Governing Cryptocurrency Exchanges with a History-Informed, Principles-Based Framework

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program University of Toronto

Prepared by Hadia Kiani

June 03, 2025

For Professor Leonard Brooks

Acknowledgements

I would like to thank my mentor, Amrit Dev, for her invaluable guidance and insights on this topic throughout the writing of this paper. Her recommendations have been invaluable in guiding me. I am also thankful for her comments on the earlier drafts of this paper, which helped me improve the quality of this paper. I would also like to thank my supportive guide, Ana Rusu, for her valuable advice on how to best approach this paper. Her guidance was invaluable in getting me started and shaping the structure of this paper. Lastly, I wish to thank my family for their constant and unwavering support throughout this journey. Undertaking this work was challenging at times, but their consistent encouragement, provided me the strength and motivation I needed to persevere. Above all, I am grateful to God for giving me the strength and patience to complete this research paper.

Table of Contents

1) Executive Summary

Ever since the release of Bitcoin Whitepaper in 2008 by Satoshi Nakamoto,[1] cryptocurrency has been on a constant bloom, garnering interest from a wide variety of audience. This bloom has been marked by the introduction of over 16,000 cryptocurrencies[2] and a market capitalization of over $3 trillion.[3] While the rapid growth of cryptocurrency has introduced numerous opportunities for innovation and flexibility, it also has serious vulnerabilities, enabling fraud perpetrators to exploit these weaknesses and providing them novel tools to perpetrate fraud.

Amid the vast spectrum of fraudulent schemes involving cryptocurrency, cryptocurrency investment fraud is one that has attracted significant attention, in part due to the speculative elements often associated with cryptocurrency. Fraud through cryptocurrency exchanges seems to have attracted considerable interest from the perpetrators and has sparked debate from the different stakeholders regarding a need for enhanced oversight of these exchanges.

This paper analyzes three cryptocurrency exchange-related fraud cases, each with distinct features, using a fraud diamond perspective to determine what, if any, are the prevalent themes. This paper is primarily focused on dissecting the "capabilities" and "opportunities" that resulted in the fraud, although limited commentary has also been made on the "motivation" and "rationalization" aspects. A high-level analysis of the current state

---

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin*, October 31, 2008. https://bitcoin.org/bitcoin.pdf.

[2] "Global Cryptocurrency Market Cap Charts." CoinGecko, accessed May 17, 2025, https://www.coingecko.com/en/global-charts. Refer to *Figure A* in Appendix.

[3] "Cryptocurrency Charts & Market Data." CoinMarketCap, accessed May 17, 2025, https://coinmarketcap.com/charts. Refer to *Figure B.1* in Appendix.

of regulatory landscape in the US and Canada has also been performed to assess the gaps in the current oversight. The paper recognizes the complex and evolving regulatory landscape in this space, as regulators are constantly adapting and taking initiatives in response to emerging fraud cases and developments in this sector, to enhance governance. Accordingly, the overall objective of the paper is to propose a fraud risk framework that provides guiding principles to regulators to enhance the effectiveness of the regulations in preventing and detecting fraud.

By drawing lessons from real world cases and providing a principles-based framework, this paper aims to support a proactive approach to fraud prevention. Such a framework provides a structured, yet a flexible approach to addressing the fraud risk in the ever-evolving cryptocurrency space. This area presents numerous opportunities for IFAs as their roles evolve beyond traditional fraud investigations, into fraud governance, risk assessments, ongoing monitoring and stakeholder education.

2) Background of Research Topic

2.1) Cryptocurrency Concepts

Before diving into the specifics of this research paper, it is important to establish a foundational understanding of cryptocurrency to contextualize the discussion that follows.

