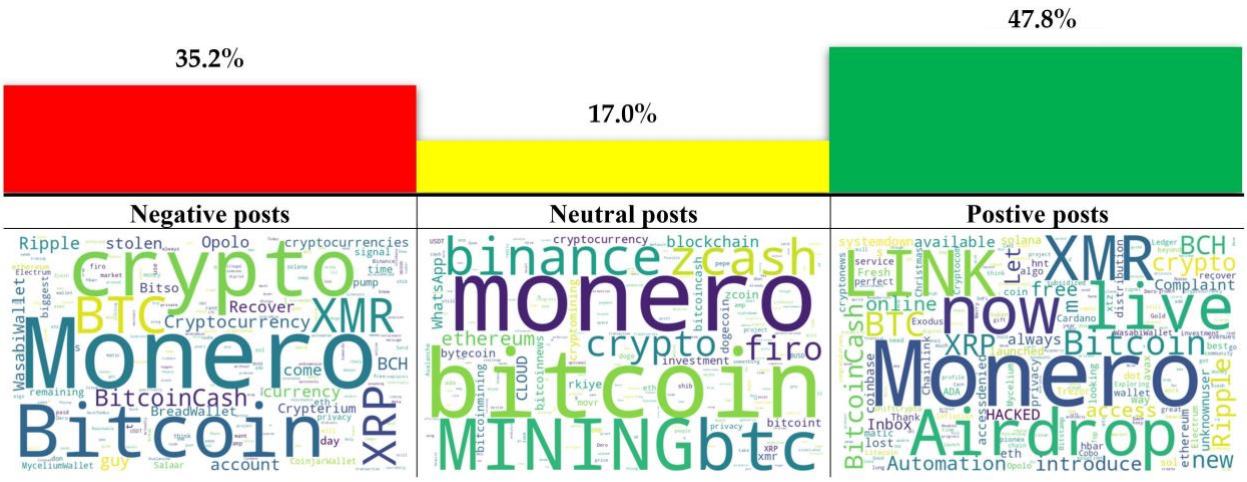

Figure 30. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Monero.

The word clouds provide a detailed snapshot of the discussions surrounding Monero, covering a wide range of topics and themes. Prominent mentions include “cryptocurrency” and “blockchain,” alongside terms like “privacy,” “wallet,” “hacked,” and “stolen,” which highlight Monero’s strong focus on privacy and security. References to other cryptocurrencies, such as “Bitcoin,” “Ethereum,” and “Ripple,” indicate comparative discussions within the broader crypto landscape. Financial aspects are also prominent, with terms like “market,” “pump,” “recover,” and “exchange” reflecting conversations about investment and speculation. Additionally, terms like “airdrop” and “mining” suggest ongoing interest in Monero’s distribution methods and mining process. In summary, findings within the Monero community span its core privacy and security features, investment potential, and market performance. While there is considerable enthusiasm for Monero’s privacy-centric approach, concerns and critical perspectives contribute to a complex and dynamic dialogue about this cryptocurrency on X.

3.4.11. Mt. Gox

Mt. Gox, founded by Jed McCaleb in 2010 and later acquired by Mark Karpeles in 2011, became one of the first prominent Bitcoin exchanges, playing a critical role in the early cryptocurrency market. However, its reputation took a major hit in 2014 when it filed for bankruptcy after losing approximately 850,000 BTC belonging to its customers, as well as an additional 200,000 BTC from its own reserves. This catastrophic event not only led to the downfall of Mt. Gox but also had a lasting impact on the cryptocurrency industry, triggering

increased scrutiny and regulatory measures around the security of cryptocurrency exchanges (Frankenfield, 2023).

Figure 31 illustrates that the sentiment surrounding Mt. Gox remains overwhelmingly negative, with 56.7% of discussions reflecting the ongoing consequences of its collapse. This negative sentiment is largely driven by the lasting distrust and disillusionment caused by the exchange's massive failure. Despite this, a smaller portion of the discourse (31.9%) maintains a positive outlook, likely driven by efforts to recover lost assets or nostalgic reflections on Mt. Gox's role in the early stages of Bitcoin's rise. Neutral sentiment, which accounts for 11.3% of the conversation, appears to consist mainly of factual discussions, such as updates on legal proceedings or historical analyses of Mt. Gox's influence on the cryptocurrency market.

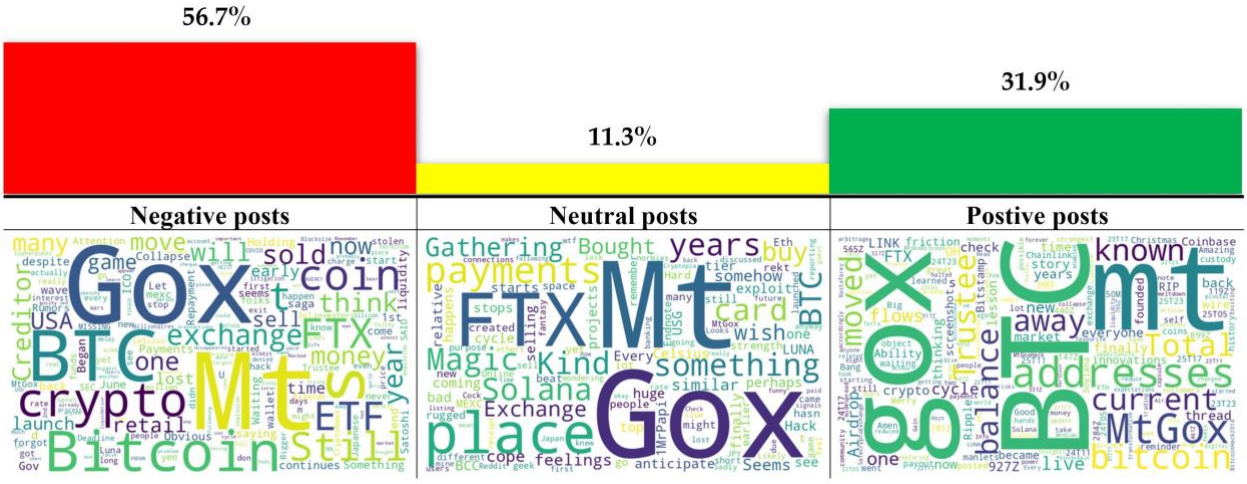

Figure 31. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about Mt. Gox.

The word clouds reveal key terms such as "Bitcoin," "exchange," "money," and "hack," which encapsulate the central narrative of Mt. Gox's rise and subsequent fall. Phrases like "collapse," "story," and "gone" highlight the dramatic downfall of the exchange, while words such as "recover" and "payments" point to ongoing efforts to address the fallout from the loss of customer funds. Other terms like "sell," "lost," and "stolen" vividly capture the adverse experiences of Mt. Gox's users during the crisis. Additionally, references to newer cryptocurrencies such as "Solana" and other crypto-related keywords indicate comparisons with more recent developments in the digital currency market, reflecting how Mt. Gox's history is often contrasted with the current state of the industry.

Overall, the data emphasizes the lasting significance of Mt. Gox within the cryptocurrency ecosystem. While negative sentiment predominates due to the shadow cast by

its catastrophic collapse, there are also moments of optimism and resolution, as stakeholders continue to navigate the aftermath of one of the most pivotal events in cryptocurrency history. These discussions reveal the complexity of Mt. Gox's legacy, as it continues to influence the cryptocurrency market's evolution.

3.4.12. Sam Bankman-Fried

SBF, formerly a prominent figure in the cryptocurrency world as the co-founder of FTX and leader of Alameda Research, experienced a dramatic rise and fall that left a lasting impact on the industry, as outlined in Chapter 2. On November 3, 2023, following a highly publicized trial, a New York jury convicted him on multiple charges, including wire fraud and conspiracy (Cohen & Godoy, 2023). The sentiment analysis of social media posts surrounding SBF provides valuable insight into the intense public reaction to his actions and the legal consequences that followed.

Figure 32 illustrates the sentiment bar graph, showing a dominant negative sentiment at 80%, reflecting widespread criticism and disillusionment toward SBF. This sentiment is likely driven by his central role in the collapse of FTX, ethical concerns about his business practices, and his sentencing, alongside the ongoing legal charges he faces. The negative sentiment represents a collective response to the perceived betrayal of trust by a figure who was once celebrated in the cryptocurrency industry. In contrast, the 15% positive sentiment likely reflects individuals who continue to appreciate SBF's earlier contributions to the crypto sector, his philanthropic efforts, or his entrepreneurial skills, despite the controversies surrounding him. The remaining 5% of neutral sentiment likely comes from observers who focus on the factual aspects of the case without offering strong personal opinions or emotional judgments.

The word clouds generated from the analysis further highlight the themes dominating public discourse surrounding SBF. Terms such as "scam," "fraud," and "trial" are highly prevalent, underscoring the focus on his legal troubles. The frequent use of words like "bankruptcy," "case," and "court" ties the public's attention to the ongoing legal proceedings and the broader financial fallout from FTX's collapse. The recurring presence of "donations" and "Democrat" reflects the controversy surrounding SBF's political donations and his influence in political circles, which was a key aspect of his public persona. Meanwhile, terms such as "Solana," "crypto," and "FTX" highlight the industries in which he was involved, and references to "settlement," "denied," and "adjournment" are indicative of the legal processes and delays that have characterized his case.

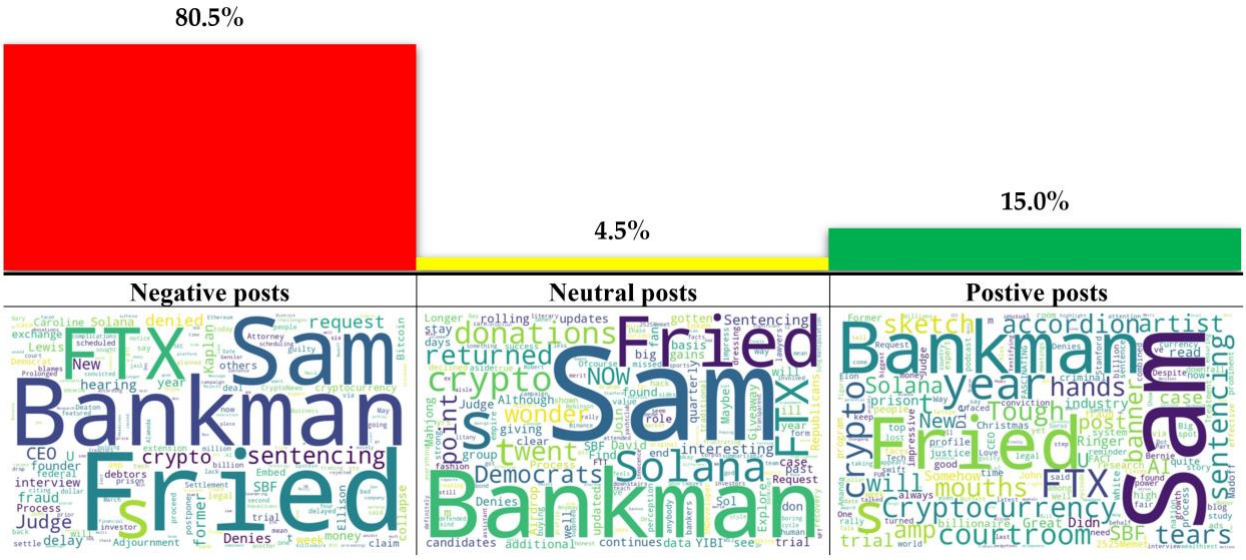

Figure 32. Sentiment distribution and corresponding word clouds illustrating negative, neutral, and positive sentiments expressed in posts about SBF.

In summary, the sentiment analysis reveals a predominantly negative perception of SBF on X, likely driven by the controversies and legal issues surrounding him. However, a notable portion of positive sentiment persists, possibly reflecting admiration for his earlier contributions to the crypto industry or other aspects of his professional and personal life. The neutral sentiment suggests that a small segment of the discourse remains objective or refrains from making strong judgments.

3.5. Bridging Cryptocurrency Markets and Public Sentiment: The Role of Real-Time Social Media Analysis in Financial Forecasting

This chapter holds considerable significance, not only for its methodological rigor but also for its novel approach to bridging the gap between the fast-moving cryptocurrency market and the real-time sentiment expressed on social media platforms. The rise of social media as a powerful tool for public expression has dramatically shifted how we understand and predict market trends. Platforms like X have become key venues for investors, enthusiasts, and critics to share opinions, concerns, and predictions, making them valuable sources for real-time sentiment analysis. This research, for instance, builds on the success of using X sentiment to predict Bitcoin's price movements, confirming that social media sentiment can offer crucial indicators of market sentiment and, by extension, financial outcomes.

The speed and volatility of the cryptocurrency market make traditional financial analysis methods less effective, particularly when it comes to DeFi and emerging crypto assets that lack the established infrastructures of traditional markets. In this context, sentiment analysis provides a timely and relevant tool to track the pulse of the market, where decentralized and highly speculative trading often takes precedence. The chapter's focus on real-time social media posts offers a unique opportunity to understand the dynamic interactions between investor sentiment, social media trends, and price fluctuations, revealing insights that might be difficult to capture through traditional financial analysis alone. This exploration taps into the immediacy of online discussions and interactions, which, in turn, are deeply intertwined with price volatility and market sentiment, particularly in the speculative world of cryptocurrency.

The integration of Python and NLP underscores the transformative potential of advanced analytical tools in today's data-driven world. Python's capabilities in data scraping, cleaning, and processing, combined with NLP's ability to analyze sentiment, enable the extraction of nuanced insights from large datasets. This methodology enhances financial analysis in the cryptocurrency space and can be applied to various fields where public sentiment influences outcomes, such as politics and consumer behavior. By focusing on real-time sentiment analysis, this study addresses a gap in the existing literature, providing valuable insights with immediate implications for market behavior. These findings are not only relevant to academia but also offer practical value to stakeholders such as investors, market analysts, influencers, and policymakers in the cryptocurrency sector.

Moreover, by examining social media data, the study enhances our understanding of the role human emotions, public perceptions, and social trends play in financial markets, where traditional models often fall short. The correlation between public sentiment on X and cryptocurrency market trends reveals significant insights into market behavior. By quantitatively analyzing sentiments (negative, neutral, and positive) and exploring the dominant themes and concerns within cryptocurrency discussions, this approach provides a real-time gauge of public opinion. These insights are invaluable for investors, policymakers, and researchers, offering a better understanding of prevailing attitudes toward cryptocurrencies and their potential market impact. In doing so, the chapter contributes to the expanding field of sentiment analysis in financial markets, particularly in the cryptocurrency sector, which is highly responsive to shifts in public sentiment (Bordoloi & Biswas, 2023; Cam et al., 2024; Déchène et al., 2024; Fang & Zhan, 2015).

It should be noted that previous studies have successfully applied NLP for predicting stock market trends, showing a correlation between public sentiment and market performance

(Cam et al., 2024; Katsafados et al., 2023). However, many existing models fail to capture the real-time impact of social media sentiment on volatile markets like cryptocurrencies due to their reliance on historical data and traditional financial indicators (Mendoza-Urdiales et al., 2022). Alternative approaches could include incorporating data from multiple social media platforms, such as Reddit, Telegram, and cryptocurrency forums, to create a more holistic view of public sentiment across different communities. Additionally, leveraging advanced sentiment classification models like RoBERTa or GPT-4 could detect more subtle emotions and contextual nuances within posts, further refining sentiment analysis. Combining these advanced approaches with traditional market analysis could enhance predictive accuracy, while cross-platform analysis would mitigate biases associated with using a single platform, offering a broader perspective on market sentiment (Kharde & Sonawane, 2016; Qi & Shabrina, 2023).

3.6. Limitations and Future Directions in Sentiment Analysis of Cryptocurrency Markets

While this research provides valuable insights, it is important to acknowledge its limitations. The reliance on X data and selected keywords may result in an incomplete view of public sentiment, potentially missing key discussions on other platforms or in languages beyond English. Furthermore, the restrictions of the X Developer Portal limited data access, capping the number of posts per keyword at 500, which reduced the overall dataset size and may have impacted the comprehensiveness of the sentiment analysis. Although an upgrade to a “Pro” user status was available, offering access to more data, the associated cost of USD 5,000 per month exceeds the doctoral project’s budget, further limiting data collection capabilities. Additionally, classifying sentiments into only negative, neutral, and positive categories may oversimplify the complexity of public opinion on cryptocurrencies. Finally, the study was conducted during the Christmas holiday period in December 2023, which may not fully capture the dynamic and fluctuating nature of cryptocurrency sentiment.

Looking ahead, future research offers numerous opportunities to deepen our understanding of sentiment analysis in financial markets. Cross-platform sentiment analysis, incorporating data from various social media platforms and discussion forums, could provide a more holistic view of public sentiment. Advanced sentiment classification techniques, using sophisticated machine learning models, could capture a broader range of emotions and nuances in the data. Longitudinal studies tracking sentiment and market trends over extended periods may reveal cyclical patterns and identify key triggers that drive market movements.

Additionally, integrating sentiment analysis with traditional financial analysis could validate its effectiveness and enhance conventional market analysis methods. While this research has its limitations, it represents an important step in merging sentiment analysis with cryptocurrency market analysis, demonstrating the value of social media data in uncovering real-time market insights. Ultimately, this chapter lays the foundation for future work that can refine our understanding of the relationship between public sentiment and financial markets, offering valuable avenues for both theoretical exploration and practical applications in the cryptocurrency sector.

Moreover, to further validate the choice of the BERT model, its performance was compared with other sentiment analysis models, including traditional machine learning models such as logistic regression and SVM, as well as other transformer-based models like RoBERTa (Garrido-Merchan et al., 2023; Turchin et al., 2023). The results consistently demonstrated that the BERT model outperformed these alternatives in terms of accuracy, precision, recall, and F1 score. To ensure the robustness of the model's performance metrics, cross-validation was performed, partitioning the dataset into multiple subsets and evaluating the model on each to confirm consistent performance. Additionally, an error analysis was conducted to identify common misclassifications, revealing that most errors occurred in posts with ambiguous language or mixed sentiments, offering valuable insights for future model improvements.

Acknowledging the limitations inherent in any machine learning model, future work will involve continuously updating the model with more recent and diverse data, fine-tuning hyperparameters, and incorporating advanced techniques to better handle nuanced sentiments. This approach addresses potential concerns regarding the model's use and underscores a commitment to methodological rigor and transparency in applying large language models for sentiment analysis.

3.7. Analyzing Research Questions: Understanding the Impact of Social Media Sentiment on Cryptocurrency Market Trends and Investor Behavior

Understanding the relationship between social media sentiment and cryptocurrency market trends is increasingly important in the context of digital currencies. Social platforms like X serve as a significant source of real-time data, providing insights into public sentiment and the factors influencing market fluctuations. The connection between sentiment dynamics on X and cryptocurrency markets sheds light on how investor behavior and market movements

are shaped. By examining the influence of sentiment on X, we gain valuable insights into the ways in which social media discussions impact market trends and decision-making processes.

Sentiment expressed on X plays a pivotal role in shaping cryptocurrency market trends. Social media platforms, particularly X, are frequently used by investors, traders, and the general public to express opinions, share market predictions, and discuss emerging trends. As cryptocurrency markets are highly reactive to news and social sentiment, shifts in public opinion on X can trigger significant market movements. Positive sentiment often correlates with upward price movements as investors may become more optimistic, while negative sentiment can lead to market sell-offs and price declines. Additionally, sentiment analysis helps identify trends related to specific cryptocurrencies, such as Bitcoin and Ethereum, and provides a predictive lens through which market fluctuations can be assessed. Investors who monitor sentiment trends on X can potentially make informed decisions that align with public perception, reducing investment risks and capitalizing on price movements (*RQ7*).

Real-time sentiment analysis has the potential to predict short-term price movements in major cryptocurrencies like Bitcoin and Ethereum. The speed at which sentiment shifts on X allows for near-instantaneous reactions to breaking news, events, or discussions, which can influence price changes. Studies have shown that sudden spikes in positive or negative sentiment often precede corresponding price fluctuations in these cryptocurrencies (Andres Rodriguez-Nieto & Eremina, 2023; Bahamazava & Nanda, 2022; Osman et al., 2024; Otabek & Choi, 2024). For instance, an influx of optimistic posts surrounding Bitcoin's adoption or Ethereum's network upgrades can result in price surges, whereas negative sentiments related to regulatory crackdowns or security breaches can drive price drops (*RQ8*). By analyzing sentiment in real-time, investors and market analysts can gain valuable insights into the immediate market response to news and developments, potentially predicting price movements before they are fully reflected in market data.

Specific cryptocurrency-related events, such as security breaches, hacks, or regulatory news, play a crucial role in shaping public sentiment and market dynamics on social media platforms like X. Events such as the FTX crash or significant regulatory announcements can drastically alter public perception and, consequently, investor behavior. Negative events, such as hacks or legal challenges, often generate waves of negative sentiment, leading to panic selling or hesitancy in investment decisions. On the other hand, positive events, such as successful network upgrades or favorable regulatory news, can spur confidence and optimism within the market, potentially triggering upward price movements (*RQ9*). By closely monitoring sentiment related to these events on social media platforms, stakeholders can better

understand how these occurrences influence the broader cryptocurrency market and adjust their strategies accordingly.

