THE CRYPTOCURRENCY AND DIGITAL ASSET FRAUD CASEBOOK, VOLUME II

DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks

Jason Scharfman

palgrave
macmillan

The Cryptocurrency and Digital Asset Fraud Casebook, Volume II

Jason Scharfman

The Cryptocurrency and Digital Asset Fraud Casebook, Volume II

DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks

palgrave
macmillan

Jason Scharfman
Corgentum Consulting, LLC
New York, NY, USA

ISBN 978-3-031-60835-3 ISBN 978-3-031-60836-0 (eBook)
https://doi.org/10.1007/978-3-031-60836-0

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is dedicated to the victims of cryptocurrency fraud and all who work tirelessly to combat it.

Preface

Since the original Bitcoin white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," was published on October 31, 2008, there has been no shortage of critics of the digital asset space. Recently, these critics have found no shortage of evidence to support their arguments. For starters, in 2022 alone, there were a series of crypto bankruptcies, the collapse of Terra (LUNA), and the exposure of the FTX fraud. More recently, other troubling trends have developed, including an explosion of cryptocurrency-enabled romance and pig butchering scams, phishing scams, and a continued series of decentralized finance (DeFi) hacks, demonstrating there is no shortage of malicious actors in the space. Additionally alarming is the growing involvement of Chinese and Russian organized criminal enterprises in crimes involving cryptocurrency and crypto-related money laundering. Even more concerning is the steady growth in state-sponsored cyberterrorism groups that increasingly involve the use of cryptocurrency in their hacks and illegal schemes. Furthermore, these fraudulent activities extend beyond simply stealing crypto into other areas of the digital asset spectrum, including decentralized autonomous organizations (DAOs), non-fungible tokens (NFTs), crypto casinos, and GameFi. Additionally, as of July 2023, it was reported that illegal crypto mining operations known as cryptojacking had increased almost 400% over the previous 12 months. With all of these different types of increasingly global, complex, and diverse frauds, it is now more important than ever for those involved in all aspects of the cryptocurrency industry to be appraised of criminal tactics and trends in fraud.

This book continues the work of the first volume of the *Cryptocurrency and Digital Asset Fraud Casebook* to continue the education on combatting fraud in the space. The first section of Chapters 1, 2 and 3 introduces the topic of cryptocurrency and digital asset fraud and crime. Chapter 1 begins the discussion with an overview of statistics relating to fraud in the space. Included in this discussion is an analysis of the impact of the COVID-19 pandemic on digital asset fraud. The chapter next discusses the backdrop of cryptocurrency bankruptcies and turmoil that laid the groundwork for the FTX fraud, including the bankruptcies of Voyager Digital and Celsius Network, and the collapse of Terra (LUNA). The chapter concludes with an analysis of the follow-on effects of the FTX fraud throughout the cryptocurrency industry.

Chapter 2 starts with a discussion of cryptocurrency romance scams, including an analysis of how they work, classifications of victims, and law enforcement challenges related to cryptocurrency romance scams. Next, the chapter discusses pig butchering scams and their explosive growth. The chapter concludes with an examination of the ways criminal money laundering groups in locations including Australia and China are involved in orchestrating and supporting these cryptocurrency-based romance and pig butchering schemes. Chapter 3 discusses frauds, hacks, and controversies in DAOs. The chapter commences with an introduction to DAOs and an analysis of The DAO Hack. Next, it discusses common types of DAO fraud and hacks and discusses price oracle manipulation and oracle alternatives. It then turns to a discussion of DAO security measures, voting and governance approaches, and vote fraud methods. The chapter concludes with an analysis of case studies in DAO fraud and controversies, including the BONq DAO hack (February 2023), the Tornado Cash DAO vote fraud case (May 2023), and the events leading up to the Azuki DAO hack (July 2023).