Cryptocurrency is digital currency, that uses cryptography to create, verify and secure transactions.[4] Since cryptocurrency only exists electronically, it has no physical form[5] and has no intrinsic value such that "they are simply worth what people are willing to pay for them in the market".[6] All transactions related to cryptocurrency are recorded on a blockchain, which is "a decentralized ledger of all transactions across a peer-to-peer network".[7] The example and diagram below by the Reserve Bank of Australia[8] provides a helpful illustration of how transactions related to cryptocurrency occur. The entire example has been summarized below:

Let's assume Alice wants to transfer one cryptocurrency to Bob. To initiate the transaction, Alice will send an electronic message with instructions to the network (blockchain) where all users on the network can see her message. As any transaction is not instantly added to the network, it sits with other pending transactions, awaiting its turn to be verified and added.

---

[4] "Crypto assets." Financial Consumer Agency of Canada, last modified December 16, 2024. https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html.

[5] "Making Sense of Bitcoin, Cryptocurrency and Blockchain." PwC, accessed on May 17, 2025. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

[6] "Digital Currencies." Reserve Bank of Australia, accessed on May 17, 2025. https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html.

[7] "Making Sense of Bitcoin, Cryptocurrency and Blockchain."

[8] "Digital Currencies"

Once the transaction is ready to be verified, the "miners" will group the pending transactions together into a "block". The information of all the transactions in the block is converted into a cryptographic code, which needs to be solved to add that block to the blockchain. Once the code is solved by miners, the block is added to the blockchain and the transaction is confirmed. After the transaction has been confirmed, Bob will receive the cryptocurrency.