In conclusion, X posts and social media sentiment analysis offer valuable insights into the cryptocurrency market, helping investors, policymakers, and industry professionals navigate the volatile landscape of digital currencies. Understanding how sentiment influences market trends, price movements, and public reactions to specific events can provide a more nuanced approach to predicting cryptocurrency behavior and making informed investment decisions.

3.8. Analyzing Hypothesis: Sentiment Dynamics on Cryptocurrency Market Trends

In conclusion, this chapter makes a significant contribution to the field of cryptocurrency analysis by employing a comprehensive methodology and innovative approach to sentiment analysis. By selecting key topics and collecting data during periods of heightened activity, it provides a nuanced understanding of cryptocurrency market dynamics. The use of advanced NLP technology, particularly Python, enhances the depth and accuracy of the analysis, attempting to set a new standard for sentiment analysis in cryptocurrency-related discourse on social media platforms like X. All of the hypotheses tested in this chapter, namely *H7*, *H8*, and *H9*, are supported.

The analysis shows that sentiment related to regulatory news or market interventions, particularly those involving key figures like Gary Gensler, significantly impacts both trading volumes and market volatility. Positive regulatory announcements lead to increased investor confidence, whereas negative sentiment related to regulatory uncertainties can contribute to heightened market volatility (*H6* is supported).

The sentiment analysis conducted during the FTX crash and the controversies surrounding SBF demonstrated how real-time social media sentiment could serve as a leading indicator of market movements. Negative sentiment during these events correlated with significant price declines, while positive sentiment from recovery efforts suggested potential market stabilization. Investors who monitor social media sentiment closely can potentially make more informed decisions and reduce investment risks (*H7* is supported).

Moreover, the analysis found a strong correlation between sentiment on X and price movements in major cryptocurrencies like Bitcoin and Ethereum. Negative sentiment often preceded price declines, while positive sentiment typically aligned with price increases,

highlighting the predictive potential of sentiment analysis in forecasting short-term market trends (*H8* is supported).

The insights generated from this research offer valuable implications for various stakeholders. Investors can gain crucial insights into market sentiment and potential price movements by monitoring prevailing sentiments on platforms like X, helping them make more informed decisions and mitigate investment risks. Policymakers can benefit from a deeper understanding of public attitudes toward cryptocurrencies, enabling them to shape more effective regulatory frameworks. Additionally, industry professionals, such as market analysts and brand managers, can utilize the findings to inform their strategic decisions and marketing campaigns, ensuring their messaging resonates with the sentiments and preferences of their target audience. Ultimately, this chapter enhances our understanding of the evolving landscape of digital currencies. By utilizing real-time public sentiment analysis, it offers actionable insights that can provide a fresh perspective on the forces shaping the cryptocurrency market.

CONCLUSIONS

The primary aim of this dissertation was to explore and analyze the critical intersections between cryptocurrency regulation, cybercrime, and market dynamics in the digital era. Through an in-depth examination of how cryptocurrencies facilitate illicit activities, the regulatory challenges confronting global authorities, and the impact of social media sentiment on market trends, this research aimed to provide a comprehensive understanding of the complexities within the cryptocurrency ecosystem. By addressing pivotal issues such as the decentralization of finance, the risks posed by the darknet, and vulnerabilities exposed by high-profile events like the collapse of FTX, this dissertation contributes to the ongoing discourse on the necessity for adaptive and effective regulatory frameworks in response to emerging threats.

Unpacking the Complexities of Cryptocurrency Regulation, Cybercrime, and Market Dynamics: Research Questions Review

The study incorporated various dimensions of cryptocurrency regulation, cybercrime, and market behavior, considering factors such as the rise of decentralized finance platforms, the role of the darknet in enabling illegal transactions, and the influence of social media on cryptocurrency market dynamics. Through a blend of literature review, case study analysis, and sentiment analysis of social media data, this research sought to offer a nuanced, multifaceted perspective on the opportunities and challenges within the cryptocurrency landscape. The key research questions focused on understanding the role of cryptocurrencies in facilitating illicit activities, the regulatory challenges faced by global authorities, and the impact of social media sentiment on market trends. These questions were examined through a combination of theoretical and empirical research, case studies, and sentiment analysis.

The study addressed the question of how the decentralized and pseudonymous features of cryptocurrencies have contributed to the rise of cybercrime. As digital currencies continue to evolve, their dual nature—promoting innovation while enabling illicit transactions—poses a growing threat to global security. The findings show that cryptocurrencies are increasingly being exploited for money laundering, ransomware attacks, and terrorism financing, complicating efforts to combat these activities (*RQ1*).

Another significant focus was the darknet's role in facilitating cryptocurrency-based cybercrime. The anonymity provided by the darknet makes it a key platform for illegal

transactions, further complicating law enforcement's ability to disrupt criminal activities. Despite regulatory efforts, these illicit practices persist, highlighting the need for stronger international cooperation and the development of advanced technologies to curb the influence of the darknet on the cryptocurrency ecosystem (*RQ2*).

The research also examined the effectiveness of current regulatory frameworks in addressing cryptocurrency-related cybercrime. It became evident that there are significant discrepancies in regulatory approaches across different jurisdictions, which expose vulnerabilities in the global financial system. The study found that some nations have taken proactive steps to regulate cryptocurrency markets, while others lag behind, thereby creating gaps that cybercriminals can exploit. This highlights the need for more coordinated and adaptive regulatory frameworks to ensure the security and legitimacy of the cryptocurrency industry (*RQ3*).

In addition, the study explored the relationship between social media sentiment and cryptocurrency market dynamics. The rapid spread of information and opinions on platforms like X has a significant influence on investor behavior and market trends. Shifts in public sentiment, whether positive or negative, can drive market fluctuations, with social media discussions often preceding price movements in major cryptocurrencies like Bitcoin and Ethereum (*RQ7*). The research confirmed that real-time sentiment analysis can offer valuable insights into short-term price movements, providing investors with predictive tools to navigate the volatile cryptocurrency market (*RQ8*).

Finally, the study addressed how specific events, such as the collapse of FTX or regulatory announcements, influence public sentiment and investor behavior. These events often generate waves of sentiment that can lead to dramatic price changes, underlining the importance of monitoring social media sentiment to understand market reactions to cryptocurrency news (*RQ9*).

In sum, the dissertation provides a multifaceted examination of the challenges and opportunities within the cryptocurrency ecosystem. The findings emphasize the need for more robust regulation, better international cooperation, and a deeper understanding of the influence of social media on market behavior. These insights are crucial for developing more effective strategies to manage the risks associated with cryptocurrencies while harnessing their potential for innovation.

Summary of Hypotheses Validation and Findings

The conclusions derived from this study are summarized in Table 5, which provides a comprehensive overview of the findings in relation to the research hypotheses. This table synthesizes the key outcomes from each chapter, illustrating the extent to which the hypotheses were accepted (supported) or rejected not supported).

Table 5. Validation of the hypotheses.

	Hypothesis	Accepted	Rejected
H1	The rise of cryptocurrency has directly facilitated the growth of cybercrime, with decentralized finance platforms providing new avenues for illicit activities such as money laundering and drug trafficking.	X	
H2	Stronger and more coordinated international cryptocurrency regulations will significantly reduce the use of cryptocurrencies in illegal activities, including ransomware attacks and terrorism financing.		X
H3	Cryptocurrency-related cybercrimes are more prevalent in countries with less comprehensive regulatory frameworks, with the darknet acting as a major facilitator of these illegal transactions.	X	
H4	FTX's marketing and public relations strategies, particularly its high-profile celebrity endorsements, were effective in creating a positive public image, which masked underlying operational and governance issues that contributed to its downfall.	X	
H5	The legal and ethical challenges faced by FTX, including allegations of fraud and mismanagement, significantly influenced investor confidence and contributed to a market-wide decline in cryptocurrency trust and value.	X	
H6	Public sentiment on X, specifically related to regulatory news or market interventions (e.g., announcements by figures like Gary Gensler), has a significant influence on the trading volumes and volatility of major cryptocurrencies such as Bitcoin and Ethereum.	X	
H7	Real-time sentiment analysis of social media data, particularly during significant events such as the FTX crash and controversies surrounding Sam Bankman-Fried (SBF), can provide actionable insights for investors, enabling them to make more informed decisions and mitigate investment risks in volatile cryptocurrency markets.	X	
H8	Cryptocurrency market trends exhibit a correlation with fluctuations in sentiment on social media platforms like X, with negative sentiment being linked to price declines and positive sentiment correlating with price increases.	X	

The results of this dissertation offer significant insights into the various factors shaping the cryptocurrency landscape, with particular emphasis on the intersection of digital currencies, cybercrime, regulation, and market dynamics.

The first three hypotheses, concerning the relationship between cryptocurrency and cybercrime, revealed strong support for the hypothesis regarding the role of cryptocurrencies in facilitating illicit activities. Cryptocurrencies such as Bitcoin and Monero, with their decentralized and pseudonymous features, have undeniably provided a fertile ground for cybercriminals. The rise of DeFi platforms, while driving financial inclusion and technological

innovation, has simultaneously exposed significant vulnerabilities that criminals exploit for money laundering and trafficking. The use of the darknet to facilitate anonymous transactions, further exacerbated by the increasing prevalence of ransomware attacks demanding cryptocurrency payments, confirms the role of digital currencies in contemporary cybercrime (*H1*).

However, the hypothesis suggesting the need for a globally coordinated regulatory approach (*H2*) was rejected (and to some degree partially supported). Although countries like Switzerland have implemented strong regulatory frameworks to combat cryptocurrency-related crime, the lack of global coordination remains a critical issue. Regulatory efforts in certain regions are undermined by less stringent measures elsewhere, contributing to the persistence of cryptocurrency-related cybercrime. This disparity highlights the necessity for an international strategy, blending regulatory reform with advanced technologies, such as blockchain analytics, to effectively tackle this issue.

The hypothesis regarding the impact of regulatory disparities in fostering cybercrime (*H3*) was fully supported. The presence of weak or poorly enforced regulations in some regions has allowed cryptocurrency-related cybercrime to thrive. This was particularly evident in the darknet, which continues to flourish in regulatory gaps. Geographical analysis of cybercrime incidences corroborated this, demonstrating that regions with limited oversight experience higher levels of illicit activity. Strengthening global regulatory standards and fostering international collaboration are essential to curb these vulnerabilities.

The results of hypotheses *H4* and *H5* shed light on the critical factors that led to FTX's rise and subsequent collapse, with a particular focus on its marketing strategies and governance failures. *H4*, which examines the role of marketing in shaping FTX's image, was strongly supported. The platform's strategic use of celebrity endorsements and partnerships with high-profile sports teams played a crucial role in cultivating an image of legitimacy and trustworthiness. Figures like Tom Brady and Gisele Bündchen helped position FTX as a reputable player in the cryptocurrency space, attracting both retail and institutional investors. This powerful marketing strategy concealed underlying operational and governance problems within the company, masking issues like conflicts of interest and a lack of financial transparency.

Similarly, *H5*, which explores the impact of legal and ethical issues on FTX's downfall, was also supported. As allegations of fraud, mismanagement, and the misuse of customer funds surfaced, investor confidence in the platform rapidly eroded. This loss of trust was compounded by legal challenges faced by FTX's leadership, including charges of wire fraud and conspiracy,

which reinforced the perception of systemic corruption within the company. The collapse of FTX not only undermined its own reputation but also had a far-reaching impact on the broader cryptocurrency market, eroding investor confidence and triggering a significant decline in cryptocurrency prices. The interplay of marketing, governance failures, and legal troubles ultimately led to the company's rapid downfall and amplified skepticism toward the cryptocurrency sector as a whole.

The final three hypotheses, *H6*, *H7*, and *H8*, which focus on the influence of social media sentiment on cryptocurrency markets, were all strongly supported. *H6* demonstrated that sentiment related to regulatory news and market interventions significantly affects market dynamics, particularly in terms of trading volumes and volatility. Positive regulatory developments tend to bolster investor confidence, while negative sentiment surrounding regulatory uncertainty can contribute to increased market volatility. This relationship underscores the sensitivity of the cryptocurrency market to public perceptions of regulatory actions.

H7 further supported the idea that real-time sentiment on social media platforms, such as X, can act as a leading indicator of market movements. During events like the FTX collapse, negative sentiment was closely correlated with significant price declines, while recovery efforts were often reflected in positive sentiment, signaling potential market stabilization. This finding highlights the predictive value of social media sentiment for market participants, offering insights that could help mitigate investment risks.

Finally, *H8* reinforced the strong correlation between social media sentiment and price fluctuations in major cryptocurrencies like Bitcoin and Ethereum. Negative sentiment was generally associated with price declines, while positive sentiment tended to align with price increases. This correlation suggests that sentiment analysis on social media platforms can provide valuable insights into short-term market trends, helping investors make more informed decisions. Together, these hypotheses demonstrate the critical role of public sentiment in shaping cryptocurrency market behavior, offering actionable insights for investors, policymakers, and industry professionals.

In summary, the hypotheses tested throughout this dissertation provide important contributions to understanding the multifaceted dynamics of the cryptocurrency market. By examining the relationships between cryptocurrency, cybercrime, regulatory efforts, market behavior, and social media sentiment, this research enhances our understanding of the sector's complexities and offers actionable insights for investors, policymakers, and industry professionals. The findings underscore the need for improved global regulatory cooperation,

transparency in governance, and a more sophisticated approach to monitoring market sentiment to ensure a stable and secure cryptocurrency environment.

Recommendations for Addressing Cryptocurrency Regulation, Cybercrime, and Market Dynamics

The following recommendations are laid out to address the critical intersections between cryptocurrency regulation, cybercrime, and market dynamics, as explored in this dissertation. These suggestions aim to provide actionable insights for policymakers, regulators, industry leaders, and investors, focusing on strengthening global governance frameworks, mitigating cybercrime risks, and enhancing market stability in the rapidly evolving digital currency landscape. By considering both the regulatory challenges and the broader market implications of cryptocurrencies, these recommendations seek to foster a more secure, transparent, and sustainable ecosystem for all stakeholders involved in the cryptocurrency sector.

Based on the primary aim of the dissertation, which was to explore and analyze the critical intersections between cryptocurrency regulation, cybercrime, and market dynamics in the digital era, the following recommendations are made:

- To mitigate the risks posed by cryptocurrency-related cybercrime, it is essential for countries to collaborate in developing and implementing comprehensive and coordinated regulatory frameworks. These frameworks should prioritize AML and KYC policies, as well as facilitate cross-border information sharing to address the gaps that cybercriminals exploit. A unified global approach would help close these vulnerabilities and enhance the effectiveness of regulatory efforts in combating illicit activities in the cryptocurrency space.
- Governments and regulatory bodies should invest in advanced blockchain analytics tools to improve their ability to track and trace illicit cryptocurrency transactions. By implementing these technologies, authorities can more effectively identify and disrupt cybercrime activities, such as money laundering, ransomware payments, and illegal trading, ultimately enhancing efforts to regulate the cryptocurrency market and reduce its use for criminal purposes.
- Given the global reach and complexity of cryptocurrency-related cybercrime, it is essential to strengthen international collaboration among law enforcement agencies, regulatory bodies, and financial institutions. The decentralized and borderless nature of digital currencies means that illicit activities often span multiple countries, making it

difficult for any single nation to effectively address these crimes. Therefore, fostering closer cooperation between nations is crucial to combating these issues on a global scale. Establishing regular global summits, as well as facilitating information exchanges and joint task forces, would provide a platform for sharing best practices, coordinating investigations, and ensuring that regulatory frameworks align across borders. This collaborative approach would not only help in tackling cross-border cryptocurrency crimes more effectively but also promote a unified and robust international response to emerging cyber threats in the digital economy.

- Governments should prioritize the establishment of clear and consistent legal definitions and standards for cryptocurrencies to address regulatory inconsistencies across jurisdictions. By creating comprehensive frameworks that define digital assets, their intended use cases, and the responsibilities of platform operators, authorities can foster a more secure and transparent environment for both users and businesses. These regulations should not only focus on consumer protection but also on mitigating the risk of cybercrime, including fraud, money laundering, and illicit transactions. Clear legal guidelines will provide greater accountability, ensuring that stakeholders within the cryptocurrency ecosystem adhere to responsible practices while also enhancing trust among investors and users. Furthermore, these standards can help streamline global regulatory efforts, ensuring a cohesive approach to cryptocurrency governance.
- Increasing public awareness about the risks associated with cryptocurrencies, particularly in relation to cybercrime, is crucial for protecting users and fostering a more secure digital ecosystem. Many individuals are drawn to the promise of high returns and financial autonomy offered by cryptocurrencies, but they may lack the knowledge to understand the inherent risks. Therefore, it is essential to implement widespread educational programs and awareness campaigns to help users grasp the potential dangers posed by cybercriminals and the vulnerabilities of unregulated platforms. These initiatives should focus on educating the public about safe transaction practices, recognizing phishing attempts, avoiding scams, and understanding how decentralized platforms may expose them to greater risks. By improving knowledge and empowering users to make informed decisions, the likelihood of falling victim to illicit activities or security breaches can be significantly reduced.
- Cryptocurrency exchanges should be mandated to implement more stringent governance measures to enhance transparency and accountability. This includes the adoption of comprehensive reporting systems that detail financial activities, as well as

the establishment of robust internal controls to prevent mismanagement and fraud. Regular external and internal audits should be conducted to ensure compliance with both industry standards and regulatory requirements. Such measures would not only help mitigate the risks of internal governance failures, as seen in the case of FTX, but also foster greater trust and confidence among investors, regulators, and users. By improving oversight and transparency, exchanges can reduce the opportunity for financial misconduct, ensuring that they operate in a more secure and reliable manner.

- Regulatory bodies should foster the development of ethical and transparent cryptocurrency platforms by offering incentives to exchanges and platforms that uphold high governance standards. These incentives could support efforts to prevent fraud, money laundering, and other illicit activities, ensuring a more secure and trustworthy cryptocurrency ecosystem.
- Regulatory authorities should consider exploring the integration of cryptocurrencies into existing financial systems within a regulated environment to reduce their appeal for illegal activities. This integration should focus on ensuring that cryptocurrencies adhere to financial industry standards for transparency and accountability, fostering a more secure and controlled ecosystem that mitigates the risk of misuse.
- Policymakers and regulators should seriously consider incorporating real-time sentiment analysis into their market monitoring strategies. The ability to track social media sentiment and public reactions as they occur can provide invaluable insights into public attitudes toward cryptocurrencies, especially during significant regulatory developments, market interventions, or periods of crisis. By leveraging sentiment data from platforms like X and other social media channels, regulators can anticipate how the market might respond to proposed changes or emerging risks. This proactive approach would allow for more agile regulatory actions, enabling authorities to address potential market disruptions before they escalate. Additionally, by understanding the emotional and psychological drivers behind market fluctuations, regulators can better assess the effectiveness of their policies and adjust them in real time, ensuring a more responsive and resilient regulatory framework. By embracing this technology, regulators can stay ahead of market dynamics, allowing them to navigate the rapidly evolving cryptocurrency space with greater precision and foresight.
- To address the complexities of cryptocurrency regulation, governments and regulatory bodies must prioritize investment in and the development of regulatory technologies. These advanced tools can play a pivotal role in enhancing the oversight of

cryptocurrency transactions and market activities. By harnessing the capabilities of AI, machine learning, and big data analytics, regulatory technologies can significantly improve the efficiency and accuracy of compliance processes. Through automation, these technologies can quickly identify patterns and anomalies, allowing regulatory authorities to detect suspicious activities in real-time, such as money laundering or market manipulation. This not only ensures a more proactive approach to regulatory enforcement but also helps to reduce the burden on human resources, allowing regulators to focus on more complex cases. Furthermore, by fostering innovation in these technologies, governments can create a more adaptable regulatory framework that keeps pace with the rapidly evolving cryptocurrency landscape. Ultimately, the integration of regulatory technologies into the regulatory ecosystem can enhance transparency, increase trust in digital currencies, and mitigate the risks associated with illicit activities.

By implementing these recommendations, policymakers, regulators, and industry leaders can strengthen the security, transparency, and stability of the cryptocurrency market, effectively mitigating the risks associated with cybercrime. This collaborative approach will help create a more secure and resilient digital economy.

In conclusion, the evolving landscape of cryptocurrency presents both tremendous opportunities and significant challenges, and addressing these requires coordinated efforts across governance, regulation, and technological innovation.

REFERENCES

Abrams, Z. (2023, December 16). *FTX's revised reorganization plan values crypto claims at time of bankruptcy*. The Block. https://www.theblock.co/post/267979/ftxs-revised-reorganization-plan-values-crypto-claims-at-time-of-bankruptcy

Adam, I. O., & Dzang Alhassan, M. (2020). Bridging the Global Digital Divide Through Digital Inclusion: The Role of ICT Access and ICT Use. *Transforming Government: People, Process and Policy*, *15*(4), Article 4. https://doi.org/10.1108/TG-06-2020-0114

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and Crypto Forensics: Investigating Crypto Frauds. *International Journal of Network Management*, *34*(2), e2255. https://doi.org/10.1002/nem.2255

Aggarwal, S., & Jaiswal, U. (2011). Kryptos + Graphein = Cryptography. *Science and Technology*, *3*(9), Article 9.

Ahuja, A., Ribeiro, V. J., & Pal, R. (2021). *A Regulatory System for Optimal Legal Transaction Throughput in Cryptocurrency Blockchains* (No. arXiv:2103.16216; Issue arXiv:2103.16216). arXiv. http://arxiv.org/abs/2103.16216

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., & Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities*, *60*, 234–245.