Chapters 4, 5 and 6 make up the second section of the book. These chapters delve into the complexities and vulnerabilities inherent in the decentralized finance (DeFi) ecosystem. Chapter 4 begins with an analysis of trends in DeFi frauds and hacks. The chapter then proceeds with an overview of flash loans and flash loan attacks. The remainder of the chapter analyzes case studies in flash loan attacks, including the Platypus Finance hack (February 2023) and the ethical hacker defense, Deus Finance flash loan and bot attacks (March 2022, April 2022, May 2023), and Kyberswap flash loan exploit (April 2023). Chapter 5 continued our conversation about DeFi with an analysis of case studies in smart contract vulnerabilities and bounty programs,

including Rodeo Finance (February 2023), Temple DAO (August 2023), and Dexible Aggregator (February 2023). The chapter then proceeds to discuss case studies in DeFi wallet hacks, reentrancy attacks, and read-only reentrancy attacks. These cases included the Binance deployer wallet hack (November 2023), the Yearn Finance hack (April 2023), and the Curve Finance hack (July 2023). Chapter 6 proceeded with an analysis of oracle attacks, defi market manipulation schemes, and rug pulls. Associated case studies include the El Dorado Exchange oracle attack (May 2023), the Mango Markets market manipulation case (October 2022), and the Ordinal Finance rug pull (April 2023). The chapter concludes with additional case studies in DeFi, including OptyFi's permanently inaccessible funds (June 2023) and the phishing attack on the Stargate Snapshot platform (December 2023).

The third section of the book is made up of Chapters 7, 8, 9, and 10. These chapters cover a wide array of case studies in fraud, hacks, and controversies from across the cryptocurrency universe. Chapter 7 begins with an overview of cryptocurrency phishing scams and provides an analysis of the different types of phishing attacks. The chapter concludes with an analysis of the mechanics of cryptocurrency spoofing scams and a discussion of the example of researcher spoofing. Chapter 8 begins with a discussion of meme coins and honeypot scams. As part of this discussion, a number of case studies in meme coin fraud and controversies are discussed, including Teddy Dodge, SafeMoon, BALD, and GROK. The chapter concludes with an analysis of frauds using deepfake technology to impersonate well-known figures such as Elon Mush, Sam Bankman-Fried, and Mark Zuckerberg in scams involving cryptocurrency.

Chapter 9 discussed decentralized applications (dApps) and cryptocurrency gaming fraud. It began with an introduction to dApps and then discussed their interactions with artificial intelligence and cryptocurrency. Next, dApp scams involving non-fungible tokens (NFTs), honeypots, and relevant case studies were presented. The chapter then discussed crypto casinos, crypto gambling fraud, and its interaction with money laundering. The chapter concluded with a discussion of GameFi, Play 2 Earn (P2E) scams, crypto fraud in online multiplayer games, and case studies.

Chapter 10 begins with a discussion about crypto exchanges and their use of digital asset wallets. The chapter then proceeds to discuss wallet drainers, cryptostealers, Malware as a service (MAAS), and ransomware attacks. The chapter concludes with an analysis of cryptojacking methods, reasons for the global growth in cryptojacking, and case studies, including cryptojacking in education and government institutions.

The fourth and final section of the book concludes with Chapters 11 and 12. Chapter 11 discusses non-fungible token (NFT) frauds, hacks, and controversies. Case studies were then discussed, including the Neopets data breach and the Pixelmon controversy. The chapter then discussed NFT rug pulls including Evolved Apes and Pixel Penguins case studies. The chapter concludes with several other case studies, including the Gutter Cat Gang Sim swap attack and the OpenSea spoofing scam. Chapter 12 began with a discussion of trends in cross-chain criminal activities. The chapter then analyzes the tactics of front-running bots, MEV bots, and MEV bot hacks. Next, we discuss the rise of state-backed cybercrime collectives, including North Korea's Lazarus Group. Additional topics discussed include Dark Web drug trafficking operations involving cryptocurrencies, crypto mining investment fraud, liquidity mining, and cloud mining are discussed. The chapter concludes with a discussion of cryptocurrency ATMs and QR code payment scams as well as a case study of a religion-based affinity scheme involving cryptocurrency.

Despite all of the fraud discussed throughout this book, there is good news on the horizon. Data suggests overall fraudulent activity in the space is declining. For 2023, Chainalysis reported that illicit crypto addresses received at least $24.2 billion, however, this was a significant decrease from a reported $39.6 billion in 2022. The types of cryptocurrencies used in fraudulent activities are also changing. While Bitcoin always remains popular, increasingly stablecoins account for the majority of the reported 2023 transaction volume.