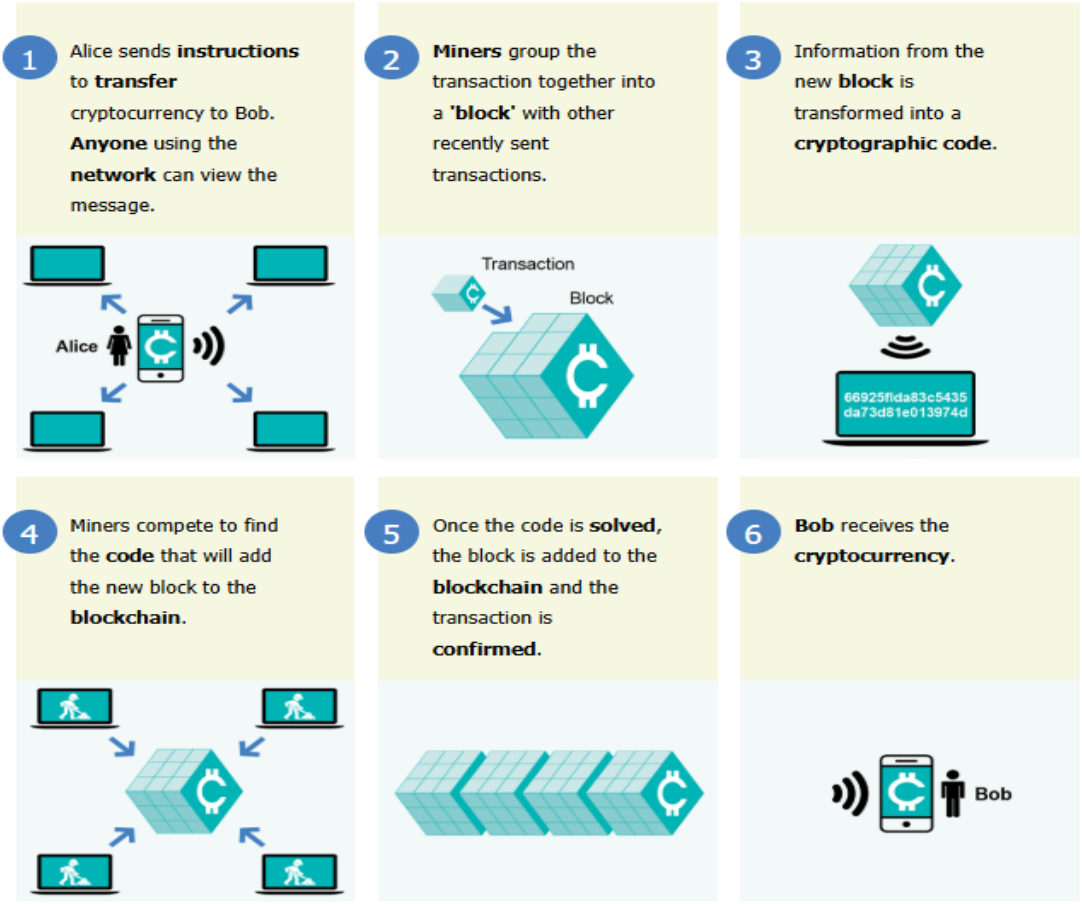


Figure 1.1[9]

[9] Ibid.

A few additional concepts to consider in the above example are:

- Alice will need the "public wallet address" of Bob to send him the cryptocurrency. A public wallet address or a public key is an address that can be shared with anybody and allows a user to send funds to a particular wallet.
- Before the transaction is sent to the network, Alice will need to digitally sign the transaction with her "private key" to prove that it is indeed Alice who wants to send the cryptocurrency. This private key is a password that allows a user to access their cryptocurrency and perform transactions. If the private key to a digital wallet is lost, the cryptocurrency would also be lost permanently and will become inaccessible for the user.
- The cryptocurrency received by Bob will be stored on the blockchain, with his private keys stored on a digital wallet, and Bob's private key will be required to access this cryptocurrency.

There are two different categories of a digital wallet – custodial wallet and non-custodial wallet. A non-custodial wallet is a digital wallet where the user has access to the private keys, whereas a custodial wallet is a digital wallet where the private keys are held by a third party that manages the users' cryptocurrencies.[10]

In addition to above, there are two more subtypes of a digital wallet – hot wallet and cold wallet.[11] A hot wallet stores the private keys online, and a user needs to be connected to the internet to access it. As they are online, these are quick and more

[10] "Cryptocurrency Wallet: What It Is, How It Works, Types, and Security." Investopedia, November 25, 2024. https://www.investopedia.com/terms/b/bitcoin-wallet.asp.

[11] Ibid.

convenient for users to access their wallets. However, this also exposes them to risks such as hacking. On the other hand, a cold wallet stores the private keys of the digital assets offline. As these are not online, they are generally safer, but less convenient than hot wallets. Before a transaction can be performed, the cryptocurrency would need to be moved from a hot wallet to a cold wallet first. While there are even more additional subtypes of the digital wallets, they are not addressed in detail here as they fall beyond the scope of this paper.

2.2) Birth of Cryptocurrency Exchanges

In 2010, after the idea was proposed on BitcoinTalk forum, the first cryptocurrency exchange Bitcoin Market was launched,[12] with the ultimate purpose of buying and selling bitcoins with each other.[13] As the use of cryptocurrency increased, many cryptocurrency exchanges and cryptocurrency asset trading platforms have emerged to facilitate the trading of crypto assets for investors.

A cryptocurrency exchange is an online platform that allows people to buy and sell cryptocurrency, facilitating the trading of digital assets. A cryptocurrency exchange can be a centralized platform (one entity acts as the intermediary between customers) or a decentralized platform (platform customers can trade with each other without any intermediary).[14] While both types of platforms facilitate the trading of cryptocurrency for users, there remains ambiguity around how they are governed. Unlike traditional trading platforms that operate under clear regulatory frameworks, many cryptocurrency exchanges operate in a grey area, where some are regulated while other can operate without any oversight. This ambiguity exposes them to vulnerabilities, consequently putting the investors at risk.

When customers use these platforms to buy, sell or store digital assets, the exchanges usually charge a fee for each transaction that happens on the platform. Hence, a higher volume of trade on these platforms translates into higher revenue earned by these

---

[12] "What was the First Crypto Exchange." Cryptohopper, accessed on May 17, 2025. https://www.cryptohopper.com/blog/what-was-the-first-crypto-exchange-449.