Aitken, F. (2020). *Trusting Cryptocurrencies: Aspects of the Common Law and Equity Affecting Cryptocurrency Owners*. University of Otago. https://www.otago.ac.nz/__data/assets/pdf_file/0015/331530/trusting-cryptocurrencies-aspects-of-the-common-law-and-equity-affecting-cryptocurrency-owners-828533.pdf

Al Jazeera. (2023, November 3). *What to know about the Sam Bankman-Fried trial verdict*. Al Jazeera. https://www.aljazeera.com/news/2023/11/3/what-to-know-about-the-sam-bankman-fried-trial-verdict

Albergotti, R., & Matsakis, L. (2022, November 17). *Effective Altruism group debated Sam Bankman-Fried's ethics in 2018 | Semafor*. https://www.semafor.com/article/11/18/2022/effective-altruism-group-debated-sam-bankman-frieds-ethics-in-2018

Alfieri, C. (2022). Cryptocurrency and National Security. *International Journal on Criminology*, *9*(1), Article 1. https://doi.org/10.18278/IJC.9.1.3

Ali, A. (2021). *Cryptocurrencies Security and Dispute Resolution.* University of Cumberlands. https://www.researchgate.net/publication/351334217_Cryptocurrencies_security_and_dispute_resolution

Aliaj, O., & Oliver, J. (2022, November 17). *Scaramucci's SkyBridge bought $10mn of FTX token in return for investment*. https://www.ft.com/content/08370364-40af-4a1c-a85e-a9243be173c8

Allison, I. (2022, November 2). *Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet*. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/

Almomani, A. (2023). Darknet Traffic Analysis, and Classification System Based on Modified Stacking Ensemble Learning Algorithms. *Information Systems and E-Business Management*, *10*, 1–32. https://doi.org/10.1007/s10257-023-00626-2

Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information*, *15*(2), Article 2. https://doi.org/10.3390/info15020109

Alter, C. (2023, March 15). *Exclusive: Effective Altruist Leaders Were Warned About Sam Bankman-Fried Years Before FTX Collapsed*. TIME. https://time.com/6262810/sam-bankman-fried-effective-altruism-alameda-ftx/

Alvarez, F., Argente, D., & Van Patten, D. (2022). *Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador* (No. 4094160). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4094160

Al-Zubaidie, M., & Jebbar, W. (2024). Transaction Security and Management of Blockchain-Based Smart Contracts in E-Banking-Employing Microsegmentation and Yellow Saddle Goatfish. *Mesopotamian Journal of CyberSecurity*, *4*(2), Article 2. https://doi.org/10.58496/MJCS/2024/005

Ambrus, I., & Mezei, K. (2022). The New Hungarian Legislation on Money Laundering and the Current Challenges of Cryptocurrencies. *Danube Publishing*, *13*(4), Article 4. https://doi.org/10.2478/danb-2022-0016

Andres Rodriguez-Nieto, J., & Eremina, K. (2023). *The Effects of COVID-19 and the Increasing Relationship Between Individual Investor Sentiment, Cryptocurrencies, and the US Market* (No. 4729404). SSRN Scholarly Paper. https://papers.ssrn.com/abstract=4729404

Andronova, I., Gusakov, N., Peoples' Friendship University of Russia (RUDN University), & Zavyalova, E. (2020). Terrorism Financing: New Challenges for International Security. *International Organisations Research Journal*, *15*(1), Article 1. https://doi.org/10.17323/1996-7845-2020-01-05

AP. (2022, November 17). Tom Brady, Larry David, Other Celebs and Sports Stars Named in FTX Lawsuit. *NBC 6 South Florida*. https://www.nbcmiami.com/news/local/tom-brady-larry-david-other-celebs-and-sports-stars-named-in-ftx-lawsuit/2911290/

Arif, T. (2023, October 29). Voyager Digital: Navigating the World of CryptoCurrency Trading. *Medium*. https://medium.com/@talha7us/voyager-digital-navigating-the-world-of-cryptocurrency-trading-a2822baa9834

Auer, R., & Tercero-Lucas, D. (2022). Distrust or Speculation? The Socioeconomic Drivers of US Cryptocurrency Investments. *Journal of Financial Stability*, *62*, 101066. https://doi.org/10.1016/j.jfs.2022.101066

Australian Home Affairs. (2022). *Exploring Cryptocurrency*. Cyber Security Industry Advisory Committee.

Aysan, A. F., Batten, J. A., Gozgor, G., Khalfaoui, R., & Nanaeva, Z. (2023). Twitter Matters for Metaverse Stocks Amid Economic Uncertainty. *Finance Research Letters*, *56*, 104116. https://doi.org/10.1016/j.frl.2023.104116

Badawi, E., & Jourdan, G.-V. (2020). Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review. *IEEE Access*, *8*, 200021–200037. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3034816

BaFin. (2018). *Money Laundering Act*. Federal Financial Supervisory Authority. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html

Bahamazava, K., & Nanda, R. (2022). The Shift of Darknet Illegal Drug Trade Preferences in Cryptocurrency: The Question of Traceability and Deterrence. *Forensic Science International: Digital Investigation*, *40*, 301377. https://doi.org/10.1016/j.fsidi.2022.301377

Bajra, U., Rogova, P. D. E., & Avdiaj, P. D. S. (2024). *Cryptocurrency Blockchain and Its Carbon Footprint: Anticipating Future Challenges* (No. 4735982). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4735982

Balaskas, A., & Franqueira, V. N. L. (2018). Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. *2018 International Conference on Cyber Security and*

Protection of Digital Services (Cyber Security), 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560672

Bambysheva, N. (2021, March 11). *BlockFi Gets A $3 Billion Valuation With New $350 Million Series D Funding*. Forbes. https://www.forbes.com/sites/ninabambysheva/2021/03/11/blockfi-gets-a-3-billion-valuation-with-new-350-million-series-d-funding/

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques. *European Journal of Law and Economics*, *47*(2), Article 2. https://doi.org/10.1007/s10657-019-09609-6

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency Scams: Analysis and Perspectives. *IEEE Access*, *9*, 148353–148373. https://doi.org/10.1109/ACCESS.2021.3123894

Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. *Buildings*, *11*(7), Article 7. https://doi.org/10.3390/buildings11070283

Bertola, F. (2020). Drug Trafficking on Darkmarkets: How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime. *American Journal of Qualitative Research*, *4*(2), Article 2. https://doi.org/10.29333/ajqr/8243

Betz, K., Giordano, M., Hillmann, H. A. K., Duncker, D., Dobrev, D., & Linz, D. (2024). The Impact of Twitter/X Promotion on Visibility of Research Articles: Results of the #TweetTheJournal Study. *IJC Heart & Vasculature*, *50*, 101328. https://doi.org/10.1016/j.ijcha.2023.101328

Bhardwaj, A., Bharany, S., & Kim, S. (2024). Fake Social Media News and Distorted Campaign Detection Framework Using Sentiment Analysis & Machine Learning. *Heliyon*, *10*(16), e36049. https://doi.org/10.1016/j.heliyon.2024.e36049

Bhaskar, V., Linacre, R., & Machin, S. (2019). The Economic Functioning of Online Drugs Markets. *Journal of Economic Behavior & Organization*, *159*, 426–441. https://doi.org/10.1016/j.jebo.2017.07.022

Bibri, S. E. (2019). On the sustainability of smart and smarter cities in the era of big data: An interdisciplinary and transdisciplinary literature review. *Journal of Big Data*, *6*(1), 25. https://doi.org/10.1186/s40537-019-0182-7

Binance. (2019, December 20). *Binance Announces Strategic Investment in Cryptocurrency Derivatives Exchange FTX*. Binance Blog.

https://www.binance.com/en/blog/all/binance-announces-strategic-investment-in-cryptocurrency-derivatives-exchange-ftx-414610870200725504

Biswas, R. (2018). *Emerging Markets Megatrends*. Springer. https://doi.org/10.1007/978-3-319-78123-5

BitDegree. (2023). *What are Darknodes?* BitDegree. https://www.bitdegree.org/crypto/learn/crypto-terms/what-are-darknodes

Bitvo. (2022, November 15). Bitvo announces termination of pending transaction with FTX Canada Inc. And FTX Trading Ltd. *Bitvo*. https://bitvo.com/press-releases/bitvo-announces-termination-of-pending-transaction-with-ftx-canada-inc-and-ftx-trading-ltd/

Blasco, N. J., & Fett, N. A. (2019). Blockchain Security: Situational Crime Prevention Theory and Distributed Cyber Systems. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(2), Article 2. https://doi.org/10.52306/02020419tegr1675

Bloomberg. (2024, September 13). Sam Bankman-Fried Seeks New Trial, Blaming Federal Judge for Ridiculing Him. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2024-09-13/sbf-seeks-new-trial-blaming-federal-judge-for-ridiculing-him

Boehm, F., & Pesch, P. (2014). Bitcoin: A First Legal Analysis. In R. Böhme, M. Brenner, T. Moore, & M. Smith (Eds.), *Financial Cryptography and Data Security* (pp. 43–54). Springer. https://doi.org/10.1007/978-3-662-44774-1_4

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), Article 2. https://doi.org/10.1257/jep.29.2.213

Bokovnya, A. Y., Shutova, A. A., Zhukova, T. G., & Ryabova, L. V. (2020). Legal Measures for Crimes in the Field of Cryptocurrency Billing. *Utopia Y Praxis Latinoamericana*, *25*(Extra7), Article Extra7. https://doi.org/10.5281/zenodo.4009713

Bordoloi, M., & Biswas, S. K. (2023). Sentiment Analysis: A Survey on Design Framework, Applications and Future Scopes. *Artificial Intelligence Review*, 1–56. https://doi.org/10.1007/s10462-023-10442-2

Botha, J. G., Botha, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *International Conference on Cyber Warfare and Security*, *18*(1), Article 1. https://doi.org/10.34190/iccws.18.1.1087

Bray, J. D. (2016). Anonymity, Cybercrime, and the Connection to Cryptocurrency. *Online Theses and Dissertations*, *344*, Article 344.

Broadhead, S. (2018). The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments. *Computer Law & Security Review*, *34*(6), Article 6. https://doi.org/10.1016/j.clsr.2018.08.005

Brown, S. D. (2016). Cryptocurrency and Criminality. *The Police Journal: Theory, Practice and Principles*, *89*(4), Article 4. https://doi.org/10.1177/0032258x16658927

Browne, R. (2022, February 2). *Crypto exchange FTX to buy Japanese rival Liquid for Asia expansion*. CNBC. https://www.cnbc.com/2022/02/02/crypto-exchange-ftx-to-buy-japanese-rival-liquid.html

Butler, S. (2019). Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King? *Journal of Cyber Policy*, *4*(3), Article 3. https://doi.org/10.1080/23738871.2019.1680720

Čábelková, I., Smutka, L., Mareš, D., Ortikov, A., & Kontsevaya, S. (2023). Environmental Protection or Economic Growth? The Effects of Preferences for Individual Freedoms. *Frontiers in Environmental Science*, *11*. https://doi.org/10.3389/fenvs.2023.1129236

Cam, H., Cam, A. V., Demirel, U., & Ahmed, S. (2024). Sentiment Analysis of Financial Twitter Posts on Twitter with the Machine Learning Classifiers. *Heliyon*, *10*(1), e23784. https://doi.org/10.1016/j.heliyon.2023.e23784

Campino, J., Brochado, A., & Rosa, Á. (2022). Initial coin offerings (ICOs): Why do they succeed? *Financial Innovation*, *8*(1), 17. https://doi.org/10.1186/s40854-021-00317-2

Caporale, G. M., Kang, W.-Y., Spagnolo, F., & Spagnolo, N. (2020). *Cyber-Attacks and Cryptocurrencies* (Working Paper No. 8124; Issue 8124). CESifo Working Paper. https://www.econstor.eu/handle/10419/216520

Carreras, T. (2023, October 6). *FTX co-founder Gary Wang drops $65bn bombshell—Who is SBF's star coder?* DL News. https://www.dlnews.com/articles/people-culture/meet-ftx-founder-gary-wang-who-testified-against-sbf/

Castillo, M. del. (2017, January 23). *Bitcoin Options Firm LedgerX Crosses Key Launch Hurdle*. https://www.coindesk.com/markets/2017/01/23/bitcoin-options-firm-ledgerx-crosses-key-launch-hurdle/

Ceekz. (2023, November 15). *The political connections of FTX and its CEO Sam Bankman Fried. How deep does the rabbit hole go?* https://www.publish0x.com/thought-process/the-political-connections-of-ftx-and-its-ceo-sam-bankman-fri-xpzlwre

Celiksoy, E., & Schwarz, K. (2023). *Investigation into Financial Transactions Used in the Online Sexual Exploitation of Children*. University of Nottingham.

CERT-Bund. (2022). Ransomware Bedrohungslage. *Bundesamt für Sicherheit in der Informationstechnik*.

CFTC. (2017a). *CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products*. Commodities Futures Trading Commission. https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_factsheet120117.pdf

CFTC. (2017b). *CFTC Grants DCO Registration to LedgerX LLC*. Commodities Futures Trading Commission. https://www.cftc.gov/PressRoom/PressReleases/7592-17

Chand, P., G., M., Sai, B., D., B., & G, L. (2024). *Blockchain Security: Work on Securing Blockchain Networks and Smart Contracts* (SSRN Scholarly Paper No. 4751504). https://papers.ssrn.com/abstract=4751504

Chen, P. (2023). The Relationship Between Blockchain and Government Regulation and Governance: The Distinctions Between Different Countries. *Applied and Computational Engineering*, *5*(1), Article 1. https://doi.org/10.54254/2755-2721/5/20230685

Chen, Y., Pereira, I., & Patel, P. C. (2020). Decentralized Governance of Digital Platforms. *Journal of Management*, *XX No. X*, 014920632091675. https://doi.org/10.1177/0149206320916755

Chen, Y.-L., Chang, Y. T., & Yang, J. J. (2023). Cryptocurrency Hacking Incidents and the Price Dynamics of Bitcoin Spot and Futures. *Finance Research Letters*, *55*, 103955. https://doi.org/10.1016/j.frl.2023.103955

Cherniei, V., Cherniavskyi, S., Babanina, V., & Tykho, O. (2021). Criminal Liability for Cryptocurrency Transactions: Global Experience. *European Journal of Sustainable Development*, *10*(4), Article 4. https://doi.org/10.14207/ejsd.2021.v10n4p304

Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. *Global Commission on Internet Governance*, *6*, Article 6.

Chimienti, M. T., Kochanska, U., & Pinna, A. (2019). Understanding the Crypto-Asset Phenomenon, Its Risks and Measurement Issues. *Economic Bulletin*, *5*, 1–23. https://doi.org/10.2866/429865

Chittum, M. (2022, December 29). *Inside the relationship between Sam Bankman-Fried's FTX and Solana, the blockchain he championed whose token is down 96% from its highs*. Markets Insider. https://markets.businessinsider.com/news/currencies/sam-bankman-fried-ftx-bankruptcy-alameda-solana-price-crash-sol-2022-12

Chittum, M. (2023, January 21). *Sam Bankman-Fried attended a top Silicon Valley prep school where his senior class prank reportedly included making $100 bills with his face on them called "Bankmans."* Yahoo Finance. https://finance.yahoo.com/news/sam-bankman-fried-attended-top-162449232.html

Choi, S., Choi, K.-S., Sungu-Eryilmaz, Y., & Park, H.-K. (2020). Illegal Gambling and Its Operation Via the Darknet and Bitcoin: An Application of Routine Activity Theory. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(1), Article 1. https://doi.org/10.52306/03010220htli7653

Choi, S., & Parti, K. (2022). Understanding the Challenges of Cryptography-Related Cybercrime and Its Investigation. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(2), Article 2. https://doi.org/10.52306/2578-3289.1134

Choi, T., Shorubalko, I., Gustavsson, S., Schön, S., & Ensslin, K. (2009). Correlated Counting of Single Electrons in a Nanowire Double Quantum Dot. *New Journal of Physics*, *11*(1), Article 1. https://doi.org/10.1088/1367-2630/11/1/013005

Christian, A. (2023, October 10). *FTX's Sam Bankman-Fried believed in "effective altruism". What is it?* https://www.bbc.com/worklife/article/20231009-ftxs-sam-bankman-fried-believed-in-effective-altruism-what-is-it

Chuan, T., & O'Leary, R. R. (2021). *China's Bitcoin Exchanges Receive Shutdown Orders and Closure Timeline*. CoinDesk. https://www.coindesk.com/markets/2017/09/15/chinas-bitcoin-exchanges-receive-shutdown-orders-and-closure-timeline/

Cimpanu, C. (2021, August 19). *Japanese crypto-exchange Liquid hacked for $94 million*. https://therecord.media/japanese-crypto-exchange-liquid-hacked-for-94-million

Ciphertrace. (2023). *Crypto Crimes & Anti-Money Laundering Report 2023*. Ciphertrace. https://ciphertrace.com/crime-and-anti-money-laundering-report-march-2023/

Cirella, G. T., & Tao, L. (2008). Measuring Sustainability: An Application using the Index of Sustainable Functionality in South East Queensland, Australia. *The International Journal of Interdisciplinary Social Sciences: Annual Review*, *3*. https://doi.org/10.18848/1833-1882/CGP/v03i08/52680

Cirella, G. T., & Tao, L. (2009). The Index of Sustainable Functionality: An Application for Measuring Sustainability. *World Academy of Science Engineering and Technology: International Journal of Humanities and Social Sciences*, *3*(4), 268–274. https://doi.org/10.5281/zenodo.1330369

Cirella, G. T., & Zerbe, S. (2014a). Index of Sustainable Functionality: Application in Urat Front Banner. In G. T. Cirella & S. Zerbe (Eds.), *Sustainable water management and*

wetland restoration in settlements of continental-arid Central Asia (pp. 137–155). Bozen University Press. https://doi.org/10.13124/9788860461094_10

Cirella, G. T., & Zerbe, S. (2014b). *Sustainable Water Management and Wetland Restoration in Settlements of Continental-Arid Central Asia*. Free University of Bozen.

CISA. (2023). *Malware, Phishing, and Ransomware*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Ciulli, F., & Kolk, A. (2023). International Business, digital technologies and sustainable development: Connecting the dots. *Journal of World Business*, *58*(4), 101445. https://doi.org/10.1016/j.jwb.2023.101445

Clements, R. (2021). *Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps* (No. 3891809). SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3891809

Cohen, L., & Godoy, J. (2023, November 3). *Sam Bankman-Fried Convicted of Multi-Billion Dollar FTX Fraud*. Reuters. https://www.reuters.com/legal/ftx-founder-sam-bankman-fried-thought-rules-did-not-apply-him-prosecutor-says-2023-11-02/

Coin Desk. (2023, September 20). *Sam Bankman-Fried's Empire Was Crushed by This Infamous Balance Sheet. Here's More of the Story*. Markets.Businessinsider.Com. https://markets.businessinsider.com/news/currencies/breaking-down-the-infamous-alameda-balance-sheet-1032644341

Collins, J. (2022). *Crypto, Crime and Control*. Global Initiative Against Transnational Organized Crime.