Law enforcement is becoming increasingly adept at tracing stolen cryptocurrencies and catching and prosecuting crypto criminals. For example, in January 2024, German police made their largest-ever Bitcoin seizure by seizing 50,000 BTC in connection with a $2.17 billion fraud. In March 2024, the UK Crown Prosecution Service (PCS) reported the largest-ever Bitcoin seizure in the UK of 61,000 Bitcoin, worth over £4.3 billion, from a massive fraud and money laundering scheme. Finally, on January 10, 2024, the industry received some needed regulatory clarity with the approval of the Bitcoin ETF by the U.S. Securities and Exchange Commission (SEC). All of the gains, however, are of little consolation to victims who have lost billions in cryptocurrency and digital asset crime. The problem of cryptocurrency and digital asset crime represents a complex web of global organized crime, international law enforcement, evolving regulations, jurisdictional challenges, and, worst of all, millions upon millions of victims. While overall trends show a decline in the percentage of total on-chain activity represented by cryptocurrency crime, certain pockets of fraud, such as pig butchering, continue to

expand at alarming rates. As the industry continues to grow, it is my hope that publications such as this will continue to promote the best remedies to abate the continued growth of cryptocurrency fraud—education, transparency, and continued vigilance.

New York, NY, USA Jason Scharfman

Contents

1

Introduction to Cryptocurrency and Digital Asset Fraud

Introduction to Cryptocurrency and Digital Asset Fraud and Crime

As the cryptocurrency and digital asset industry has continued to grow significantly in recent years, unfortunately, frauds in the space have also seen a similar meteoric rise. Perhaps more concerning, the sophistication of fraud has continued to expand on numerous fronts. While criminals have continued to focus on well-established scams such as romance scams, celebrity impersonation, fake contests, and fraudulent investment schemes, they have also continued to develop new and innovative fraud techniques, including sophisticated wallet drainers, malware as a service, complex phishing schemes, and an increasingly complex Decentralized Finance (DeFi) attacks.

Additionally, cryptocurrency and digital asset fraud is increasingly a global problem, and victims come from all walks of life. In many cases, those involved in carrying out different aspects of these crypto frauds are themselves being victimized. Further complicating the landscape and the importance of cracking down on crypto fraud are the national security implications this criminal activity can have, especially when driven by large hacking groups from countries such as North Korea.

To begin with, let us examine the data in the following table, which summarizes the total value received by so-called illicit cryptocurrency addresses that have been classified as such based on historical activity[1]:

J. Scharfman, *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II*,
https://doi.org/10.1007/978-3-031-60836-0_1

Year	Total cryptocurrency value received by illicit addresses
2023	$24.2 billion
2022	$39.6 billion
2021	$23.2 billion
2020	$9.4 billion
2019	$12.5 billion
2018	$4.6 billion

While the amounts of the actual losses involved in cryptocurrency crime are astounding, equally staggering are the methods used to orchestrate these crimes. According to data from the Federal Trade Commission, from the period January 2021 to March 2022, the top frauds by reported cryptocurrency losses were broken out as follows:

Type of fraud	Amount
Investment-related fraud	$575 million
Romance scams	$185 million
Business imposters	$93 million
Government imposters (i.e., scammers pretend to be from a government agency)	$40 million

Effect of COVID-19 Pandemic on Digital Asset Fraud Trends

The COVID-19 Pandemic, also known as the coronavirus disease 2019, has precipitated profound transformations across the global economy, notably within the digital asset sector. The pivot to digital platforms for financial transactions and investments, driven by lockdowns and social distancing, has significantly expanded the digital asset market. This expansion, however, paralleled an increase in fraudulent activities. The first of the COVID-19 pandemic was reported in the city of Wuhan, Hubei province, China, in December 2019. In 2020, the sector witnessed losses exceeding $1.9 billion due to cryptocurrency-related fraud, marking a significant uptick from the preceding year.[2] This statistic underscores the scale of the challenge that the pandemic introduced to the digital financial ecosystem. A report by TransUnion highlighted an 80% spike in suspected digital fraud attempts globally,

compared to pre-pandemic levels, underscoring the escalating challenge of securing digital transactions and assets against fraudulent activities.[3]