[13] "New Exchange (Bitcoin Market)." Bitcoin Forum, accessed on May 17, 2025. https://bitcointalk.org/index.php?topic=20.0. Refer to *Figure C* in Appendix.

[14] "Centralized vs Decentralized Crypto Exchanges: What's the Difference?" *CoinLedger*, accessed May 24, 2025. https://coinledger.io/learn/centralized-vs-decentralized-crypto-exchanges.

exchanges. In essence, the success of an exchange depends primarily on the volume of transactions on the exchange, motivating exchanges to have as many customers use their platform. On the other hand, while motivations vary, often times customers may be drawn to trade cryptocurrency due to the volatility in its price, which is often impacted by the market demand and sentiment – factors that can be driven by expectations of rising prices itself, leading to a circular dynamic.

Another notable point regarding cryptocurrency exchanges is that transactions that happen within an exchange (i.e. customers on the exchange transacting with each other) are not recorded on the blockchain and may only be recorded internally.[15] Per Chainalysis, a blockchain data analysis firm that traces cryptocurrency transactions, "*Only the exchange itself knows which deposits and withdrawals are associated with specific customers, and that information is kept in the exchange's order books, which aren't visible on blockchains or in analysis tools like Reactor*".[16] This is applicable specifically to centralized exchanges as transactions that happen on decentralized cryptocurrency exchanges are published to a blockchain and are transparent.[17] This factor is worth noting, given that a large amount of confidence in cryptocurrency is associated with the transparency, accuracy and immutability features of blockchain.

---

[15] Alison Jimenez. "Cryptocurrency Traceability: Unraveling underlying assumptions." *Dynamic Securities Analytics, Inc.,* February 1, 2024. https://securitiesanalytics.com/cryptocurrency_traceability.

[16] "Why You Can't Trace Funds Through Services Using Blockchain Analysis (and Why You Don't Need to Anyway)." *Chainalysis Blog,* October 9, 2020. https://www.chainalysis.com/blog/blockchain-analysis-trace-through-service-exchange/.

[17] Allie Grace Garnett, "Centralized vs. decentralized crypto exchanges – which should you choose?" *Britannica Money*, accessed May 24, 2025, https://www.britannica.com/money/centralized-vs-decentralized-crypto.

2.3) Growth & Fraud in the Cryto Space

When it was introduced in 2009, Bitcoin, the first ever cryptocurrency, was worth $0.[18] At the time of this analysis, it is worth $103,191.[19] This growth in the value of Bitcoin offers a glimpse into the rapidly scaling nature of cryptocurrency. Additionally, as of the date of this analysis, the global market capitalization of cryptocurrency is $3.39 trillion, representing a growth of 32.98% from one year ago,[20] with at least 818 exchanges in existence, 15.60 million cryptocurrencies tracked, and a 24-hour trading volume of over $95 billion.[21] Among its many magnets, the decentralized landscape and the speculative nature of cryptocurrency are the major drivers of interest.

Consistent with broader trends, as the industry has grown, the crime and unethical activity in the space has also grown. Per the Chainalysis Crypto Crime Report in 2024, the value received by illicit addresses totalled $40.9 billion.[22] The crime in the crypto space varies from crypto scams, ransomware attacks, stolen funds and terrorist financing among other things.

The constant evolving nature and the lack of any defined set of laws and regulations for the cryptocurrency space makes it more vulnerable to criminal activities. Historically, the lack of regulations around cryptocurrency exchanges has placed the investments of

---

[18] John Edwards, "Bitcoin's Price History." *Investopedia*, January 23, 2025. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.

[19] "Bitcoin USD Price (BTC-USD) Historical Data." Yahoo Finance, accessed May 17, 2025. https://finance.yahoo.com/quote/BTC-USD/history/.

[20] "Global Cryptocurrency Market Cap Charts." Refer to *Figure A* in Appendix.

[21] "Number of Cryptocurrencies Tracked." CoinMarketCap, accessed May 17, 2025, https://coinmarketcap.com/charts/number-of-cryptocurrencies-tracked/. Refer to *Figure B.2* in Appendix.