Cong, L. W., Harvey, C. R., Rabetti, D., & Wu, Z.-Y. (2022). *An Anatomy of Crypto-Enabled Cybercrimes* (No. 4188661; Issue 4188661). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4188661

Connolly, L., & Wall, D. S. (2019). The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Conventus Law. (2021, April 20). Financial Crimes Compliance For Cryptocurrency: Why Can't We All Agree? *Conventus Law*. https://conventuslaw.com/report/financial-crimes-compliance-for-cryptocurrency-why/

Copeland et al. (2022, July 18). *Crypto lender Celsius loaned $75 million to Three Arrows Capital*. The Block. https://www.theblock.co/post/158164/crypto-lender-celsius-loaned-75-million-to-three-arrows-capital

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The Destabilising Effects of Cryptocurrency Cybercriminality. *Economics Letters*, *191*, 108741. https://doi.org/10.1016/j.econlet.2019.108741

Courtois, N. T. (2014). *Crypto Currencies and Bitcoin*. UCL. http://www.nicolascourtois.com/bitcoin/paycoin_may_2014.pdf

Crawley, J. (2022a, January 31). *FTX Reaches $32B Valuation With $400M Fundraise*. https://www.coindesk.com/business/2022/01/31/ftx-reaches-32b-valuation-with-400m-fundraise/

Crawley, J. (2022b, September 9). *Crypto Investor FTX Ventures to Take 30% Stake in SkyBridge Capital*. https://www.coindesk.com/business/2022/09/09/ftx-ventures-to-take-30-stake-in-skybridge-capital-report/

Cripps, H., Singh, A., Mejtoft, T., & Salo, J. (2020). The Use of Twitter for Innovation in Business Markets. *Marketing Intelligence & Planning*, *38*(5), 587–601. https://doi.org/10.1108/MIP-06-2019-0349

Critien, J. V., Gatt, A., & Ellul, J. (2022). Bitcoin Price Change and Trend Prediction Through Twitter Sentiment and Data Volume. *Financial Innovation*, *8*(1), Article 1. https://doi.org/10.1186/s40854-022-00352-7

Cumming, G. S., & von Cramon-Taubadel, S. (2018). Linking Economic Growth Pathways and Environmental Sustainability by Understanding Development as Alternate Social–Ecological Regimes. *Proceedings of the National Academy of Sciences of the United States of America*, *115*(38), 9533–9538. https://doi.org/10.1073/pnas.1807026115

Custers, B., Oerlemans, J. J., & Pool, R. (2020). Laundering the Profits of Ransomware; Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*, *28*(2), Article 2. https://doi.org/10.1163/15718174-02802002

Das, V. (2021, January 24). *Market Makers: Unsung Heroes of Financial Markets – Michigan Journal of Economics*. https://sites.lsa.umich.edu/mje/2021/01/24/market-makers-unsung-heroes-of-financial-markets/

David, O. (2023, October 4). Controversial FTX Founder Sam Bankman-Fried's Trial Underway: Here's How the Jurors Were Selected. *DailyCoin*. https://dailycoin.com/how-sam-bankman-frieds-jurors-were-selected/

Davies, G. (2020). Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. *The Journal of Criminal Law*, *84*(5), Article 5. https://doi.org/10.1177/0022018320952557

De Blasis, R., Galati, L., Webb, A., & Webb, R. I. (2023). Intelligent Design: Stablecoins (In)stability and Collateral During Market Turbulence. *Financial Innovation*, *9*(1), 85. https://doi.org/10.1186/s40854-023-00492-4

De Jong, O. (2022, November 15). *FTX/Alameda, What Happened?* HackerNoon. https://hackernoon.com/ftxalameda-what-happened

de Vries, A., & Stoll, C. (2021). Bitcoin's growing e-waste problem. *Resources, Conservation and Recycling*, *175*, 105901. https://doi.org/10.1016/j.resconrec.2021.105901

Dean, G., & Huileng, T. (2023, September 22). *Sam Bankman-Fried's parents are embroiled in the crypto exchange's troubles. Here's what we know about the Stanford Law professors.* Business Insider. https://www.businessinsider.com/sam-bankman-fried-sbf-who-are-his-parents-barbara-joseph-2022-12

Déchène, M., Lesperance, K., Ziernwald, L., & Holzberger, D. (2024). From Research to Retweets—Exploring the Role of Educational Twitter (X) Communities in Promoting Science Communication and Evidence-Based Teaching. *Education Sciences*, *14*(2), Article 2. https://doi.org/10.3390/educsci14020196

Del Monaco, S. (2020). Money Mules and Tumblers Money Laundering During the Cryptocurrency Era: Money Laundering During the Cryptocurrency Era. *Ricerche Giuridiche*, *2*, Article 2. https://doi.org/10.30687/Rg/2281-6100/2022/01/004

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies*. Rand Corporation.

Dixon, S. J. (2023, November 15). *X/Twitter: Number of Users Worldwide 2024*. Statista. https://www.statista.com/statistics/303681/twitter-users-worldwide/

Doherty, B. (2021, May 16). *Icon: The Untold Story Of Crypto Billionaire Sam Bankman-Fried*. Forbes. https://www.forbes.com/sites/bdoherty/2021/05/16/icon-the-untold-story-of-crypto-billionaire-sam-bankman-fried/

DOJ. (2015). *Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL*. United States Department of Justice. https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil

DOJ. (2017). *Alphabay, the Largest Online "Dark Market," Shut Down*. United States Department of Justice. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

DOJ.gov. (2023, June 27). *Criminal Division | United States v. Samuel Bankman-Fried | United States Department of Justice*. https://www.justice.gov/criminal/criminal-fraud/case/united-states-v-samuel-bankman-fried

dos Reis, E. F., Teytelboym, A., ElBahrawy, A., De Loizaga, I., & Baronchelli, A. (2024). Identifying Key Players in Dark Web Marketplaces Through Bitcoin Transaction Networks. *Scientific Reports*, *14*(1), Article 1. https://doi.org/10.1038/s41598-023-50409-5

Draper, L. (2022). Protecting Children in the Age of End-to-End Encryption. *Joint PIJIP/TLS Research Paper Series*. https://digitalcommons.wcl.american.edu/research/80

Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The Current State of Cryptocurrency Forensics. *Forensic Science International: Digital Investigation*, *46*, 301576. https://doi.org/10.1016/j.fsidi.2023.301576

Dupont, B., & Holt, T. (2022). The Human Factor of Cybercrime. *Social Science Computer Review*, *40*(4), Article 4. https://doi.org/10.1177/08944393211011584

Dupuis, D., & Gleason, K. (2020). Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic. *Journal of Financial Crime*, *28*(1), Article 1. https://doi.org/10.1108/JFC-06-2020-0113

Durrant, S. (2018). *Understanding the Nexus Between Cryptocurrencies and Transnational Crime Operations*. City University of New York. https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1070&context=jj_etds

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*, *4*(5), Article 5. https://doi.org/10.30525/2256-0742/2018-4-5-75-81

Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an Instrument of Terrorist Financing. *Baltic Journal of Economic Studies*, *7*(5), Article 5. https://doi.org/10.30525/2256-0742/2021-7-5-67-72

Dyson, S., Buchanan, W., & Bell, L. (2018). The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime. *The Journal of the British Blockchain Association*, *1*(2), Article 2. https://doi.org/10.31585/jbba-1-2-(8)2018

Eckl, Y. (2022, July 26). The downfall of Three Arrows Capital (3AC): What went wrong? *CryptoSlate*. https://cryptoslate.com/the-downfall-of-three-arrows-capital-3ac-what-went-wrong/

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective Dynamics of Dark Web Marketplaces. *Scientific Reports*, *10*(1), Article 1. https://doi.org/10.1038/s41598-020-74416-y

Elliptic. (2023a). *The $477 Million FTX Hack: A New Blockchain Trail*. https://www.elliptic.co/blog/the-477-million-ftx-hack-following-the-blockchain-trail

Elliptic. (2023b). *Three Individuals Implicated in the $477 Million FTX Heist?* https://www.elliptic.co/blog/three-individuals-implicated-in-the-477-million-ftx-heist

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *Sage Open*, *4*(1), 2158244014522633. https://doi.org/10.1177/2158244014522633

Etto, F. (2017). *Know Your Coins: Public vs. Private Cryptocurrencies*. Distributed Bitcoin. https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22

Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Europol. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol Spotlight - Cryptocurrencies - Tracing the evolution of criminal finances.pdf

Faber, J., & Fonseca, L. M. (2014). How Sample Size Influences Research Outcomes. *Dental Press Journal of Orthodontics*, *19*(4), 27–29. https://doi.org/10.1590/2176-9451.19.4.027-029.ebo

Fang, X., & Zhan, J. (2015). Sentiment Analysis Using Product Review Data. *Journal of Big Data*, *2*(1), 5. https://doi.org/10.1186/s40537-015-0015-2

Fatouros, G., Soldatos, J., Kouroumali, K., Makridis, G., & Kyriazis, D. (2023). Transforming Sentiment Analysis in the Financial Domain with ChatGPT. *Machine Learning with Applications*, *14*, 100508. https://doi.org/10.1016/j.mlwa.2023.100508

FBI. (2022). *2021 Internet Crime Report*. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Feiner, L. (2022, April 25). *Twitter Accepts Elon Musk's Buyout Deal*. CNBC. https://www.cnbc.com/2022/04/25/twitter-accepts-elon-musks-buyout-deal.html

FinCen. (2024). *Financial Crimes Enforcement Network*. United States Department of the Treasury Financial Crimes Enforcement Network. https://www.fincen.gov/

Finklea, K. (2017). *Dark Web*. Congressional Research Service. Congressional Research Service

Florea, I. O., & Nitu, M. (2020). Money Laundering Through Cryptocurrencies. *Romanian Economic Journal*, *22*(76), Article 76.

Fosso Wamba, S., Kala Kamdjoug, J. R., Epie Bawack, R., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech: A Systematic Review and Case Studies in the Supply Chain. *Production Planning & Control*, *31*(2–3), Article 2–3. https://doi.org/10.1080/09537287.2019.1631460

Frankenfield, J. (2023, May 30). *What Was Mt. Gox? Definition, History, Collapse, and Future*. Investopedia. https://www.investopedia.com/terms/m/mt-gox.asp

FTX Trading (2021, August 10). *FTX and Kevin O'Leary Announce Long-Term Investment and Spokesperson Relationship*. https://www.prnewswire.com/news-releases/ftx-and-kevin-oleary-announce-long-term-investment-and-spokesperson-relationship-301352189.html

Gamerman et al., E. (2007, December 28). *How the Schools Stack Up*. https://www.wsj.com/public/resources/documents/info-COLLEGE0711-sort.html

Garrido-Merchan, E. C., Gozalo-Brizuela, R., & Gonzalez-Carvajal, S. (2023). Comparing BERT Against Traditional Machine Learning Models in Text Classification. *Journal of Computational and Cognitive Engineering*, *2*(4), Article 4. https://doi.org/10.47852/bonviewJCCE3202838

Ge Huang, V. (2023, October 28). *Bankman-Fried Breaks Down Alameda's Relationship with FTX*. WSJ. https://www.wsj.com/livecoverage/sam-bankman-fried-trial-testimony/card/bankman-fried-breaks-down-alameda-s-relationship-with-ftx-lnazzyhT22rQtUilPTvd

George, K. (2023, September 1). *Robinhood Bought Back $606M of Stock Previously Owned by FTX's Sam Bankman-Fried*. Investopedia. https://www.investopedia.com/robinhood-bought-back-usd606m-of-stock-previously-owned-by-sam-bankman-fried-7964870

Gercke, M. (2009). *Understanding Cybercrime: A Guide for Developing Countries*. International Telecommunication Union (ITU), Telecommunication Development Centre. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

German Federal Office of Justice. (2021). *German Criminal Code (Strafgesetzbuch–StGB)*. German Federal Office of Justice. https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

Ghalwesh, A., Ouf, S., & Sayed, A. (2020). A Proposed System for Securing Cryptocurrency Via the Integration of Internet of Things with Blockchain. *International Journal of Economics and Financial Issues*, *10*(3), Article 3.

Godlove, N. (2014). Regulatory Overview of Virtual Currency. *Oklahoma Journal of Law & Technology*, *10*(1), Article 1.

Godoy, J. (2023, October 19). *US SEC Drops Claims Against Two Ripple Labs Executives*. Reuters. https://www.reuters.com/markets/us/sec-dropping-claims-against-ripple-executives-court-filing-2023-10-19/

Gohwong, S. G. (2019). *The State of the Art of Cryptography-Based Cyber-Attacks* (No. 3546334; Issue 3546334). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.3546334

Goldbarsht, D. (2024). Adapting Confiscation and Anti-Money Laundering Laws to the Digital Economy: Exploring the Australian Interplay Between Proceeds and Technology. *Journal of Money Laundering Control*, *27*(3), 472–488. https://doi.org/10.1108/JMLC-09-2023-0142

Goldstein, M., Vogel, K. P., & Yaffe-Bellany, D. (2022, December 17). Restaurateur, Political Donor, Tipster: The Many Roles of FTX's Ryan Salame. *The New York Times*. https://www.nytimes.com/2022/12/17/business/ftx-ryan-salame.html

Gómez-Hernández, J. A., & García-Teodoro, P. (2024). Lightweight Crypto-Ransomware Detection in Android Based on Reactive Honeyfile Monitoring. *Sensors*, *24*(9), Article 9. https://doi.org/10.3390/s24092679

Goodell, G., & Aste, T. (2019). Can Cryptocurrencies Preserve Privacy and Comply With Regulations? *Frontiers in Blockchain*, *2*, 1–14. https://doi.org/10.3389/fbloc.2019.00004

Goundar, S., Chand, R., Tafsil, F., Mala, R., & Nath, R. (2019). Comparison of Three Different Darknet Cryptocurrencies in e-Commerce in Our Digital Era. In *Blockchain Technologies, Applications and Cryptocurrencies* (pp. 215–229). World Scientific. https://doi.org/10.1142/9789811205279_0010

Goundar, S., Singh, A., Saini, S., Tafsil, F., Shabnam, S., & Prakash, K. (2019). An Overview of Cryptocurrencies for Online Payments of Enterprise Systems. In *Blockchain Technologies, Applications and Cryptocurrencies* (pp. 249–266). World Scientific. https://doi.org/10.1142/9789811205279_0012

Goundar, S., Tabunakawai, N., Tamata, J., Deb, A., & Nusair, S. (2019). Cryptocurrencies—An Assessment of Global Adoption Trends. In *Blockchain Technologies, Applications and Cryptocurrencies* (pp. 231–248). World Scientific. https://doi.org/10.1142/9789811205279_0011

GovTrack, U. (2016). *Tax Filing Simplification Act of 2016 (2016—S. 2789)*. GovTrack.Us. https://www.govtrack.us/congress/bills/114/s2789

Grasselli, M. R., & Lipton, A. (2021). *Cryptocurrencies and the Future of Money* (No. arXiv:2109.10177; Issue arXiv:2109.10177). arXiv. https://doi.org/10.48550/arXiv.2109.10177

Gray, I. W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2023). *Money Over Morals: A Business Analysis of Conti Ransomware* (No. arXiv:2304.11681; Issue arXiv:2304.11681). arXiv. http://arxiv.org/abs/2304.11681

Greenberg, A. (2023). New Clues Suggest Stolen FTX Funds Went to Russia-Linked Money Launderers. *Wired*. https://www.wired.com/story/ftx-hack-400-million-crypto-laundering/

Grobys, K., Junttila, J., Kolari, J. W., & Sapkota, N. (2021). On the Stability of Stablecoins. *Journal of Empirical Finance*, *64*, 207–223. https://doi.org/10.1016/j.jempfin.2021.09.002

Gryszczyńska, A. (2021). The Impact of the COVID-19 Pandemic on Cybercrime. *Bulletin of the Polish Academy of Sciences: Technical Sciences*, *69*(4), Article 4. https://doi.org/10.24425/bpasts.2021.137933

Gupta, A., Maynard, S. B., & Ahmad, A. (2021). *The Dark Web Phenomenon: A Review and Research Agenda* (No. arXiv:2104.07138; Issue arXiv:2104.07138). arXiv. https://doi.org/10.48550/arXiv.2104.07138

Hafner, M., Pereira, M. H., Dietl, H., & Beccuti, J. (2024). The Four Types of Stablecoins: A Comparative Analysis. *Ledger*, *9*. https://doi.org/10.5195/ledger.2024.326

Hale, E. (2023, October 2). *What is FTX founder Sam Bankman-Fried's trial about?* Al Jazeera. https://www.aljazeera.com/economy/2023/10/2/what-is-ftx-founder-sam-bankman-frieds-trial-about

Haqshanas, R. (2022, November 15). *Defunct Billion-Dollar Crypto Hedge Fund Three Arrows Capital Speaks Out, Blames Collapse on FTX*. Cryptonews. https://cryptonews.com/news/defunct-billion-dollar-crypto-hedge-fund-three-arrows-capital-speaks-out-blames-collapse-on-ftx.htm

Harryarsana, I. G. K. B. (2022). A Comparison of Regulation of Bitcoin as Crypto (Digital) Currency. *UNTAG Law Review*, *6*(2), Article 2. https://doi.org/10.56444/ulrev.v6i2.3452

Hart, B. (2022, November 16). *All the Ways the FTX Implosion Is Shaking the Sports World*. Intelligencer. https://nymag.com/intelligencer/2022/11/sam-bankman-frieds-ftx-implosion-shakes-the-sports-world.html

Hatta, M. (2020). Deep Web, Dark Web, Dark Net. *Annals of Business Administrative Science*, *19*(6), 277–292. https://doi.org/10.7880/abas.0200908a

Helms, K. (2023, December 22). *SEC Chair Gary Gensler Issues Crypto Warnings as Anticipation of Spot Bitcoin ETF Approval Soars*. Bitcoin.com.

https://news.bitcoin.com/sec-chair-gary-gensler-issues-crypto-warnings-as-anticipation-of-spot-bitcoin-etf-approval-soars/

Helwig, N. E., Hong, S., & Hsiao-wecksler, E. T. (2022). *Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies*. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf

Hendrickson, J. R., & Luther, W. J. (2022). Cash, Crime, and Cryptocurrencies. *The Quarterly Review of Economics and Finance*, *85*, 200–207. https://doi.org/10.1016/j.qref.2021.01.004

Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An Economic Analysis of Ransomware and Its Welfare Consequences. *Royal Society Open Science*, *7*(3), Article 3. https://doi.org/10.1098/rsos.190023

Hetler, A. (2023, November 6). *FTX Scam Explained: Everything You Need to Know*. Tech Target. https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know

Higbee, A. (2018). The Role of Crypto-Currency in Cybercrime. *Computer Fraud & Security*, *2018*(7), Article 7. https://doi.org/10.1016/S1361-3723(18)30064-2

Holt, T. J., Lee, J. R., & Griffith, E. (2023). An Assessment of Cryptomixing Services in Online Illicit Markets. *Journal of Contemporary Criminal Justice*, *39*(2), 222–238. https://doi.org/10.1177/10439862231158004

ICE. (2020). *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 "Real Rape" and Child Pornography Videos, Funded by Cryptocurrency*. United States Department of Homeland Security, United States Immigration and Customs Enforcement. https://www.ice.gov/news/releases/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child

Ilijevski, I., Ilik, G., & Babanoski, K. (2023). Cryptocurrency Abuse for the Purposes of Money Laundering and Terrorism Financing: Policies and Practical Aspects in the European Union and North Macedonia. *European Scientific Journal ESJ*, *3*. https://doi.org/10.19044/esipreprint.3.2023.p23

Influence Watch. (2023). *Mind the Gap*. InfluenceWatch. https://www.influencewatch.org/political-party/mind-the-gap/

Interpol. (2020). *Online African Organized Crime from Surface to Dark Web*. European Commission. https://south.euneighbours.eu/publication/interpol-report-online-african-organized-crime-surface-darkweb/

IQ wiki. (2022, July 19). *FTX - Exchanges*. IQ.Wiki. https://iq.wiki/wiki/ftx

Irwin, A., & Slay, J. (2010). Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. *International Cyber Resilience Conference*, *8*, 41–51.

Ivaniuk, V., & Banakh, S. (2020). Cryptocurrency-Related Cybercrimes in Ukraine. *Osteuropa Recht*, *66*(1), Article 1. https://doi.org/10.5771/0030-6444-2020-1-217

Jha, P. (2023, January 2). *Sam Bankman-Fried's Alameda Research troubles predate FTX: Report*. Cointelegraph. https://cointelegraph.com/news/sam-bankman-fried-s-alameda-research-troubles-predate-ftx-report

Johari, R. J., Zul, N. B., Talib, N., & Hussin, S. A. H. S. (2019). Money Laundering: Customer Due Diligence in the Era of Cryptocurrencies. *Proceedings of the 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019)*. 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019), Cirebon, Indonesia. https://doi.org/10.2991/aebmr.k.200305.033

John, A., Shen, S., Wilson, T., & Wilson, T. (2021, September 24). China's top regulators ban crypto trading and mining, sending bitcoin tumbling. *Reuters*. https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

Jung, B., Choi, K.-S., & Lee, C. (2022). Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(2), Article 2. https://doi.org/10.52306/2578-3289.1135

Jung, K. (2022). Freedom to Morph? An Analysis of Morphed Imagery, Child Pornography, and the First Amendment. *Catholic University Journal of Law and Technology*, *30*(2), 33–64.