With the onset of the pandemic, the landscape of digital asset fraud evolved dramatically. Scammers were able to capitalize on large portions of the global population being confined to their homes with Internet access. This period has been marked by what some deemed a "scamdemic," with a global epidemic of scams and frauds coinciding with the pandemic, raising unprecedented concerns in areas such as phishing attacks.[4] Interestingly, during this time, cryptocurrencies have also been viewed as safe havens, similar to precious metals, providing diversification benefits for investors amid the crisis.[5] This suggests a nuanced impact of the pandemic on digital assets because, alongside an increase in fraud, there has also been an enhanced perception of digital currencies as a secure investment option. The ***FBI's Internet Crime Complaint Center (IC3)*** noted a substantial increase in cryptocurrency-related fraud reports, with over 82,135 incidents in 2020, nearly doubling the figures from 2019.[6] These amplified fraud signals demonstrate not just the growing allure of digital assets but also the opportunistic exploitation of pandemic-induced vulnerabilities by fraudsters.

The regulatory landscape reacted dynamically to the pandemic's challenges, with global regulators stepping up to fortify the digital asset sector against the uptick in fraudulent activities. The ***Financial Action Task Force (FATF)*** exemplified this proactive stance by revising its guidelines to enforce stricter compliance requirements for virtual asset service providers, including enhanced due diligence and more rigorous monitoring systems.[7] These regulatory adjustments were precisely aimed at mitigating the risks posed by the pandemic, emphasizing the need for a robust regulatory framework to protect investors and the integrity of the digital asset market.

Pandemic Response Accountability Committee (PRAC)

Regulatory efforts to address crypto fraud during the pandemic have intensified, with a focus on mitigating risks and enhancing oversight. The ***Pandemic Response Accountability Committee (PRAC)*** has been actively involved in combating fraud against pandemic response programs, particularly targeting small business loan recipients at the highest risk of fraud.[8] Additionally, the Department of Justice's COVID-19 Fraud Enforcement Task Force, of which the PRAC is a member, has been instrumental in uncovering fraud schemes and providing valuable leads for the Inspector General community.[9] Lessons learned from the pandemic underscore the importance of stronger financial regulation and supervision, as well as the development of global standards to

stem the risks associated with crypto assets.[10] These developments highlight a concerted effort by regulatory authorities to adapt and respond to emerging threats posed by crypto fraud during the pandemic, laying the groundwork for more robust regulatory frameworks in the future.

Technological Sophistication of Fraud in the Pandemic Era

The technological intricacy of fraud schemes saw significant advancements during the pandemic. Cybercriminals leveraged the situation to deploy sophisticated techniques such as ***deepfake*** technology and advanced phishing schemes to orchestrate more convincing scams. The utilization of these technologies not only diversified the fraud landscape but also presented significant challenges in detection and prevention. During the pandemic, there was a notable increase in the deployment of sophisticated fraud mechanisms, indicating a shift toward more complex and hard-to-detect scams.[11] This evolution points to a critical need for ongoing innovation in cybersecurity measures to counteract the evolving threat landscape.

Cryptocurrency-Related COVID-19 Economic Injury Disaster Loan (EIDL)/Paycheck Protection Program (PPP) Fraud

As part of the U.S. government's COVID-19 financial assistance programs, the Small Business Administration's (SBA) managed programs, including the COVID-19 Economic Disaster Loan (EIDL) and Paycheck Protection Program (PPP) whereby assistance funds were loaned out and, in some cases, simply given to qualifying businesses impacted by the pandemic. As with most government programs, scammers came out in droves to try to steal from the PPP program. According to the SBA itself, a staggering 17% of all the funds paid out, or roughly over $200 billion, were potentially fraudulent.[12]

The cryptocurrency industry was no exception to the EIDL and PPP-related fraud. These cases are related to allegations of fraud being carried out in multiple ways and in multiple areas of the crypto industry. In one case in November 2022, the owner of a pooled Bitcoin fund was alleged to have fraudulently applied for over $400,000 in PPP loans. The following is an excerpt from the U.S. Department of Justice related to this matter[13]:

"A Dallas man who allegedly devised a scheme to defraud a pandemic-era financial program out of hundreds of thousands of dollars has been federally

charged announced U.S. Attorney for the Northern District of Texas Chad E. Meacham.