Kabra, S., & Gori, S. (2023). Drug Trafficking on Cryptomarkets and the Role of Organized Crime Groups. *Journal of Economic Criminology*, *2*, 100026. https://doi.org/10.1016/j.jeconc.2023.100026

Kamps, J., & Kleinberg, B. (2018). To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps. *Crime Science*, *7*(1), Article 1. https://doi.org/10.1186/s40163-018-0093-5

Katsafados, A. G., Nikoloutsopoulos, S., & Leledakis, G. N. (2023). Twitter Sentiment and Stock Market: A COVID-19 Analysis. *Journal of Economic Studies*, *50*(8), 1866–1888. https://doi.org/10.1108/JES-09-2022-0486

Kaushik, K., Bhardwaj, A., Kumar, M., Gupta, S. K., & Gupta, A. (2022). A Novel Machine Learning-Based Framework for Detecting Fake Instagram Profiles. *Concurrency and Computation: Practice and Experience*, *34*(28), e7349. https://doi.org/10.1002/cpe.7349

Kavitha, M., & Golden, J. (2024). Smarter and Resilient Smart Contracts Applications for Smart Cities Environment Using Blockchain Technology. *Automatika*, *65*(2), 572–583. https://doi.org/10.1080/00051144.2024.2307228

Kayani, U., & Hasan, F. (2024). Unveiling Cryptocurrency Impact on Financial Markets and Traditional Banking Systems: Lessons for Sustainable Blockchain and Interdisciplinary Collaborations. *Journal of Risk and Financial Management*, *17*(2), Article 2. https://doi.org/10.3390/jrfm17020058

Keane, K. (2020). Does Bitcoin Use Affect Crime Rates? *The Corinthian*, *20*(1). https://kb.gcsu.edu/thecorinthian/vol20/iss1/2

Kemp, P. (2023, November 2). *Satoshi Nakamoto Created Bitcoin in 2009. He Mysteriously Vanished in 2011, with Billions to His Name*. Canadian Broadcasting Corporation. https://www.cbc.ca/documentaries/the-passionate-eye/satoshi-nakamoto-created-bitcoin-in-2009-he-mysteriously-vanished-in-2011-with-billions-to-his-name-1.7014958

Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks*, *11*(3), Article 3. https://doi.org/10.3390/risks11030051

Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, *30*(3), Article 3. https://doi.org/10.1177/1057567719827051

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, *43*(2), Article 2. https://doi.org/10.1007/s12103-017-9394-6

Kfir, I. (2020). Cryptocurrencies, National Security, Crime and Terrorism. *Comparative Strategy*, *39*(2), Article 2. https://doi.org/10.1080/01495933.2020.1718983

Kharde, V., & Sonawane, S. S. (2016). Sentiment Analysis of Twitter Data: A Survey of Techniques. *International Journal of Computer Applications*, *139*(11), Article 11. https://doi.org/10.5120/ijca2016908625

Kien, L. T., & Binh, N. H. (2021). Crime in Era of Digital Technology: What Can Change with Cryptocurrency Status Clarification for Development of Information Environment of

Vietnam? *Webology*, *18*(Special Issue), Article Special Issue. https://doi.org/10.14704/WEB/V18SI04/WEB18141

Kiernan, P. (2022, November 21). *Sam Bankman-Fried was No. 2 top donor to Democrats, only behind Soros*. Mint. https://www.livemint.com/market/cryptocurrency/sam-bankman-fried-ftx-team-among-top-political-donors-before-bankruptcy-11669031663161.html

Kim, H., Jang, S. M., Kim, S.-H., & Wan, A. (2018). Evaluating Sampling Methods for Content Analysis of Twitter Data. *Social Media + Society*, *4*(2), 2056305118772836. https://doi.org/10.1177/2056305118772836

Knauth, D. (2023, January 31). FTX sues Voyager Digital to claw back $446 million in 2022 loan payments. *Reuters*. https://www.reuters.com/legal/ftx-sues-voyager-digital-claw-back-446-million-2022-loan-payments-2023-01-31/

Knight, O. (2022, June 17). *FTX Agrees to Acquire Canadian Trading Platform Bitvo as It Eyes Regional Expansion*. https://www.coindesk.com/business/2022/06/17/ftx-agrees-to-acquire-canadian-trading-platform-bitvo-as-it-eyes-regional-expansion/

Kolhatkar, S. (2023, September 25). Inside Sam Bankman-Fried's Family Bubble. *The New Yorker*. https://www.newyorker.com/magazine/2023/10/02/inside-sam-bankman-frieds-family-bubble

Kovach, S. (2021, February 8). *Tesla buys $1.5 billion in bitcoin, plans to accept it as payment*. CNBC. https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html

Kristoufek, L. (2015). What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. *PLoS ONE*, *10*(4), Article 4. https://doi.org/10.1371/journal.pone.0123923

Kutera, M. (2022). Cryptocurrencies as a Subject of Financial Fraud. *Journal of Entrepreneurship, Management and Innovation*, *18*(4), Article 4. https://doi.org/10.7341/20221842

Lacson, W., & Jones, B. (2016). The 21st Century Dark Net Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology*, *10*(1), Article 1. https://doi.org/10.5281/zenodo.58521

Lang, H., & Mccrank, J. (2022, December 22). Who were the key figures at Sam Bankman-Fried's FTX? *Reuters*. https://www.reuters.com/business/who-were-key-figures-sam-bankman-frieds-ftx-2022-12-22/

Lapuh Bele, J. (2021). Cryptocurrencies as Facilitators of Cybercrime. *SHS Web of Conferences*, *111*, 01005. https://doi.org/10.1051/shsconf/202111101005

Lawson, A. (2023, March 26). Caught in the FTX storm: How a crypto high-flyer fell to Earth. *The Observer*. https://www.theguardian.com/technology/2023/mar/26/caught-in-the-ftx-storm-how-a-crypto-high-flyer-fell-to-earth

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An Assessment of the State of Firearm Sales on the Dark Web. *Journal of Crime and Justice*, *44*, 1–15. https://doi.org/10.1080/0735648X.2022.2058062

Lee, L. (2019). Cybercrime Has Evolved: It's Time Cyber Security Did Too. *Computer Fraud and Security*, *2019*(6), Article 6. https://doi.org/10.1016/S1361-3723(19)30063-6

Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., & Shin, S. (2019). Cybercriminal Minds: An Investigative Study of Cryptocurrency Abuses in the Dark Web. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23055

Legge, M. (2022, February 25). *Crypto bull market strategies*. Koinly: Calculate Your Bitcoin and Crypto Taxes. https://koinly.io/blog/bull-market-strategies/

Legge, M. (2023, July 31). *Crypto Taxes India: Ultimate Guide 2023.* Koinly Blog. https://koinly.io/guides/crypto-tax-india/

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency. *Journal of Financial Crime*, *30*(4), 1036–1054. https://doi.org/10.1108/JFC-07-2022-0161

Li, N., Qi, M., Xu, Z., Zhu, X., Zhou, W., Wen, S., & Xiang, Y. (2024). Blockchain Cross-Chain Bridge Security: Challenges, Solutions, and Future Outlook. *Distrib. Ledger Technol.*, 1–35. https://doi.org/10.1145/3696429

Liao, K., Zhao, Z., Doupe, A., & Ahn, G.-J. (2016). Behind Closed Doors: Measurement and Analysis of Cryptolocker Ransoms in Bitcoin. *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 1–13. https://doi.org/10.1109/ECRIME.2016.7487938

LilMoonLambo. (2019, October 11). Interview with Edward Moncada, Founder and CEO, Blockfolio. *Medium*. https://medium.com/@liluzivertcoin/interview-with-edward-moncada-founder-and-ceo-blockfolio-6c0d787b7cdb

Lin, D., Wu, J., Fu, Q., Yu, Y., Lin, K., Zheng, Z., & Yang, S. (2023). *Towards Understanding Crypto Money Laundering in Web3 Through the Lenses of Ethereum Heists* (No. arXiv:2305.14748; Issue arXiv:2305.14748). arXiv. http://arxiv.org/abs/2305.14748

Lindqwister, L., & Tong, A. (2022, December 23). *Inside Sam Bankman-Fried's Parents' Beautiful Historic Home, It Even Has a Pool*. The San Francisco Standard.

https://sfstandard.com/2022/12/22/inside-sam-bankman-frieds-parents-beautiful-historic-home/

Lipton, A. (2021). Cryptocurrencies Change Everything. *Quantitative Finance*, *21*(8), Article 8. https://doi.org/10.1080/14697688.2021.1944490

Luong, H. T. (2023). Foundations and Trends in the Darknet-Related Criminals in the Last 10 Years: A Systematic Literature Review and Bibliometric Analysis. *Security Journal*. https://doi.org/10.1057/s41284-023-00383-4

Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology*, *62*(6), Article 6. https://doi.org/10.1093/BJC/AZAB118

Manjula, B., Shilpa, B., & Sundaresh, M. (2022). Analysis of Cryptocurrency, Bitcoin and the Future. *East Asian Journal of Multidisciplinary Research*, *1*(7), Article 7. https://doi.org/10.55927/eajmr.v1i7.803

Masciandaro, D., Barone, R., & Masciandaro, D. (2019). Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques. *European Journal of Law and Economics*, *47*(December), Article December. https://doi.org/10.2139/ssrn.3303871

Mataković, I. C. (2022). Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review. *International E-Journal of Criminal Sciences Artículo*, *5*(2022), Article 2022.

Matarese, V. (2013). Using strategic, critical reading of research papers to teach scientific writing: The reading–research–writing continuum. In *Supporting Research Writing* (pp. 73–89). Elsevier. https://doi.org/10.1016/B978-1-84334-666-1.50005-9

Maxwell, F. (2022). Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age: Moving from Criminalisation to Prevention. *The International Journal of Children's Rights*, *31*(1), 61–88. https://doi.org/10.1163/15718182-30040004

Mayyasi, A., & Smith, S. V. (2017, March 22). Episode 760: Tax Hero. *NPR*. https://www.npr.org/sections/money/2017/03/22/521132960/episode-760-tax-hero

Mazambani, L. (2024). *Determinants of Public Trust in Digital Money: The Case of Central Bank Digital Currency* (No. 4708114). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4708114

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service Economy Within the Darknet. *Computers & Security*, *92*, 101762. https://doi.org/10.1016/j.cose.2020.101762

Mendoza-Urdiales, R. A., Núñez-Mora, J. A., Santillán-Salgado, R. J., & Valencia-Herrera, H. (2022). Twitter Sentiment Analysis and Influence on Stock Performance Using Transfer Entropy and EGARCH Methods. *Entropy*, *24*(7), 874. https://doi.org/10.3390/e24070874

Mirea, M., Wang, V., & Jung, J. (2019). The Not so Dark Side of the Darknet: A Qualitative Study. *Security Journal*, *32*(2), Article 2. https://doi.org/10.1057/s41284-018-0150-5

Moffett, T. (2023). CFTC & SEC: The Wild West of Cryptocurrency Regulation. *University of Richmond Law Review*, *57*(2), Article 2.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), Article 1. https://doi.org/10.1080/00396338.2016.1142085

Morelato, M., Bozic, S. M., Rhumorbarbe, D., Broséus, J., Staehli, L., Esseiva, P., Roux, C., & Rossy, Q. (2020). An Insight into Prescription Drugs and Medicine on the Alphabay Cryptomarket. *Journal of Drug Issues*, *50*(1), Article 1. https://doi.org/10.1177/0022042619872955

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), Article 3. https://doi.org/10.1515/popets-2018-0025

Mthembu, N., Sanusi, K. A., & Eita, J. H. (2022). Do Stock Market Volatility and Cybercrime Affect Cryptocurrency Returns? Evidence from South African Economy. *Journal of Risk and Financial Management*, *15*(12), Article 12. https://doi.org/10.3390/jrfm15120589

Mubarak, D., & Manjunath, H. (2021). A Study on Cryptocurrency in India. *International Journal of Research and Analytical Reviews*, *8*(1), Article 1.

Munawa, F. (2023). *Bitcoin Use Cases Are Seeing Explosive Growth, Trust Machines Says*. CoinDesk. https://www.coindesk.com/tech/2023/04/28/bitcoin-use-cases-are-seeing-explosive-growth-trust-machines-says/

Muslim, A. K., Mohd Dzulkifli, D. Z., Nadhim, M. H., & Abdellah, R. H. (2019). A Study of Ransomware Attacks: Evolution and Prevention. *Journal of Social Transformation and Regional Development*, *1*(1), Article 1. https://doi.org/10.30880/jstard.2019.01.01.003

Naheem, M. A. (2021). Do Cryptocurrencies Enable and Facilitate Modern Slavery? *Journal of Money Laundering Control*, *24*(3), Article 3. https://doi.org/10.1108/JMLC-07-2020-0073

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography*, *1*, 1–9.

Naqvi, S. (2018). Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1–5. https://doi.org/10.1145/3230833.3233290

Navani, S., & Cirella, G. T. (2024). Cybercrimes in the Cryptocurrency Domain: Identifying Types, Understanding Motives and Techniques, and Exploring Future Directions for Technology and Regulation. *Journal of Geography, Politics and Society*, *14*(2), 43. https://doi.org/10.26881/jpgs.2024.2.01

Navazan, H. (2022, July 20). *FATF Update on Emerging Risks; Cross-Chain; DeFi & Unhosted Wallets*. Crystal Blockchain Analytics for Crypto Compliance. https://crystalblockchain.com/articles/targeted-fatf-update-on-emerging-risks-cross-chain-defi-unhosted-wallets/

Nayak, B. K. (2010). Understanding the Relevance of Sample Size Calculation. *Indian Journal of Ophthalmology*, *58*(6), 469–470. https://doi.org/10.4103/0301-4738.71673

Nazzari, M. (2023). From Payday to Payoff: Exploring the Money Laundering Strategies of Cybercriminals. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09505-1

Nazzari, M., & Riccardi, M. (2024). Cleaning Mafia Cash: An Empirical Analysis of the Money Laundering Behaviour of 2800 Italian Criminals. *European Journal of Criminology*, 14773708231224981. https://doi.org/10.1177/14773708231224981

Newbery, E. (2021, June 1). *BlockFi Review 2024: What Went Wrong and Alternatives to Consider | The Motley Fool*. https://www.fool.com/the-ascent/cryptocurrency/blockfi-review/

Nganga, M. (2023, October 14). *ICO vs. IPO: Key Differences explained*. CoinGape. https://coingape.com/education/ico-vs-ipo/

Nialldawson. (2015, April 17). *Silkroad 3.0, a "Darknet" Blackmarket Website*. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Silkroad30.png

Nishant, N., Lang, H., Nishant, N., & Lang, H. (2023, April 25). Binance.US calls off $1.3 billion deal for Voyager's assets. *Reuters*. https://www.reuters.com/markets/deals/binanceus-calls-off-13-bln-deal-voyagers-assets-2023-04-25/

Nole. (2022, November 11). *Mercedes suspends FTX sponsor deal; removes logos from F1 cars*. https://www.motorsport.com/f1/news/mercedes-suspends-ftx-sponsor-deal-removes-logos-from-f1-cars/10398017/

Nouwen, yvonne. (2017). Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues. *ECPAT International Journal*, *12*, Article 12.

Nurhadiyanto, L. (2020). The Identification of Money Laundering on Drug Trafficking. *Asia Pacific Fraud Journal*, *5*(1), Article 1. https://doi.org/10.21532/apfjournal.v5i1.137

Olbrecht, A., & Pieters, G. (2023). Crypto-Currencies and Crypto-Assets: An Introduction. *Eastern Economic Journal*, *49*(2), Article 2. https://doi.org/10.1057/s41302-023-00246-1

Oldemburgo, V. de M., Cheung, F., & Inzlicht, M. (2024). Twitter (X) Use Predicts Substantial Changes in Well-Being, Polarization, Sense of Belonging, and Outrage. *Communications Psychology*, *2*(1), Article 1. https://doi.org/10.1038/s44271-024-00062-z

Omeljaniuk, J. (2020). Cryptocurrencies as a Generic Object of Crime in Polish Criminal Law. *Annual Center Review*, *12–13*, Article 12–13. https://doi.org/10.15290/acr.2019-2020.12-13.05

opensecrets.org. (2023, March 31). *Super PACs*. OpenSecrets. https://www.opensecrets.org/PACS/superpacs.php?cycle=

Osman, M. B., Urom, C., Guesmi, K., & Benkraiem, R. (2024). Economic Sentiment and the Cryptocurrency Market in the Post-Covid-19 Era. *International Review of Financial Analysis*, *91*, 102962. https://doi.org/10.1016/j.irfa.2023.102962

Otabek, S., & Choi, J. (2024). Multi-Level Deep Q-Networks for Bitcoin Trading Strategies. *Scientific Reports*, *14*(1), Article 1. https://doi.org/10.1038/s41598-024-51408-w

Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., & Han, W. (2022). An Overview on Cross-Chain: Mechanism, Platforms, Challenges and Advances. *Computer Networks*, *218*, 109378. https://doi.org/10.1016/j.comnet.2022.109378

Özer, M., Vukovic, D., Frömmel, M., & Kamişli, M. (2024). *Does Bitcoin Shocks Truly Cointegrate with Financial and Commodity Markets?* (No. 4735090). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4735090

Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, *6*(2), 117–133. https://doi.org/10.1007/s42786-022-00044-x

Ozturk, L., & Sulungur, E. (2021). The Regulation Problem of Cryptocurrencies. *M3 Publishing*, *5*(2021), Article 2021. https://www.doi.org/10.5038/9781955833035

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware Payments in the Bitcoin Ecosystem. *Journal of Cybersecurity*, *5*(1), Article 1. https://doi.org/10.1093/cybsec/tyz003

Parnell, W. (2023, March 30). *Bankman-Fried pleads not guilty to five new charges*. Politico. https://www.politico.com/news/2023/03/30/bankman-fried-pleads-not-guilty-to-five-new-charges-00089702

Patel, P. C., & Richter, J. (2020). The Relationship Between Terrorist Attacks and Cryptocurrency Returns. *Applied Economics*, *53*(8), Article 8. https://doi.org/10.1080/00036846.2020.1819952

Patsakis, C., Politou, E., Alepis, E., & Hernandez-Castro, J. (2023). Cashing Out Crypto: State of Practice in Ransom Payments. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00766-z

Perkins, N. (2021). *Cryptocurrency: The Economics of Money and Selected Policy Issues*. Congressional Research Service.

Pernice, I. G. A., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, *10*(2), Article 2. https://doi.org/10.14763/2021.2.1561

Peshkar, P. (2023, January 25). BlockFi's Financials Show $1.2B FTX Exposure. *CryptoTicker*. https://cryptoticker.io/en/blockfi-financials-ftx-exposure/

Peters, K. (2023, November 22). *Binance Exchange*. Investopedia. https://www.investopedia.com/terms/b/binance-exchange.asp

Pham, H., Nguyen Thanh, B., Ramiah, V., & Moosa, N. (2022). The Effects of Hacking Events on Bitcoin. *Journal of Public Affairs*, *22*(S1), e2744. https://doi.org/10.1002/pa.2744

Phugger, B. (2021, October 4). *China's Central Bank Declares All Cryptocurrency Transactions Illegal*. Blockchain: Baker Mckenzie. https://blockchain.bakermckenzie.com/2021/10/04/chinas-central-bank-declares-all-cryptocurrency-transactions-illegal/

Piazza, F. (2017). Bitcoin in the Dark Web: A Shadow Over Banking Secrecy and a Call for Global Response. *Southern California Interdisciplinary Law Journal*, *26*(3), Article 3.

Pieroni, C. (2018). La Crypto Nostra: How Organized Crime Thrives in the Era of Cryptocurrency. *Technology*, *20*(5), Article 5.

Pilinkiene, V., Dumciuviene, D., Schenk-Hoppé, K. R., Ilbiz, E., & Kaunert, C. (2022). Sharing Economy for Tackling Crypto-Laundering: The Europol Associated Global Conference on Criminal Finances and Cryptocurrencies. *Sustainability*, *14*(11), Article 11. https://doi.org/10.3390/su14116618

Poleo, G. R. (2023, November 2). *How Caroline Ellison became celebrated Alameda CEO*. Mail Online. https://www.dailymail.co.uk/news/article-12698571/How-Caroline-Ellison-celebrated-Alameda-CEO-exposed-fraudster-testifying-against-ex-boyfriend-Sam-Bankman-Fried.html

Pongratz, N. (2021, April 9). *Sam Bankman Fried Explains His Arbitrage Techniques*. Yahoo Finance. https://finance.yahoo.com/news/sam-bankman-fried-explains-arbitrage-132901181.html

Pop, C., & Colonescu, I.-E. (2021). Cryptocurrencies' Puzzle. *Studia Universitatis Babeş-Bolyai Negotia*, *66*(2), Article 2. https://doi.org/10.24193/subbnegotia.2021.2.06

Prentice, R. (2023, November 2). *Crypto Ethics: FTX and Sam Bankman-Fried*. Ethics Unwrapped. https://ethicsunwrapped.utexas.edu/crypto-ethics-ftx-and-sam-bankman-fried

Press Release (from Justice.gov) (2022, December 13). *Southern District of New York, United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried | United States Department of Justice*. https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried

Priyambudi, & Sinaga, H. D. P. (2021). Prosecutorial Discretion in Tackling the Cryptocurrency Crime in Indonesia. *Webology*, *Volume 18*(No. 2), Article No. 2. https://doi.org/10.14704/WEB/V18I2/WEB18308

Pushkarev, V. V., Artemova, V. V., Ermakov, S. V., Alimamedov, E. N., & Popenkov, A. V. (2020). Criminal Prosecution of Persons, Who Committed Criminal, Acts Using the Cryptocurrency in the Russian Federation. *Revista San Gregorio*, *1*(42), e1566. https://doi.org/10.36097/rsan.v1i42.1566

Qi, Y., & Shabrina, Z. (2023). Sentiment Analysis Using Twitter Data: A Comparative Application of Lexicon- and Machine-Learning-Based Approach. *Social Network Analysis and Mining*, *13*(1), Article 1. https://doi.org/10.1007/s13278-023-01030-x

Quarmby, B. (2022, December 9). *Kevin O'Leary lost the $15M he was paid to be FTX's spokesperson*. Cointelegraph. https://cointelegraph.com/news/kevin-o-leary-lost-the-15m-he-was-paid-to-be-ftx-s-spokesperson

Quoine. (2019). *Liquid.com Announces First Close of Ongoing Series C Funding, Hits Tech Unicorn Status*. PR Newswire. https://www.prnewswire.com/in/news-releases/liquid-com-announces-first-close-of-ongoing-series-c-funding-hits-tech-unicorn-status-896775587.html

Rajagopal, K. (2020, March 4). Supreme Court Sets Aside RBI Ban on Cryptocurrency Transactions. *The Hindu*. https://www.thehindu.com/news/national/supreme-court-sets-aside-rbi-ban-on-cryptocurrency-transactions/article61967124.ece

Raman, R., Kumar Nair, V., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Dark Web Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals. *Heliyon*, *9*(11), e22269. https://doi.org/10.1016/j.heliyon.2023.e22269

Recskó, M., & Aranyossy, M. (2024). User Acceptance of Social Network-Backed Cryptocurrency: A Unified Theory of Acceptance and Use of Technology (Utaut)-Based Analysis. *Financial Innovation*, *10*(1), 57. https://doi.org/10.1186/s40854-023-00511-4

Reddy, E. (2020). Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill. *Statute Law Review*, *41*(2), Article 2. https://doi.org/10.1093/slr/hmz001

Reddy, E., & Minaar, A. (2018). Cryptocurrency: A Tool and Target for Cybercrime. *Acta Criminologica: Southern African Journal of Criminology*, *31*(3), Article 3.

Reddy, E., Minaar, A., Omeljaniuk, J., Rueckert, C., Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A., Sheikh Abdullah, S. N. H., Moore, D., Rid, T., Teichmann, F. M. J., Falker, M. C., Pilinkiene, V., Dumciuviene, D., Schenk-Hoppé, K. R., Ilbiz, E., Kaunert, C., Zimba, A., Wang, Z., … Sindre, G. (2020). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *Journal of Cybersecurity*, *10*(2), Article 2. https://doi.org/10.57019/jmv.1108783

Reiff, N., Mansa, J., & Velasquez, V. (2023). *Howey Test Definition: What It Means and Implications for Cryptocurrency*. Investopedia. https://www.investopedia.com/terms/h/howey-test.asp

Renear, A. H., & Palmer, C. L. (2009). Strategic Reading, Ontologies, and the Future of Scientific Publishing. *Science*, *325*(5942), 828–832. https://doi.org/10.1126/science.1157784

RenProject. (2022, March 28). *Darknodes*. https://docs.renproject.io/darknodes/

Reuters. (2023, July 7). *Report: QB Brady lost $30M in collapse of FTX*. ESPN.Com. https://www.espn.co.uk/nfl/story/_/id/37974774/report-tom-brady-lost-30m-collapse-crypto-giant-ftx

Reynolds, P., & Irwin, A. S. M. (2017). Tracking Digital Footprints: Anonymity Within the Bitcoin System. *Journal of Money Laundering Control*, *20*(2), Article 2. https://doi.org/10.1108/JMLC-07-2016-0027

Riahi, R., Bennajma, A., Jahmane, A., & Hammami, H. (2024). Investing in Cryptocurrency Before and During the COVID-19 Crisis: Hedge, Diversifier or Safe Haven? *Research in International Business and Finance*, *67*, 102102. https://doi.org/10.1016/j.ribaf.2023.102102

Rieckmann, J., & Stuchtey, T. (2023). *Dark Crypto: The Use of Cryptocurrency for Illegal Purposes*. Friedrich Naumann Foundation For Freedom.

Rizzo, P. (2017, January 9). *Indonesia's AML Watchdog Links Bitcoin to Islamic State*. CoinDesk. https://www.coindesk.com/markets/2017/01/09/indonesias-aml-watchdog-links-bitcoin-to-islamic-state/

Robertson, A. (2022, August 10). *Hackers and fraudsters used crypto bridge RenBridge to launder $540 million, says report*. The Verge. https://www.theverge.com/2022/8/10/23299841/crypto-bridge-renbridge-used-launder-money-russia-north-korea-ransomware-report

Robins-Early, N. (2022, November 22). *FTX's Bahamas unit paid co-CEO's MAGA Republican congressional candidate girlfriend $400,000*. Insider. https://www.insider.com/ftx-bahamas-michelle-bond-ryan-salame-bankman-fried-girlfriend-400000-2022-11

Rooney, K. (2020, March 13). *Bitcoin loses half of its value in two-day plunge*. CNBC. https://www.cnbc.com/2020/03/13/bitcoin-loses-half-of-its-value-in-two-day-plunge.html

Rosenberg, E. (2023, November 6). *Who Is Sam Bankman-Fried?* Investopedia. https://www.investopedia.com/who-is-sam-bankman-fried-6830274

Rubasundram, G. A. (2019). The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity. *International Journal of Recent Technology and Engineering*, *7*(5), Article 5.

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box* (No. 2676615; Issue 2676615). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.2676615

Rueckert, C. (2019). Cryptocurrencies and Fundamental Rights. *Journal of Cybersecurity*, *5*(1), Article 1. https://doi.org/10.1093/cybsec/tyz004

Saiedi, E., Broström, A., & Ruiz, F. (2021). Global Drivers of Cryptocurrency Infrastructure Adoption. *Small Business Economics*, *57*(1), Article 1. https://doi.org/10.1007/s11187-019-00309-8

Sanusi, K. A., & Dickason-Koekemoer, Z. (2022). Cryptocurrency Returns, Cybercrime and Stock Market Volatility: GAS and Regime Switching Approaches. *International*

Journal of Economics and Financial Issues, *12*(6), Article 6. https://doi.org/10.32479/IJEFI.13555

Sanz-Bas, D., del Rosal, C., Náñez Alonso, S. L., & Echarte Fernández, M. Á. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws*, *10*(3), Article 3. https://doi.org/10.3390/laws10030057

Sayid, M. R. N. (2023). The Fusion of Blockchain, Pornography and Human Trafficking in a Global Digital Dragnet That Forms the Online Child Sex Trafficking. *Russian Law Journal*, *11*(5s), Article 5s. https://doi.org/10.52783/rlj.v11i5s.891

Schaffer, J. (Director). (2022, February 13). *FTX Super Bowl Don't miss out with Larry David*. Video recording.

Șcheau, M. C., Crăciunescu, S. L., Brici, I., & Achim, M. V. (2020). A Cryptocurrency Spectrum Short Analysis. *Journal of Risk and Financial Management*, *13*(8), Article 8. https://doi.org/10.3390/jrfm13080184

Schickler, J. (2023, January 9). *FTX Opposition to $1B Binance Deal Is "Hypocrisy and Chutzpah," Voyager Says*. https://www.coindesk.com/policy/2023/01/09/ftx-opposition-to-1b-binance-deal-is-hypocrisy-and-chutzpah-voyager-says/

Schneider, N. (2019). Decentralization: An Incomplete Ambition. *Journal of Cultural Economy*, *12*(4), 265–285. https://doi.org/10.1080/17530350.2019.1589553

Schwartz, B. (2022, December 6). *Former FTX engineer quietly became multimillion-dollar Democratic donor after new role at cryptocurrency exchange*. CNBC. https://www.cnbc.com/2022/12/06/former-ftx-engineer-quietly-became-millionaire-democratic-donor.html

Schwartz, B., & Mangan, D. (2023, February 23). *FTX founder Sam Bankman-Fried hit with four new criminal charges*. CNBC. https://www.cnbc.com/2023/02/23/ftx-founder-sam-bankman-fried-hit-with-new-criminal-charges.html

Scorechain. (2022, November 22). *Scorechain investigates the FTX hack*. Scorechain Blog. https://blog.scorechain.com/scorechain-investigates-the-ftx-hack/

Sebele-Mpofu, F. Y. (2020). Saturation Controversy in Qualitative Research: Complexities and Underlying Assumptions. A Literature Review. *Cogent Social Sciences*. https://www.tandfonline.com/doi/abs/10.1080/23311886.2020.1838706

Sherer, J. A., McLellan, M. L., Fedeles, E. R., & Sterling, N. L. (2016). Ransomware: Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web Annual Survey. *Richmond Journal of Law & Technology*, *23*(3), Article 3.

Sherman, N., & Tidy, J. (2022, November 11). Crypto giant FTX collapses into bankruptcy. *BBC News*. https://www.bbc.com/news/business-63601213

Shinder, L. D., & Cross, M. (2008). *Scene of the Cybercrime* (L. Shinder & M. B. T.-S. of the C. (Second E. Cross, Eds.). Syngress. https://doi.org/10.1016/B978-1-59749-276-8.00018-2

Shome, A. (2023, April 26). *FTX Sells LedgerX for $50 Million*. Financial and Business News | Finance Magnates. https://www.financemagnates.com/cryptocurrency/ftx-sells-ledgerx-for-50-million/

Sicignano, G. J. (2021). Money Laundering using Cryptocurrency: The Case of Bitcoin! *Athens Journal of Law*, *7*(2), Article 2. https://doi.org/10.30958/ajl.7-2-7

Sidhpurwala, H. (2023). *A Brief History of Cryptography*. Red Hat. https://www.redhat.com/en/blog/brief-history-cryptography

Sigalos, M. (2022a, July 11). *From $10 billion to zero: How a crypto hedge fund collapsed and dragged many investors down with it*. CNBC. https://www.cnbc.com/2022/07/11/how-the-fall-of-three-arrows-or-3ac-dragged-down-crypto-investors.html

Sigalos, M. (2022b, November 15). *From $32 billion to criminal investigations: How Sam Bankman-Fried's crypto empire vanished overnight*. CNBC. https://www.cnbc.com/2022/11/15/how-sam-bankman-frieds-ftx-alameda-empire-vanished-overnight.html

Sigalos, M., & Goswami, R. (2022, December 12). *FTX founder Sam Bankman-Fried arrested in the Bahamas after U.S. files criminal charges*. CNBC. https://www.cnbc.com/2022/12/12/ftx-founder-sam-bankman-fried-arrested-in-the-bahamas-after-us-files-criminal-charges.html

Sigler, K. (2018). Crypto-Jacking: How Cyber-Criminals Are Exploiting the Crypto-Currency Boom. *Computer Fraud and Security*, *2018*(9), Article 9. https://doi.org/10.1016/S1361-3723(18)30086-1

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes*. Rand Corporation. https://doi.org/10.7249/RR4418

Singh, S., & Nambiar, V. (2024). Role of Artificial Intelligence in the Prevention of Online Child Sexual Abuse: A Systematic Review of Literature. *Journal of Applied Security Research*, *0*(0), 1–42. https://doi.org/10.1080/19361610.2024.2331885

Soni, N. (2024). Letter to the Editor: "Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework." *Egyptian Journal of Forensic Sciences*, *14*(1), 22. https://doi.org/10.1186/s41935-024-00396-z

Sovbetov, Y. (2018). *Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero* (No. 3125347; Issue 3125347). SSRN Scholarly Paper. https://papers.ssrn.com/abstract=3125347

Stroukal, D., & Nedvědová, B. (2016). Bitcoin and Other Cryptocurrency as an Instrument of Crime in Cyberspace. *Proceedings of 4th Business & Management Conference*. 4th Business & Management Conference, Istanbul. https://doi.org/10.20472/BMC.2016.004.018

Suslenko, V., Zatonatska, T., Dluhopolskyi, O., & Kuznyetsova, A. (2022). Use of Cryptocurrencies Bitcoin and Ethereum in the Field of E-Commerce: Case Study of Ukraine. *Financial and Credit Activity Problems of Theory and Practice*, *1*(42), Article 42. https://doi.org/10.55643/fcaptp.1.42.2022.3603

Swiss Federal Council. (2015, January 14). *Federal Council Approves the 2014 Foreign Policy Report*. Swiss Federal Council. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-55885.html

Syme, P. (2023, October 4). *In his first job, Sam Bankman-Fried designed a system that called Trump's 2016 win before major news outlets—But the firm still lost $300 million on election night*. Yahoo Finance. https://finance.yahoo.com/news/first-job-sam-bankman-fried-103217906.html

Tabachnik, C. (2023, August 11). *FTX founder Sam Bankman-Fried jailed by federal judge for alleged witness tampering—CBS News*. https://www.cbsnews.com/news/sam-bankman-fried-ftx-jail-federal-judge-witness-tampering/

Talaat, A. S. (2023). Sentiment Analysis Classification System Using Hybrid BERT Models. *Journal of Big Data*, *10*(1), Article 1. https://doi.org/10.1186/s40537-023-00781-w

Tan, B. (2024). *Central Bank Digital Currency Adoption: A Two-Sided Model* (No. 4734056). SSRN Scholarly Paper. https://doi.org/10.5089/9798400268113.001

Tan, K. L., Lee, C. P., & Lim, K. M. (2023). A Survey of Sentiment Analysis: Approaches, Datasets, and Future Research. *Applied Sciences*, *13*(7), Article 7. https://doi.org/10.3390/app13074550

Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A., & Sheikh Abdullah, S. N. H. (2021). Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets.

3rd International Cyber Resilience Conference, 1–5. https://doi.org/10.1109/CRC50527.2021.9392446

Team, C. (2024, January 18). 2024 Crypto Crime Trends from Chainalysis. *Chainalysis*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

Teichmann, F., & Falker, M.-C. (2020a). Cryptocurrencies and Financial Crime: Solutions from Liechtenstein. *Journal of Money Laundering Control*, *24*(4), Article 4. https://doi.org/10.1108/JMLC-05-2020-0060

Teichmann, F., & Falker, M.-C. (2020b). Money Laundering Through Cryptocurrencies. In E. G. Popkova & B. S. Sergi (Eds.), *Artificial Intelligence: Anthropogenic Nature vs. Social Origin* (pp. 500–511). Springer International Publishing. https://doi.org/10.1007/978-3-030-39319-9_57

Teichmann, F., & Falker, M.-C. (2024). Terrorist Financing Via the Banking Sector. *Crime, Law and Social Change*. https://doi.org/10.1007/s10611-023-10133-7

Thamizhisai, M. D., Bharathi, S., Bhuvaneshwaran, U., Immanuvel, S. M., & Patchaiyappan, M. (2024). Enhancing Forensic Investigations Leveraging Blockchain and Smart Contracts for Security and Transparency. *International Journal of Scientific Research in Science and Technology*, *11*(3), Article 3.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and Future Financial Crime. *Crime Science*, *11*(1), 1. https://doi.org/10.1186/s40163-021-00163-8

Turchin, A., Masharsky, S., & Zitnik, M. (2023). Comparison of BERT implementations for natural language processing of narrative medical documents. *Informatics in Medicine Unlocked*, *36*, 101139. https://doi.org/10.1016/j.imu.2022.101139

Turchyn, N., & Turchyn, A. (2021). Legal Regulation of Cryptocurrency in Ukraine. *Economics, Finance, Law*, *5*(1), Article 1. https://doi.org/10.37634/efp.2021.5(1).6

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science*, *2*(November), Article November. https://doi.org/10.3389/fcomp.2020.600596

UNODC. (2020). *Darknet Cybercrime Threats to Southeast Asia*. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/southeastasiaandpacific//Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

UNODC. (2023). *World Drug Report 2023*. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/data-and-analysis/world-drug-report-2023.html

van Nguyen, T., Truong, T. V., & Lai, C. K. (2022). Legal Challenges to Combating Cybercrime: An Approach from Vietnam. *Crime, Law and Social Change*, *77*(3), Article 3. https://doi.org/10.1007/S10611-021-09986-7/TABLES/3

van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin Money Laundering: Mixed Results?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin. *Journal of Financial Crime*, *25*(2), Article 2. https://doi.org/10.1108/JFC-11-2016-0067

Varanasi et al., L. (2023, October 9). *Caroline Ellison is a math whiz, trader, and shadow figure behind FTX's collapse. She's testifying this week in the criminal trial of her ex-colleague and boyfriend, Sam Bankman-Fried.* Business Insider. https://www.businessinsider.com/who-is-caroline-ellison-the-mind-behind-ftx-collapse

Verduyn, M. C. (2018). *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Routledge. https://library.oapen.org/bitstream/handle/20.500.12657/29557/1000376.pdf?sequence=1&isAllowed=y

Virga, J. M. (2015). International Criminals and Their Virtual Currencies: The Need for an International Effort in Regulating Virtual Currencies and Combating Cyber Crime. *Revista de Direito Internacional*, *12*(2), Article 2. https://doi.org/10.5102/rdi.v12i2.3557

Volevodz, A. (2024). *About the State and Some Trends of Cryptocurrency-Related Crime* (No. 4693186). SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4693186

Wang, N. (2022, November 10). *FTX Assets Frozen by Bahamian Regulator*. https://www.coindesk.com/business/2022/11/10/ftx-digital-markets-assets-frozen-by-bahamian-regulator-bloomberg/

Wang, S., & Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing: A Journal of Policy and Practice*, *15*(4), Article 4. https://doi.org/10.1093/police/paab059

Wang, T. (2022, August 22). *FTX Could Buy BlockFi for Only $15M – or a Lot More If Crypto Lender Hits Big Goals*. https://www.coindesk.com/business/2022/08/22/ftx-could-buy-blockfi-for-only-15m-or-a-lot-more-if-crypto-lender-hits-big-goals/

Wang, Y., Guo, J., Yuan, C., & Li, B. (2022). Sentiment Analysis of Twitter Data. *Applied Sciences*, *12*(22), Article 22. https://doi.org/10.3390/app122211775

Watters, C. (2023). When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws*, *12*(2), Article 2. https://doi.org/10.3390/laws12020033

Weiss, B. (2023, October 13). *Inside the meeting where Caroline Ellison came clean to Alameda staff, per a secret recording from an employee who started 3 days earlier*. Fortune Crypto. https://fortune.com/crypto/2023/10/12/caroline-ellison-alameda-all-hands-meeting-yolo-sam-bankman-fried-sbf-ftx/

Wen, L., Bao, L., Chen, J., Grundy, J., Xia, X., & Yang, X. (2024). Market Manipulation of Cryptocurrencies: Evidence from Social Media and Transaction Data. *ACM Transactions on Internet Technology*. https://doi.org/10.1145/3643812

Whitworth, E. (2023, October 24). Sam Bankman-Fried at Jane Street: Success—but Not Enough. *Shortform Books*. https://www.shortform.com/blog/sam-bankman-fried-jane-street/

Wiblin, R., & Harris, K. (2018, June 22). *How the audacity to fix things without asking permission can change the world*. 80,000 Hours. https://80000hours.org/podcast/episodes/tara-mac-aulay-operations-mindset/

Widhiyanti, H. N., Hussein, S. M., & Ganindha, R. (2023). Indonesian Cryptocurrencies Legislative Readiness: Lessons from the United States. *Sriwijaya Law Review*, *7*(1), Article 1. https://doi.org/10.28946/slrev.Vol7.Iss1.2138.pp150-172

Williams, D. (2023, November 2). *Southern District of New York | Statement Of U.S. Attorney Damian Williams On The Conviction Of Samuel Bankman-Fried | United States Department of Justice*. https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-conviction-samuel-bankman-fried

Wronka, C. (2022a). "Cyber-Laundering": The Change of Money Laundering in the Digital Age. *Journal of Money Laundering Control*, *25*(2), Article 2. http://dx.doi.org/10.1108/JMLC-04-2021-0035

Wronka, C. (2022b). Money Laundering Through Cryptocurrencies: Analysis of the Phenomenon and Appropriate Prevention Measures. *Journal of Money Laundering Control*, *25*(1), Article 1. http://dx.doi.org/10.1108/JMLC-02-2021-0017

Xie, R. (2019). Why China Had to Ban Cryptocurrency but the US Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the US and China. In *Wash. U. Global Stud. L. Rev.* (Vol. 18). Washington University Global Studies Law Review.