John Corbin Corona, 35, was indicted on October 5, 2022, on one count of wire fraud and one count of money laundering. He was arrested on Monday and made his initial appearance before U.S. Magistrate Judge Toliver today.

> "As millions of small business owners grappled with the fallout from the pandemic, this defendant raked in a couple hundred thousand bucks at his fellow citizens' expense," said U.S. Attorney Chad Meacham. "The Paycheck Protection Program, funded by taxpayers, was designed to help small businesses stay afloat during the pandemic. The Justice Department will relentlessly pursue those who defrauded the PPP."

According to the indictment, Mr. Corona—the owner of HODL LLC, a cryptocurrency company operating a purported bitcoin pooled investment fund known as Bitcoin Bank America—fraudulently applied for two Paycheck Protection Program (PPP) loans totaling over $413,000 through BlueVine Inc. and FundBox, Inc., financial technology companies that partnered with third-party PPP lenders, including Celtic Bank.

According to the indictment, Mr. Corona inflated HODL LLC's payroll and misrepresented his business's number of employees in the PPP loan applications that he submitted to BlueVine and Fundbox. In support of the PPP loan applications, he also submitted IRS Form 941s (Employer's Quarterly Federal Tax Return) that allegedly contained false information about his business.

The indictment also alleges that after Celtic Bank deposited $206,902 in PPP loan proceeds into Mr. Corona's bank account, Mr. Corona transferred over $155,000 in PPP loan funds to Coinbase Inc., a cryptocurrency exchange platform."

In many other cases, people used EIDL and PPP money that was obtained under fraudulent means to simply purchase cryptocurrencies. An example of this was the July 2023 allegations raised against a Nevada doctor and his wife for fraudulently obtaining nearly $1.3 million in economic relief loans and then using the funds to purchase stocks and cryptocurrencies.[14]

In another example, in May 2023, two men pled guilty to stealing over $7 million in COVID-19 relief funds by using techniques including falsifying payroll records and creating fake tax returns. The stolen funds were used to purchase vehicles, undertake home renovations, pay personal expenses, and finally purchase cryptocurrencies.[15]

In July 2020, a Texas man, Joshua Thomas Argires, took out a fraudulent PPP loan in the amount of $956,600 for a company called "Texas Barbecue." The problem was that its investigators later uncovered that Texas Barbecue had no documented employees, no online reviews, and no bank account until four days prior to the PPP loan request.[16] Another fraudulent request was also allegedly filed by Mr. Argires for another company called Houston Landscaping that also reportedly had no employees. In total over $1.1 million in fraudulent loans. After receiving the loans some of this money was later transferred to a Coinbase account where it generated a profit.[17]

In July 2022, a California man named Lebnitz Tran pled guilty to submitting at least 27 fraudulent PPP loan applications and at least seven fraudulent EIDL applications to obtain over $3.6 million that was spent on, among other items, a $100,000 Tesla and cryptocurrencies.[18]

In August 2023, Dana McIntyre, the former owner of a Boston area pizzeria, was sentenced to two years in federal prison and ordered to pay $679,156 in restitution and forfeiture for taking fraudulent PPP loans. He had used the funds to purchase an alpaca farm in Vermont, pay personal expenses, and purchase airtime for cryptocurrency themed radio show.[19]

Laundering Fiat into Crypto

Although blockchains provide public records of transactions, in some instances, because of the supposed anonymity of cryptocurrencies, some criminals attempt to take fiat earned through non-crypto-related schemes. Once the fiat is stolen (either in physical or electronic forms), it is then transferred into crypto. The criminals usually attempt to further obfuscate the sources of the illegal funds by running the crypto through networks of offshore crypto exchanges and mixers.

Some of the attempts to launder fiat through crypto were related to the fraudulent loan cases of EIDL and PPP that were discussed in the previous section. One example involves a former social media influencer named Danny Devan, whose real name is Denish Sahadevan, who became famous on TikTok for creating financial literacy content focused on investing in cryptocurrencies and stocks.[20] Mr. Devan pled guilty to federal charges that he took out of 70 fraudulent PPP loans worth over $1.2 million and then laundered some of those funds in cryptocurrencies and a gold physical Bitcoin.[21]

Case Studies in Cryptocurrency Bankruptcy and Turmoil

In order to better understand the backdrop for more recent developments in cryptocurrency fraud, it is important first to develop an understanding of key events that have impacted the space. We will proceed with discussing a series of cryptocurrency-related bankruptcies and turmoil within the space that set the stage for the FTX fraud and its follow-on effects.

Cryptopia (January 2019)

In January 2019, the New Zealand-based cryptocurrency exchange Cryptopia experienced a significant security breach, leading to the platform going offline and reporting "significant" losses.[22] The hack not only resulted in substantial financial damage but also raised concerns about the security measures implemented by exchanges to protect users' assets. The incident prompted Cryptopia to suspend its services, as it worked to assess the extent of the losses and to implement measures to prevent further breaches.

Following the hack, Cryptopia struggled to recover from the financial and reputational damage it sustained. In May 2019, the exchange filed for bankruptcy protection in the United States. This move was aimed at preserving vital user data stored on servers in Arizona and managing the liquidation process more effectively.[23] This step was necessary to address the complexities arising from the hack, including securing assets and information still under its control. The bankruptcy filing highlighted the challenges faced by cryptocurrency exchanges in maintaining security and trust, emphasizing the need for robust security protocols and transparent communication with users in the aftermath of such incidents.

Fcoin (February 2020)

FCoin was a cryptocurrency exchange platform that operated using a novel "trans-fee mining" model, where traders were incentivized with native tokens for their trading activities. The exchange FCoin has faced significant challenges, culminating in a complex scenario involving insolvency, token buybacks, and unresolved user debts. FCoin, once a prominent player in the crypto exchange market, announced its insolvency in February 2020, revealing a shortfall of up to $130 million worth of Bitcoin.[24] This disclosure came after the exchange encountered Bitcoin outflow issues just two

months post-launch, signaling deep-rooted financial and operational difficulties.[25] FCoin struggled to manage its assets eventually leading to its inability to fulfill user withdrawals and ultimately declaring bankruptcy.

Further complicating matters, FCoin initiated a buyback scheme in 2018, committing to repurchase $24 million of its own tokens to inject capital into a new fund of funds.[26] This move, often seen as a strategy to manage token supply and stabilize the market price, underscores the broader industry practices where exchanges engage in buybacks and token burns to influence token economics positively. However, FCoin's efforts in this direction were insufficient to counterbalance the operational challenges it faced. As FCoin ceased operations, it left a substantial debt to its users, estimated between $67 million to $125 million, sparking outrage and concern within the crypto community.[27]

Hodlnaut (January 2022)

Hodlnaut, a cryptocurrency lending platform, faced significant challenges in January 2022 that led to judicial managers being appointed to oversee its restructuring efforts.[28] Initially, need to explore various options to salvage the business and repay its creditors. Amid these efforts, Hodlnaut's judicial managers received a buyout offer from OPNX, valued at $30 million. This proposal was seen as a potential lifeline for the embattled lender, which had over 17,000 customers awaiting the recovery of their funds.[29]

However, the offer from OPNX was rejected due to concerns over the liquidity of the FLEX token, which had plummeted by 90% in value.[30] The decline in the FLEX token's value raised doubts about the viability of the offer and its ability to adequately compensate Hodlnaut's creditors and facilitate the company's recovery. The rejection of OPNX's bid underscored the complexities involved in navigating the aftermath of a crypto platform's collapse, highlighting the challenges in securing a viable path forward for Hodlnaut and its stakeholders. In November 2022, it was reported that Hodlnaut would be liquidated.[31]

Babel Finance (July 2022)