Yaffe-Bellany, D., & DelMundo, J. N. (2023, October 10). The Places That Sam Bankman-Fried Left Behind. *The New York Times*. https://www.nytimes.com/2023/10/10/technology/sam-bankman-fried-ftx-photos.html

Yaffe-Bellany, D., & Moreno, J. E. (2023, October 12). Sam Bankman-Fried's Closest Friends Become His Foes in Courtroom Clash. *The New York Times*. https://www.nytimes.com/2023/10/12/technology/sam-bankman-fried-friends-witnesses.html

Yahoo News. (2024, April 11). *Bankman-Fried appeals FTX fraud conviction, 25-year sentence*. Yahoo News. https://www.yahoo.com/news/bankman-fried-appeals-ftx-fraud-183747767.html

Yakovenko, A. (2021, January 14). FTX Chooses Solana for Serum: A High-Speed, Non-Custodial Decentralized Derivatives Exchange. *Solana*. https://medium.com/solana-labs/ftx-chooses-solana-for-serum-a-high-speed-non-custodial-decentralized-derivatives-exchange-c346a27c1f2b

Yeşiltaş, S., Şen, A., Arslan, B., & Altuğ, S. (2022). A Twitter-Based Economic Policy Uncertainty Index: Expert Opinion and Financial Market Dynamics in an Emerging Market Economy. *Frontiers in Physics*, *10*. https://doi.org/10.3389/fphy.2022.864207

Yunandi, F., & Leksono, A. B. (2023). Criminal Sanctions Against Money Laundering Crimes in the Perspective of Economic Analysis of Law. *Rechtsnormen Journal of Law*, *1*(2), Article 2. https://doi.org/10.55849/rjl.v1i2.391

Zandt. (2023, November 23). *Infographic: What Are the Biggest Crypto Exchanges?* Statista Daily Data. https://www.statista.com/chart/28721/cryptocurrency-exchanges-with-the-highest-trading-volume-year-to-date

Zaunseder, A., & Bancroft, A. (2020). Pricing of Illicit Drugs on Darknet Markets: A Conceptual Exploration. *Drugs and Alcohol Today*, *21*(2), Article 2. https://doi.org/10.1108/DAT-12-2019-0054

Zavoli, I. (2022). *The Use of Cryptocurrencies in the UK Real Estate Market: An Assessment of Money Laundering Risks* (No. 4033765). SSRN Scholarly Paper. https://papers.ssrn.com/abstract=4033765

Zhang, M., Zhang, X., Zhang, Y., & Lin, Z. (2024). Security of Cross-chain Bridges: Attack Surfaces, Defenses, and Open Problems. *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, 298–316. https://doi.org/10.1145/3678890.3678894

Zheng, X. (2024). Research on Blockchain Smart Contract Technology Based on Resistance to Quantum Computing Attacks. *PLOS ONE*, *19*(5), e0302325. https://doi.org/10.1371/journal.pone.0302325

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zilnieks, V., & Erins, I. (2023). Cross-Chain Bridges: A Potential Solution to Standardising Distributed Ledger Technology in Payment Systems. *Information Technology and Management Science*, *26*(1), 27–34. https://doi.org/10.7250/itms-2023-0004

Zimba, A., Wang, Z., Mulenga, M., & Odongo, N. H. (2020). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. *Journal of Computer Information Systems*, *60*(4), Article 4. https://doi.org/10.1080/08874417.2018.1477076

Zuckerman, G. (2022, November 30). Early Alameda Staffers Quit After Battling Sam Bankman-Fried Over Risk, Compliance Concerns. *Wall Street Journal*. https://www.wsj.com/articles/early-alameda-staffers-quit-after-battling-sam-bankman-fried-over-risk-compliance-concerns-11669810723

LIST OF TABLES

LIST OF FIGURES

APPENDICES

APPENDIX A

FTX POLITICAL DONATIONS IN 2021-2022 CAMPAIGN CYCLE

Recipient	Total (USD)	Recipient Type	View
Protect Our Future PAC	28,000,000	Carey	Liberal
American Dream Federal Action	15,000,000	Carey	Conservative
House Majority PAC	6,000,000	Carey	Liberal
GMI PAC	4,051,947	Outside Group	Bipartisan
Senate Leadership Fund	3,500,000	Outside Group	Conservative
Senate Majority PAC	3,000,000	Outside Group	Liberal
Congressional Leadership Fund	2,750,000	Carey	Conservative
Women Vote!	2,250,000	Outside Group	Liberal
America United (Carey)	1,300,000	Carey	Liberal
LGBTQ Victory Fund	1,100,000	Carey	Liberal
Mind the Gap	1,000,000	Outside Group	Liberal
Stand for New York Cmte	867,000	Outside Group	Conservative
National Wildlife Federation Action Fund	810,000	Outside Group	Bipartisan
Results for NC	700,000	Outside Group	Conservative
Priorities USA Action	500,000	Carey	Liberal
DNC Services Corp	365,000	Political Party	Democrat
EMILY's List Non-Federal	350,000	527	Liberal
Opportunity for Tomorrow	300,000	Outside Group	Liberal
Value in Electing Women PAC	250,000	Carey	Conservative
Democratic Congressional Campaign Cmte	250,000	Political Party	Democrat
Democratic Majority for Israel	250,000	Carey	Liberal
Alabama Conservatives Fund	205,000	Outside Group	Conservative
American Patriots PAC	150,000	Outside Group	Conservative
National Republican Congressional Cmte	134,700	Political Party	Republican
National Republican Senatorial Cmte	109,500	Political Party	Republican
Democratic Party of Maine	70,000	Political Party	Democrat
Heartland Resurgence	50,000	Outside Group	Conservative
Club for Growth Action	50,000	Outside Group	Conservative
Moving Broward Forward PAC	40,000	Outside Group	Liberal
Bond Michelle	37,300	Candidate (R-NY01)	Republican
Democratic Senatorial Campaign Cmte	36,500	Political Party	Democrat
Santos George	29,000	Candidate (R-NY03)	Republican
Stabenow Debbie	26,100	Candidate (D-MIS2)	Democrat
Democratic Party of New Hampshire	25,000	Political Party	Democrat
Republican National Cmte	25,000	Political Party	Republican
Flynn Carrick	24,755	Candidate (D-OR06)	Democrat
Hoeven John	23,200	Candidate (R-NDS1)	Republican
Boozman John	23,200	Candidate (R-ARS2)	Republican
Activate America	22,000	Outside Group	Liberal
Democratic Party of Iowa	19,756	Political Party	Democrat
Democratic Party of Oregon	17,100	Political Party	Democrat
ActBlue Non-Federal	15,800	527	Liberal
Gottheimer Josh	14,500	Candidate (D-NJ05)	Democrat
Murray Patty	14,500	Candidate (D-WAS2)	Democrat
Thompson Glenn	11,600	Candidate (R-PA15)	Republican
Emmer Tom	11,600	Candidate (R-MN06)	Republican
Democratic Party of Texas	10,000	Political Party	Democrat
Working Harder PAC	10,000	LeadPAC	Democrat
Democratic Party of Pennsylvania	10,000	Political Party	Democrat
Michigan Democratic State Central Cmte	10,000	Political Party	Democrat
Massachusetts Democratic State Cmte	10,000	Political Party	Democrat
Democratic Party of Arizona	10,000	Political Party	Democrat
Democratic Party of Nebraska	10,000	Political Party	Democrat

Democratic Party of Wisconsin	10,000	Political Party	Democrat
Georgia Federal Elections Cmte	10,000	Political Party	Democrat
Washington State Democratic Central Cmte	10,000	Political Party	Democrat
Democratic Party of Virginia	10,000	Political Party	Democrat
Democratic Executive Cmte of Florida	10,000	Political Party	Democrat
Democratic Party of Kansas	10,000	Political Party	Democrat
Democratic State Central Cmte/Maryland	10,000	Political Party	Democrat
New York State Democratic Cmte	10,000	Political Party	Democrat
Democratic Party of New Mexico	10,000	Political Party	Democrat
Democratic Party of North Carolina	10,000	Political Party	Democrat
Great Lakes PAC	10,000	LeadPAC	Democrat
Freedom Fund	10,000	LeadPAC	Republican
New York Republican Federal Campaign Cmte	10,000	Political Party	Republican
Arkansas for Leadership	10,000	LeadPAC	Republican
Heartland Values PAC	10,000	LeadPAC	Republican
New Jersey Democratic State Cmte	9,999	Political Party	Democrat
Democratic Party of Mississippi	9,756	Political Party	Democrat
Connecticut Democratic State Central Cmte	9,756	Political Party	Democrat
Democratic Party of Oklahoma	9,756	Political Party	Democrat
Minnesota Democratic Farmer Labor Party	9,756	Political Party	Democrat
West Virginia State Democratic Exec Cmte	9,756	Political Party	Democrat
Indiana Democratic Congressional Victory Cmte	9,756	Political Party	Democrat
Democratic Party of South Dakota	9,756	Political Party	Democrat
Democratic Party of Illinois	9,756	Political Party	Democrat
Democratic Party of Ohio	9,756	Political Party	Democrat
Democratic Party of Arkansas	9,756	Political Party	Democrat
Democratic Party of California	9,756	Political Party	Democrat
Utah State Democratic Cmte	9,756	Political Party	Democrat
Democratic Party of Hawaii	9,756	Political Party	Democrat
Democratic Party of the District of Columbia	9,756	Political Party	Democrat
North Dakota Democratic-Nonpartisan League Party	9,756	Political Party	Democrat
Democratic State Central Cmte/Louisiana	9,756	Political Party	Democrat
Democratic Party of Tennessee	9,756	Political Party	Democrat
Rhode Island Democratic State Cmte	9,756	Political Party	Democrat
Democratic Party of Idaho	9,756	Political Party	Democrat
Democratic Party of Alaska	9,756	Political Party	Democrat
Democratic Party of Delaware	9,756	Political Party	Democrat
Wyoming State Democratic Central Cmte	9,756	Political Party	Democrat
State Democratic Exec Cmte of Alabama	9,756	Political Party	Democrat
Democratic Party of South Carolina	9,756	Political Party	Democrat
Democratic Party of Montana	9,756	Political Party	Democrat
Missouri Democratic State Cmte	9,756	Political Party	Democrat
Democratic Party of Vermont	9,752	Political Party	Democrat
Thune John	9,200	Candidate (R-SDS1)	Republican
Padilla Alex	8,720	Candidate (D-CAS1)	Democrat
Jeffries Hakeem	8,700	Candidate (D-NY08)	Democrat
Aguilar Pete	8,700	Candidate (D-CA31)	Democrat
Manchin Joe	8,700	Candidate (D-WVS1)	Democrat
Craig Angie	8,700	Candidate (D-MN02)	Democrat
Balint Becca	8,700	Candidate (D-VT01)	Democrat
Gillibrand Kirsten	8,700	Candidate (D-NYS1)	Democrat
Hassan Maggie	8,700	Candidate (D-NHS1)	Democrat
Smith Tina	8,700	Candidate (D-MNS1)	Democrat
Ernst Joni	8,700	Candidate (R-IAS2)	Republican
Leavitt Karoline	8,700	Candidate (R-NH01)	Republican
Cassidy Bill	8,700	Candidate (R-LAS1)	Republican
Murkowski Lisa	8,700	Candidate (R-AKS2)	Republican
Romney Mitt	8,700	Candidate (R-UTS1)	Republican
Summitt PAC	7,500	LeadPAC	Democrat
Maloney Sean Patrick	6,800	Candidate (D-NY18)	Democrat
Marlinga Carl	6,800	Candidate (D-MI10)	Democrat
Auchincloss Jake	6,800	Candidate (D-MA04)	Democrat
Britt Katie Boyd	6,000	Candidate (R-ALS2)	Republican
DeLauro Rosa	5,800	Candidate (D-CT03)	Democrat

Conole Francis	5,800	Candidate (D-NY22)	Democrat
Schumer Charles E	5,800	Candidate (D-NYS2)	Democrat
Welch Peter	5,800	Candidate (D-VT01)	Democrat
Horsford Steven	5,800	Candidate (D-NV04)	Democrat
Boyle Brendan	5,800	Candidate (D-PA02)	Democrat
Carter Troy	5,800	Candidate (D-LA02)	Democrat
Gallego Ruben	5,800	Candidate (D-AZ07)	Democrat
Torres Ritchie	5,800	Candidate (D-NY15)	Democrat
Garbarino Andrew	5,800	Candidate (R-NY02)	Republican
Miller Max	5,800	Candidate (R-OH07)	Republican
Houchin Erin	5,800	Candidate (R-IN09)	Republican
Simpson Mike	5,800	Candidate (R-ID02)	Republican
Johnson Dusty	5,800	Candidate (R-SD01)	Republican
Collins Susan M	5,800	Candidate (R-MES2)	Republican
Zeldin Lee	5,800	Candidate (R-NY01)	Republican
Molinaro Marc	5,800	Candidate (R-NY19)	Republican
Sasse Ben	5,800	Candidate (R-NES2)	Republican
Masters Blake	5,800	Candidate (R-AZS1)	Republican
Shaffer Jeremy	5,800	Candidate (R-PA17)	Republican
Booker Cory	5,700	Candidate (D-NJS2)	Democrat
Prairie PAC	5,000	LeadPAC	Democrat
People's Voice PAC	5,000	LeadPAC	Democrat
AXNE PAC	5,000	LeadPAC	Democrat
Build The Bench PAC	5,000	LeadPAC	Democrat
Country Roads PAC	5,000	LeadPAC	Democrat
Purpose PAC	5,000	LeadPAC	Democrat
Valley First Leadership PAC	5,000	LeadPAC	Democrat
Jobs Education & Families First	5,000	LeadPAC	Democrat
Serving Our Country PAC	5,000	LeadPAC	Democrat
Limitless Horizons PAC	5,000	LeadPAC	Democrat
Giddy Up PAC	5,000	LeadPAC	Democrat
Velvet Hammer PAC	5,000	LeadPAC	Democrat
Shore PAC	5,000	LeadPAC	Democrat
Hawaii PAC	5,000	LeadPAC	Democrat
Granite Values	5,000	LeadPAC	Democrat
PAC to the Future	5,000	LeadPAC	Democrat
BRIDGE PAC	5,000	LeadPAC	Democrat
Off the Sidelines	5,000	LeadPAC	Democrat
New Voice PAC	5,000	LeadPAC	Democrat
OC Jobs & Education	5,000	LeadPAC	Democrat
Jersey Values PAC	5,000	LeadPAC	Democrat
JIMMY PAC	5,000	LeadPAC	Democrat
Hope PAC	5,000	LeadPAC	Democrat
M-PAC	5,000	LeadPAC	Democrat
GOLD PAC	5,000	LeadPAC	Democrat
Impact (Schumer)	5,000	LeadPAC	Democrat
Narragansett Bay PAC	5,000	LeadPAC	Democrat
Fair Shot PAC	5,000	LeadPAC	Democrat
Blue Nevada PAC	5,000	LeadPAC	Democrat
Committee for a Democratic Future	5,000	LeadPAC	Democrat
BFB PAC	5,000	LeadPAC	Democrat
Forward Together PAC	5,000	LeadPAC	Democrat
Keystone America PAC	5,000	LeadPAC	Democrat
Motor City PAC	5,000	LeadPAC	Democrat
Continuing America's Strength & Security	5,000	LeadPAC	Republican
Jobs Opportunity & New Ideas PAC	5,000	LeadPAC	Republican
Hern Kevin	5,000	Candidate (R-OK01)	Republican
Bluegrass Cmte	5,000	LeadPAC	Republican
Denali Leadership PAC	5,000	LeadPAC	Republican
Free State PAC	5,000	LeadPAC	Republican
Greater Tomorrow PAC	5,000	LeadPAC	Republican
Hawkeye PAC	5,000	LeadPAC	Republican
Reclaim America PAC	5,000	LeadPAC	Republican
Alamo PAC	5,000	LeadPAC	Republican

Majority Cmte PAC	5,000	LeadPAC	Republican
Tomorrow Is Meaningful	5,000	LeadPAC	Republican
Americans for Legislating Excellence PAC	5,000	LeadPAC	Republican
Texas Red	5,000	LeadPAC	Republican
Dakota PAC	5,000	LeadPAC	Republican
Defend Our Conservative Senate PAC	5,000	LeadPAC	Republican
Believe In America PAC	5,000	LeadPAC	Republican
Malinowski Tom	4,485	Candidate (D-NJ07)	Democrat
Republican Party of West Virginia	3,700	Political Party	Republican
Cleaver Emanuel	2,900	Candidate (D-MO05)	Democrat
Kildee Dan	2,900	Candidate (D-MI05)	Democrat
Golden Jared	2,900	Candidate (D-ME02)	Democrat
Garcia Jesus	2,900	Candidate (D-IL04)	Democrat
Luria Elaine	2,900	Candidate (D-VA02)	Democrat
Kelly Mark	2,900	Candidate (D-AZS1)	Democrat
Caraveo Yadira	2,900	Candidate (D-CO08)	Democrat
Budzinski Nikki	2,900	Candidate (D-IL13)	Democrat
Magaziner Seth	2,900	Candidate (D-RI02)	Democrat
Warner Mark	2,900	Candidate (D-VAS2)	Democrat
Baldwin Tammy	2,900	Candidate (D-WIS1)	Democrat
Pocan Mark	2,900	Candidate (D-WI02)	Democrat
Kelly Robin	2,900	Candidate (D-IL02)	Democrat
Carbajal Salud	2,900	Candidate (D-CA24)	Democrat
Correa Lou	2,900	Candidate (D-CA46)	Democrat
O'Halleran Tom	2,900	Candidate (D-AZ01)	Democrat
Pettersen Brittany	2,900	Candidate (D-CO07)	Democrat
Rose Max	2,900	Candidate (D-NY11)	Democrat
Trahan Lori	2,900	Candidate (D-MA03)	Democrat
Pappas Chris	2,900	Candidate (D-NH01)	Democrat
Hoyle Val	2,900	Candidate (D-OR04)	Democrat
Frankel Lois	2,900	Candidate (D-FL21)	Democrat
Clarke Yvette	2,900	Candidate (D-NY09)	Democrat
Tester Jon	2,900	Candidate (D-MTS1)	Democrat
Titus Dina	2,900	Candidate (D-NV01)	Democrat
Quigley Mike	2,900	Candidate (D-IL05)	Democrat
Ruiz Raul	2,900	Candidate (D-CA36)	Democrat
Beatty Joyce	2,900	Candidate (D-OH03)	Democrat
Stevens Haley	2,900	Candidate (D-MI11)	Democrat
Fletcher Lizzie	2,900	Candidate (D-TX07)	Democrat
Brown Shontel	2,900	Candidate (D-OH11)	Democrat
Kim Elizabeth	2,900	Candidate (D-NY10)	Democrat
Pallone Frank Jr	2,900	Candidate (D-NJ06)	Democrat
Matsui Doris	2,900	Candidate (D-CA06)	Democrat
Cardenas Tony	2,900	Candidate (D-CA29)	Democrat
Fetterman John	2,900	Candidate (D-PAS1)	Democrat
Wexton Jennifer	2,900	Candidate (D-VA10)	Democrat
Patel Suraj	2,900	Candidate (D-NY12)	Democrat
Garcia Robert	2,900	Candidate (D-CA42)	Democrat
Biaggi Alessandra	2,900	Candidate (D-NY17)	Democrat
Thompson Bennie G	2,900	Candidate (D-MS02)	Democrat
Pelosi Nancy	2,900	Candidate (D-CA12)	Democrat
Wyden Ron	2,900	Candidate (D-ORS2)	Democrat
Ruppersberger Dutch	2,900	Candidate (D-MD02)	Democrat
Castor Kathy	2,900	Candidate (D-FL14)	Democrat
Dingell Debbie	2,900	Candidate (D-MI12)	Democrat
Panetta Jimmy	2,900	Candidate (D-CA20)	Democrat
Kamlager Sydney	2,900	Candidate (D-CA37)	Democrat
Gillen Laura	2,900	Candidate (D-NY04)	Democrat
Carper Tom	2,900	Candidate (D-DES1)	Democrat
Ryan Tim	2,900	Candidate (D-OH13)	Democrat
Bennet Michael	2,900	Candidate (D-COS1)	Democrat
Kuster Ann	2,900	Candidate (D-NH02)	Democrat
Payne Donald M Jr	2,900	Candidate (D-NJ10)	Democrat
Masto Catherine Cortez	2,900	Candidate (D-NVS2)	Democrat

Lee Susie	2,900	Candidate (D-NV03)	Democrat
Harder Josh	2,900	Candidate (D-CA10)	Democrat
Neguse Joseph	2,900	Candidate (D-CO02)	Democrat
Spanberger Abigail	2,900	Candidate (D-VA07)	Democrat
Quartey Quaye	2,900	Candidate (D-CA27)	Democrat
McGarvey Morgan	2,900	Candidate (D-KY03)	Democrat
Villegas Gilbert	2,900	Candidate (D-IL03)	Democrat
Casar Greg	2,900	Candidate (D-TX35)	Democrat
Reed Jack	2,900	Candidate (D-RIS2)	Democrat
Bishop Sanford	2,900	Candidate (D-GA02)	Democrat
Shaheen Jeanne	2,900	Candidate (D-NHS2)	Democrat
Sinema Kyrsten	2,900	Candidate (D-AZS2)	Democrat
Coleman Bonnie Watson	2,900	Candidate (D-NJ12)	Democrat
Barragan Nanette	2,900	Candidate (D-CA44)	Democrat
Rosen Jacky	2,900	Candidate (D-NVS1)	Democrat
Axne Cindy	2,900	Candidate (D-IA03)	Democrat
Slotkin Elissa	2,900	Candidate (D-MI08)	Democrat
McBath Lucy	2,900	Candidate (D-GA06)	Democrat
Vasquez Gabe	2,900	Candidate (D-NM02)	Democrat
Foushee Valerie	2,900	Candidate (D-NC04)	Democrat
Durbin Dick	2,900	Candidate (D-ILS1)	Democrat
Eshoo Anna	2,900	Candidate (D-CA18)	Democrat
Costa Jim	2,900	Candidate (D-CA16)	Democrat
Schatz Brian	2,900	Candidate (D-HIS1)	Democrat
Peters Gary	2,900	Candidate (D-MIS1)	Democrat
Frost Maxwell	2,900	Candidate (D-FL10)	Democrat
Menendez Rob	2,900	Candidate (D-NJ08)	Democrat
Crockett Jasmine	2,900	Candidate (D-TX30)	Democrat
Jackson Jeff	2,900	Candidate (D-NC14)	Democrat
Grassley Chuck	2,900	Candidate (R-IAS1)	Republican
Scalise Steve	2,900	Candidate (R-LA01)	Republican
Bilirakis Gus	2,900	Candidate (R-FL12)	Republican
Miller-Meeks Mariannette	2,900	Candidate (R-IA02)	Republican
Rubio Marco	2,900	Candidate (R-FLS2)	Republican
Fleischmann Chuck	2,900	Candidate (R-TN03)	Republican
Griffith Morgan	2,900	Candidate (R-VA09)	Republican
Hudson Richard	2,900	Candidate (R-NC08)	Republican
Dunn Neal	2,900	Candidate (R-FL02)	Republican
Lesko Debbie	2,900	Candidate (R-AZ08)	Republican
Letlow Julia	2,900	Candidate (R-LA05)	Republican
Oz Mehmet	2,900	Candidate (R-PAS1)	Republican
Abraham Lincoln PAC	2,900	LeadPAC	Republican
MVL PAC	2,900	LeadPAC	Republican
Moran Jerry	2,900	Candidate (R-KSS2)	Republican
Carter John	2,900	Candidate (R-TX31)	Republican
Burgess Michael	2,900	Candidate (R-TX26)	Republican
McCaul Michael	2,900	Candidate (R-TX10)	Republican
Scott Tim	2,900	Candidate (R-SCS1)	Republican
Carter Buddy	2,900	Candidate (R-GA01)	Republican
Reschenthaler Guy	2,900	Candidate (R-PA14)	Republican
Green Jennifer-Ruth	2,900	Candidate (R-IN01)	Republican
McConnell Mitch	2,900	Candidate (R-KYS1)	Republican
Cornyn John	2,900	Candidate (R-TXS1)	Republican
Rodgers Cathy McMorris	2,900	Candidate (R-WA05)	Republican
Walberg Tim	2,900	Candidate (R-MI07)	Republican
Bucshon Larry	2,900	Candidate (R-IN08)	Republican
Stefanik Elise	2,900	Candidate (R-NY21)	Republican
Fitzpatrick Brian	2,900	Candidate (R-PA01)	Republican
Budd Ted	2,900	Candidate (R-NC13)	Republican
Rutherford John	2,900	Candidate (R-FL04)	Republican
Pence Greg	2,900	Candidate (R-IN06)	Republican
Burr Richard	2,900	Candidate (R-NCS2)	Republican
Aderholt Robert B	2,900	Candidate (R-AL04)	Republican
Schweikert David	2,900	Candidate (R-AZ06)	Republican

Harris Andy	2,900	Candidate (R-MD01)	Republican
Paul Rand	2,900	Candidate (R-KYS2)	Republican
Van Drew Jeff	2,900	Candidate (R-NJ02)	Republican
Armstrong Kelly	2,900	Candidate (R-ND01)	Republican
Joyce John	2,900	Candidate (R-PA13)	Republican
Bishop Dan	2,900	Candidate (R-NC09)	Republican
Hinson Ashley	2,900	Candidate (R-IA01)	Republican
Gonzales Tony	2,900	Candidate (R-TX23)	Republican
Lawler Mike	2,900	Candidate (R-NY17)	Republican
Rogers Hal	2,900	Candidate (R-KY05)	Republican
Calvert Ken	2,900	Candidate (R-CA42)	Republican
Cole Tom	2,900	Candidate (R-OK04)	Republican
McCarthy Kevin	2,900	Candidate (R-CA23)	Republican
Crawford Rick	2,900	Candidate (R-AR01)	Republican
Womack Steve	2,900	Candidate (R-AR03)	Republican
Johnson Ron	2,900	Candidate (R-WIS2)	Republican
Stewart Chris	2,900	Candidate (R-UT02)	Republican
Joyce David P	2,900	Candidate (R-OH14)	Republican
Moolenaar John	2,900	Candidate (R-MI04)	Republican
Higgins Clay	2,900	Candidate (R-LA03)	Republican
Curtis John	2,900	Candidate (R-UT03)	Republican
Crenshaw Dan	2,900	Candidate (R-TX02)	Republican
Guest Michael	2,900	Candidate (R-MS03)	Republican
Garcia Mike	2,900	Candidate (R-CA25)	Republican
Crane Eli	2,900	Candidate (R-AZ02)	Republican
Walker Herschel	2,900	Candidate (R-GAS2)	Republican
Alford Mark	2,900	Candidate (R-MO04)	Republican
Duncan Jeff	2,900	Candidate (R-SC03)	Republican
Johnson Bill	2,900	Candidate (R-OH06)	Republican
Wenstrup Brad	2,900	Candidate (R-OH02)	Republican
Mooney Alex	2,900	Candidate (R-WV02)	Republican
Marshall Roger	2,900	Candidate (R-KSS1)	Republican
Laturner Jake	2,900	Candidate (R-KS02)	Republican
Vance J D	2,900	Candidate (R-OHS2)	Republican
Cornicelli Robert	2,900	Candidate (R-NY02)	Republican
Laxalt Adam	2,900	Candidate (R-NVS2)	Republican
Finstad Brad	2,900	Candidate (R-MN01)	Republican
Latta Bob	2,900	Candidate (R-OH05)	Republican
Turner Michael R	2,900	Candidate (R-OH10)	Republican
Guthrie Brett	2,900	Candidate (R-KY02)	Republican
Palazzo Steven	2,900	Candidate (R-MS04)	Republican
Cline Ben	2,900	Candidate (R-VA06)	Republican
Gimenez Carlos	2,900	Candidate (R-FL26)	Republican
Clyde Andrew	2,900	Candidate (R-GA09)	Republican
Harshbarger Diana	2,900	Candidate (R-TN01)	Republican
Edwards Chuck	2,900	Candidate (R-NC11)	Republican
Barrasso John	2,900	Candidate (R-WYS1)	Republican
Granger Kay	2,900	Candidate (R-TX12)	Republican
Diaz-Balart Mario	2,900	Candidate (R-FL25)	Republican
Palmer Gary	2,900	Candidate (R-AL06)	Republican
Newhouse Dan	2,900	Candidate (R-WA04)	Republican
Cammack Kat	2,900	Candidate (R-FL03)	Republican
Jackson Ronny	2,900	Candidate (R-TX13)	Republican
Schmitt Eric	2,900	Candidate (R-MOS1)	Republican
Himes Jim	2,800	Candidate (D-CT04)	Democrat
Schrier Kim	2,500	Candidate (D-WA08)	Democrat
DR RAUL PAC	2,500	LeadPAC	Democrat
Treasure State PAC	2,500	LeadPAC	Democrat
Luchadora PAC	2,500	LeadPAC	Democrat
Leading People Forward PAC	2,500	LeadPAC	Democrat
AnniePAC	2,500	LeadPAC	Democrat
LOIS PAC	2,500	LeadPAC	Democrat
Visionary PAC	2,500	LeadPAC	Democrat
One Voice	2,500	LeadPAC	Democrat

Wolverine PAC	2,500	LeadPAC	Democrat
Victory by Investing Building & Empowering PAC	2,500	LeadPAC	Democrat
SAC PAC	2,500	LeadPAC	Democrat
Athena PAC	2,500	LeadPAC	Democrat
Blue Majority PAC	2,500	LeadPAC	Democrat
Getting Stuff Done PAC	2,500	LeadPAC	Democrat
Because Women Can	2,500	LeadPAC	Democrat
Spike PAC	2,500	LeadPAC	Democrat
Montana Red	2,500	LeadPAC	Republican
Lank PAC	2,500	LeadPAC	Republican
Nevada Democratic Victory	2,100	Political Party	Democrat
Help Elect Republicans Now	2,100	LeadPAC	Republican
Sherrill Mikie	1,585	Candidate (D-NJ11)	Democrat
Flood Mike	1,500	Candidate (R-NE01)	Republican
Khanna Ro	1,000	Candidate (D-CA17)	Democrat
Garcia Cassy	1,000	Candidate (R-TX28)	Republican
Chavez-Deremer Lori	1,000	Candidate (R-OR05)	Republican
De La Cruz Monica	1,000	Candidate (R-TX15)	Republican
Scheller Lisa	1,000	Candidate (R-PA07)	Republican
Kiggans Jen	1,000	Candidate (R-VA02)	Republican
Salazar Maria	1,000	Candidate (R-FL27)	Republican
Total	75,389,555		

Source: https://www.opensecrets.org/orgs/ftx-us/

APPENDIX B

FEDERAL CRIMINAL TRIAL, Case S5 22 Cr. 673 (LAK)

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK

United States vs Sam Bank-Friedman

Case Number: S5 22 Cr. 673 (LAK)

Plaintiff: UNITED STATES OF AMERICA

Defendant: SAMUEL BANKMAN-FRIED

Filing Date: December 9, 2022

December 13, 2022
United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried
https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried

December 22, 2022
United States Attorney Announces Extradition Of FTX Founder Samuel Bankman-Fried To The United States And Guilty Pleas Of Former CEO Of Alameda Research And Former Chief Technology Officer Of FTX
https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-extradition-ftx-founder-samuel-bankman-fried-united

March 6, 2024
United States v. Samuel Bankman-Fried, a/k/a "SBF," 22 Cr. 673 (LAK)
https://www.justice.gov/usao-sdny/united-states-v-samuel-bankman-fried-aka-sbf-22-cr-673-lak

March 28, 2024
Samuel Bankman-Fried Sentenced To 25 Years In Prison
https://www.justice.gov/usao-sdny/pr/samuel-bankman-fried-sentenced-25-years-prison

November 2, 2023
Statement Of U.S. Attorney Damian Williams On The Conviction Of Samuel Bankman-Fried
https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-conviction-samuel-bankman-fried

PRESS RELEASE

Statement Of U.S. Attorney Damian Williams On The Conviction Of Samuel Bankman-Fried

Thursday, November 2, 2023

Share

For Immediate Release

U.S. Attorney's Office, Southern District of New York

> ***"Sam Bankman-Fried perpetrated one of the biggest financial frauds in American history – a multibillion-dollar scheme designed to make him the King of Crypto – but while the cryptocurrency industry might be new and the players like Sam Bankman-Fried might be new, this kind of corruption is as old as time. This case has always been about lying, cheating, and stealing, and we have no patience for it.***
>
> ***When I became U.S. Attorney, I promised we would be relentless in rooting out corruption in our financial markets. This is what relentless looks like. This case moved at lightning speed – that was not a coincidence, that was a choice. This case is also a warning to every fraudster who thinks they're untouchable, that their crimes are too complex for us to catch, that they are too powerful to prosecute, or that they are clever enough to talk their way out of it if caught. Those folks should think again, and cut it out. And if they don't, I promise we'll have enough handcuffs for all of them.***
>
> ***This verdict would not have been possible without the amazing work by the career prosecutors from my Office and the FBI agents who have given their all for this case. We have pushed them hard, and they have delivered every step of the way. They are the best of the best, and I am grateful for them.***
>
> ***This case has received a tremendous amount of attention, and I understand why that is, but the women and men of the Southern District of New York consistently deliver outstanding public service on behalf of the American people – without fear or favor and often without any public recognition. They do it because they believe in the rule of law, because they love this country, and because they are patriots. I am proud to serve with them."***

* * *

Bankman-Fried, 31, of Stanford, California, was convicted of two counts of wire fraud conspiracy, two counts of wire fraud, and one count of conspiracy to commit money laundering, each of which carries a maximum sentence of 20 years in prison. He was also convicted of conspiracy to commit commodities fraud and conspiracy to commit securities fraud, each of which carries a maximum sentence of five years in prison.

The statutory maximum sentences are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendant will be determined by a judge.

Contact
Nicholas Biase
(212) 637-2600

Updated November 2, 2023

SEC COMPLAINT, Case 1:22-cv-10501

Filed: December 13, 2022
UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK
SECURITIES AND EXCHANGE COMMISSION (Plaintiff) v. SAMUEL BANKMAN-FRIED (Defendant).

Civil Action No. 22-cv-10501 (28 pages)
https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-219.pdf

CFTC COMPLAINT, Case 1:22-cv-10503

Filed: December 13, 2022
UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK
COMMODITY FUTURES TRADING COMMISSION (Plaintiff) v. SAMUEL BANKMAN-FRIED, FTX TRADING LTD D/B/A FTX.COM, AND ALAMEDA RESEARCH LLC (Defendants).

Complaint for injunctive and other equitable relief and for civil monetary penalties under the commodity exchange act and commission regulations

Complaint (40 pages)
https://www.cftc.gov/media/7986/enfftxtradingcomplaint121322/download

Press Release Number 8638-22
https://www.cftc.gov/PressRoom/PressReleases/8638-22

SEC COMPLANT, Case 1:22-cv-10794

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK
SECURITIES AND EXCHANGE COMMISSION (Plaintiff) v. CAROLINE ELLISON and ZIXIAO “GARY” WANG (Defendants).

Civil Action No. 22-cv-10794 (38 pages)
https://www.sec.gov/files/litigation/complaints/2023/comp25617.pdf

APPENDIX C

PYTHON SCRIPT FOR EVALUATION

The sentiment analysis utilized the BERT model, specifically the "nlptown/bert-base-multilingual-uncased-sentiment" version. BERT, a state-of-the-art transformer-based model, is renowned for its effectiveness across various NLP tasks, including sentiment analysis. The selected model was pre-trained on a large corpus of multilingual text data and fine-tuned for sentiment classification tasks. Performance metrics included accuracy, precision, recall, and F1 score. Evaluation of the model on the test set ensured that the performance metrics accurately reflected its ability to generalize to new, unseen data.

```
Accuracy:  \( \frac{\text{Number of correct predictions}}{\text{Total number of predictions}} \)
Precision: \( \frac{\text{True Positives}}{\text{True Positives + False Positives}} \)
Recall:    \( \frac{\text{True Positives}}{\text{True Positives + False Negatives}} \)
F1 score:  \( 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision + Recall}} \)

# Python Script for Evaluation
# To provide transparency, here is an example of the Python code used to calculate the performance metrics

```python
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score
import numpy as np

# Assuming y_true are the true labels and y_pred are the predicted labels from the model

# Example labels (1 for positive, 0 for neutral, -1 for negative)
y_true = np.array([1, 0, -1, 1, 0, -1, 1, 1, 0, -1])
y_pred = np.array([1, 0, -1, 0, 0, -1, 1, 1, 1, -1])

# Calculating the metrics
accuracy = accuracy_score(y_true, y_pred)
precision = precision_score(y_true, y_pred, average='macro')
recall = recall_score(y_true, y_pred, average='macro')
f1 = f1_score(y_true, y_pred, average='macro')

print(f'Accuracy: {accuracy:.2f}')
print(f'Precision: {precision:.2f}')
print(f'Recall: {recall:.2f}')
print(f'F1 Score: {f1:.2f}')
```
```

PYTHON SCRIPT FOR COLLECTION AND ANALYSIS OF X POSTS

A Python script was developed and implemented to collect and analyze posts from the platform X, specifically tailored to gather datasets for each keyword examined in Chapter 3's analysis. Its functionality was optimized to handle large volumes of data efficiently while maintaining high performance. Rigorous testing and iterative refinement ensured the script met the specific requirements of the data collection and analysis process. Furthermore, the script was designed to align with best practices in coding standards and comply with data privacy regulations.

```
# Python Script for Collection and Analysis of X Posts
#!/usr/bin/env python3
      !pip install emot
      from tweepy import Client
      import tweepy
      import pandas as pd
      import re
      import numpy as np
      import csv
      from datetime import datetime
      from tweepy import OAuthHandler
      import matplotlib.pyplot as plt
      from wordcloud import WordCloud
      import nltk
      import emot
      from emot.emo_unicode import UNICODE_EMOJI, EMOTICONS_EMO
      nltk.download('stopwords')
      from nltk.corpus import stopwords
      from nltk.tokenize import RegexpTokenizer
      %matplotlib inline
      from transformers import pipeline, AutoModelForSequenceClassification, AutoTokenizer

# Hiding private keys, from the X Developer Portal
      consumerKey = 'HIDDEN'
      consumerSecret = 'HIDDEN'
      accessToken = HIDDEN'
      accessTokenSecret = 'HIDDEN'
      bearer_token="HIDDEN"

## connecting to X API v2 and loading the posts into Dataframe
## function for getting recent posts data
      def getPosts():

# Asking for the search term and the desired number of posts in English language
         global keyword
         keyword = input('insert search term: ')
         query = f'{keyword} -is:repost lang:en'
         num_posts = int(input('how many posts do you want? '))
         # Specify the date range
         start_date = input('Enter start date (YYYY-MM-DD): ')
         end_date = input('Enter end date (YYYY-MM-DD): ')

         # Convert the date strings to datetime objects,
         start_datetime = datetime.strptime(start_date, '%Y-%m-%d')
         end_datetime = datetime.strptime(end_date, '%Y-%m-%d')

# Connecting to the X API using the client and the bearer_token credentials from config.py
 client = Client(bearer_token)

# Using tweepy paginator to get posts from X API within the specified date range
  posts = []
         for post in tweepy.Paginator(client.search_recent_posts,
                                      query=query,
                                      post_fields=['id', 'created_at', 'public_metrics', 'text', 'source'],
                                      max_results=100,
                                      start_time=start_datetime.isoformat() + 'Z',
                                      end_time=end_datetime.isoformat() + 'Z').flatten(limit=num_posts):
            posts.append(post)
         return posts

# Function to Extract, transform, and load (ETL) posts
  def postsETL(posts):
         result = []

# Regex function to clean the post text from hashtags, mentions and links
 def cleanPosts(text):
         # Include the line to remove mentions
            clean_text = ' '.join(re.sub(\(@[A-Za-z]+[A-Za-z0-9-_]+)|([^0-9A-Za-z \\t])|(\\w+:\\/\\/\\S+)\, \ \, text).split())
            return clean_text,

# Function to unpack the posts list into a dataframe
         for post in posts:
            result.append({
               'id': post.id,
               'text': post.text,
               'clean_post': cleanPosts(post.text),
               'created_at': post.created_at,
               'source': post.source,
               'reposts': post.public_metrics['repost_count'],
               'replies': post.public_metrics['reply_count'],
               'likes': post.public_metrics['like_count'],
               'quote_count': post.public_metrics['quote_count']
```

```
            })
        df = pd.DataFrame(result)
        return df

## Performing the sentiment analysis using a base BERT model
#using a transformers model BERT to perform the sentiment analysis on the clean_posts column.
    def sentimentAnalysis(df):
        tokenizer = AutoTokenizer.from_pretrained('nlptown/bert-base-multilingual-uncased-sentiment')
        model = AutoModelForSequenceClassification.from_pretrained('nlptown/bert-base-multilingual-uncased-sentiment')
        classifier = pipeline(\sentiment-analysis\, model=model, tokenizer=tokenizer)
        res = df['clean_post'].apply(lambda x: classifier(x[:512]))
        return res

 ## function to add the list resulting from the analysis to the original dataframe as score, sentiment and stars

#The sentiment is either negative, positive or neutral, and the number of stars go from 1 to 5
#1 being the most negative sentiment and 5 being the most positive
def sentimentToDf(df,res):
        posts_stars = []
        posts_scores = []
        posts_sentiment = []
        #looping over the list of result to unpack it into the original posts dataframe
        for i in range(res.size):
            posts_stars.append(int(float(res[i][0]['label'].split()[0])))
            posts_scores.append(res[i][0]['score'])
            if res[i][0]['label'] == '4 stars' or res[i][0]['label'] == '5 stars':
                posts_sentiment.append('positive')
            elif res[i][0]['label'] == '1 star' or res[i][0]['label'] == '2 stars':
                posts_sentiment.append('negative')
            else :
                posts_sentiment.append('neutral')
        df['scores'] = posts_scores
        df['sentiment'] = posts_sentiment
        df['stars'] = posts_stars
        return df

#fucntion to Create the wordclouds using data from a column of a dataframe
def creatWordCloud(df,clm_name):
        text = \ \.join(line for line in df[clm_name])
        # Create the wordcloud object
        wordcloud = WordCloud(width=980, height=580, margin=0,collocations = False, background_color = 'white').generate(text)
        # Display the generated image:
        plt.figure(figsize=(12,5))
        plt.imshow(wordcloud, interpolation='bilinear')
        plt.axis(\off\)
        plt.margins(x=0, y=0)
        plt.show()
        return plt

## Creating report function to get insight from the analyzed posts
#creating a function to show the result of the sentiment analysis from the final df
def showReport(df):
        print(f'* the posts show that the sentiment around \{keyword}\ is mainly {df.groupby(by=\sentiment\).id.count().sort_values(ascending=False).index[0]
}')
        print(f'* this is how the overall sentiment and stars ratings breakdown on the {len(df)} total records we recovered : ')
        print(df.groupby([\stars\]).count()['id'])

        # Build the percentage of star count reviews by category bar graph.

star_perc = 100 * df.groupby([\stars\]).count()['id'] / len(df)
        plt.pie(star_perc,
             labels=[\1 star\, \2 stars\, \3 stars\, '4 stars', '5 stars'],
             colors=[\red\, \orange\, \gold\, 'turquoise', 'green'],
             explode=[0.05, 0.05, 0.05, 0.05, 0.05],
             autopct='%1.1f%%',
             shadow=True, startangle=150),
        plt.title(\percentage of Total posts by star ratings\),
        # Show Figure,
        plt.show(),
        # Build the sentiment reviews by category bar graph.,
        sent_perc = 100 * df.groupby([\sentiment\]).count()['id'] / len(df),
        plt.pie(sent_perc,
             labels=[egative\, eutral\, \Positive\,],
             colors=[\red\, \gold\, 'green'],
             explode=[0.05, 0.05, 0.05],
             autopct='%1.1f%%',
             shadow=True, startangle=150),
        plt.title(\percentage of total posts by sentiment \)
        # Show Figure
        plt.show()

#function to creat word clouds for each post sentiment,
def sentimentWordcloud(df):
        print(\We generate Wordclouds for each sentiment to see the words that appear most often for each one :\)
        print(\_____\),
        print('Wordcloud for negative sentiment posts : ')
```

```
        creatWordCloud(df.query('sentiment == egative\'),\clean_post\)
        print('Wordcloud for neutral sentiment posts : ')
        creatWordCloud(df.query('sentiment == eutral\'),\clean_post\)
        print('Wordcloud for positive sentiment posts : ')
        creatWordCloud(df.query('sentiment == \positive\'),\clean_post\)

 ## creating call function to streamline the process
     def postTodf():
        print (\this is a simple X sentiment analysis bot, please follow the instruction to know X's last thoughts. \- the posts collected are the last specified
number of posts about a keyword of your choice\)
        print ('connection to X IPA')
        df = postsETL(getPosts())
        print ('retrieving posts -- ')
        return df

     def sentimentTodf(df):
        print('----------------------------------------')
        print('sentiment analysis in progress.')
        print('this might take a minute ...')
        final_df = sentimentToDf(df,sentimentAnalysis(df))
        print('----------------------------------------')
        return final_df

     def finalReport(final_df):
        print('creating report ...')
        print(f'the report represents the sentiment around \{keyword}\, stars represent the sentiment of a post \ from 1 being most negative to 5 being most
positive ...')
        print(\_____\\),
        showReport(final_df)
        sentimentWordcloud(final_df)
```