Babel Finance is a Hong Kong-based crypto lender. In June 2022, the firm announced a suspension of withdrawals, citing "unusual liquidity pressures" amid a broader downturn in the crypto market.[32] This decision reflected the strain many crypto lenders were experiencing due to the volatile nature of

cryptocurrency markets and the knock-on effects of broader economic challenges considering the issuance of a crypto-backed stablecoin in conjunction with a decentralized finance platform as a strategy to repay creditors after experiencing significant losses.[33]

This move comes after Babel Finance faced liquidity issues, leading to the suspension of withdrawals and the loss of $280 million through customer fund trading activities.[34] The proposed stablecoin, part of a broader effort to address the company's financial challenges, aims to generate revenue to cover the $766 million owed to creditors.[35] Babel Finance's plan to introduce a stablecoin as a repayment method underscores the ongoing attempts within the crypto industry to find innovative solutions to financial distress, while also highlighting the risks and complexities of operating within this rapidly evolving sector.

Zipmex (July 2022)

In 2022, Zipmex, a cryptocurrency exchange focused on Southeast Asia, filed for bankruptcy protection in Singapore amidst a significant downturn in the crypto market.[36] This move came as a response to the looming threat of legal actions from creditors. Zipmex's decision to seek bankruptcy protection highlighted the broader impact of the bear market on crypto firms and followed the pause of customer withdrawals, signaling severe liquidity issues within the exchange.

The situation was further complicated by the exchange's exposure to the collapse of Hong Kong-based crypto lender Babel Finance, to which Zipmex had reportedly lent as much as $100 million.[37] This financial entanglement with a failing entity underscored the interconnected risks prevalent in the crypto industry. The bankruptcy filing by Zipmex in Singapore was a notable event, reflecting the challenges faced by cryptocurrency exchanges during market downturns and the cascading effects of financial distress within the sector.

Voyager Digital (July 2022)

Voyager Digital was a cryptocurrency brokerage company. The firm promised users the ability to earn interest on their cryptocurrency deposits. This approach, however, exposed Voyager to significant risks, particularly as it extended credit lines to large institutional borrowers like Three Arrows Capital. The downfall of these borrowers amidst a wider crypto market slump

left Voyager in a precarious financial state, culminating in a Chapter 11 bankruptcy filing.[38] This move was designed as a strategic restructuring effort to salvage the company from its debts and operational challenges.

The FTC's subsequent legal action against Voyager Digital and its former executive underscores the regulatory scrutiny facing the crypto industry.[39] The agency's charges, focused on misleading claims regarding FDIC insurance, highlight the tension between crypto's innovative zeal and the need for consumer protection. The FTC's settlement with Voyager, while not including the former CEO, Stephen Ehrlich, who faces ongoing litigation, marks a significant moment of accountability. It serves as a cautionary tale for the crypto industry, emphasizing the importance of truthful advertising and the protection of consumer assets.

The National Basketball Association (NBA) found itself entangled in legal challenges due to its promotional partnership with Voyager. A class-action lawsuit accused the NBA of gross negligence, alleging that the league's endorsement led fans to invest in a platform that would eventually suffer losses exceeding $4.2 billion.[40]

Core Scientific (December 2022)

Core Scientific is a blockchain infrastructure and software solutions provider specializing in high-performance computing and large-scale cryptocurrency mining operations.[41] In late December 2022 Core Scientific, grappling with financial distress exacerbated by plummeting Bitcoin prices and soaring energy costs, filed for Chapter 11 bankruptcy.[42] This event was not a reflection of the broader market conditions affecting the crypto mining industry at the time.

The filing for bankruptcy was a strategic move, aiming not for liquidation but for restructuring. Core Scientific's goal was to recalibrate its operational framework. In January 2024 when the company received court approval for its restructuring plan.[43] Central to Core Scientific's restructuring plan was an equity stake agreement with Bitmain and Anchorage.[44]

Building upon the crypto bankruptcies we have discussed, several large cryptocurrency projects experienced significant turmoil in a relatively short period in 2022. While largely spurred on by the failure of FTX, which turned out to be a fraud, and the cascading effects that followed, prior to FTX, the impetus for much of the turmoil that followed can be traced back to Terra (LUNA).