[22] "The 2025 Crypto Crime Report," pg. 3. *Chainalysis*, February 2025. https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf.

numerous people at risk. Combined with the high volatility of cryptocurrency, anonymity of blockchain and the constantly evolving fraud schemes, fraud detection faces its own challenges, making it harder to recover the funds that have been victims of cryptocurrency scams. Hence, fraud prevention is the first line of defense in mitigating the frauds in cryptocurrency ecosystem and minimizing the losses for investors. To develop an effective fraud prevention strategy, it is essential to take lessons from history and build controls that prevent the same vulnerabilities from being exploited again. Additionally, given the rapidly changing environment of this ecosystem, it is crucial that a structured, but adaptive approach is followed to address the evolving risks. As discussed in the next section, this research paper achieves both of these objectives by analyzing real-world cases and recommending a tailored fraud risk framework that provides overarching, flexible principles for maintaining oversight in the cryptocurrency industry.

3) Research Scope

3.1) Objectives & Motivation

The objectives of this research paper are to analyze three specific cryptocurrency exchange frauds, each with different characteristics, from the lens of fraud diamond. The focus is to identify specific factors that contributed to the opportunity, capability, motivation and rationalizations of such frauds. The application of this lens enables us to pinpoint the causes to specific elements, leading to development of enhanced fraud preventative strategies.

Using the guidelines from 2016 COSO Fraud Risk Management Guide,[23] this paper provides overarching principles that can be used by regulators to enhance the fraud risk governance, fraud risk assessments, fraud investigations and ongoing monitoring practices for the cryptocurrency industry. Using the learnings from the cases analyzed, specific preventive and detective controls have also been recommended. The objective is to provide broad principles that can be adopted to promote proactive fraud prevention in this industry.

The motivation for selecting this topic stems from the growing ecosystem and increasing fraud incidents in the cryptocurrency industry. As this space continues to evolve, the frequency of such incidents can only be expected to increase. Hence, this is a valuable area of study, especially given the evolving regulatory landscape and need for clearer guidance. Understanding these patterns can contribute meaningfully to the development of effective fraud prevention strategies within an emerging and fast-moving industry.

[23] Committee of Sponsoring Organizations of the Treadway Commission. "Fraud Risk Management Guide – Executive Summary." *Committee of Sponsoring Organizations of the Treadway Commission,* September 2016. https://www.coso.org/_files/ugd/3059fc_02c01fde6552479196535bcfee8ea60e.pdf.

3.2) Documents Reviewed and Relied Upon

In analyzing the cryptocurrency cases, the primary sources of information that have been relied upon are the court or securities commissions' decisions related to the specific case. Secondary sources of information are the news articles covering the given case, in the instances where there was media coverage. In some instances, the archived websites of the exchanges have also been referred to, in order to obtain the representations made by these exchanges to their customers.

In summarizing the current state of the regulatory landscape, the primary sources of information are the websites or information circulars published by the regulatory body. Specifically, for Canada, information from the Canadian Securities Administrators website has been relied upon, whereas for the US, information from the Securities and Exchange Commission (SEC) website and Commodity Futures Trading Commission (CFTC) website has been relied upon. Secondary sources of information are the commentary by various stakeholders on these regulations.

Lastly, the fraud risk framework principles proposed are grounded in the key learnings from the case analysis. The recommendations may align with those proposed by regulatory bodies, industry experts, and other key stakeholders, as this remains an area of active discussion among industry participants. This paper has aimed to appropriately cite all sources to ensure full credit is given to the original contributors.

All sources have been referenced within the paper as footnotes, and have been listed under the **Bibliography** section at the end of the paper as well.

4) Methodology

4.1) Selected Cases

This section outlines the rationale for the cases that have been selected for further analysis in this paper.

Cryptocurrency exchanges serve as a centralized platform that brings together a wide range of investors, consequently, holding a large amount of assets and a high financial exposure. Accordingly, when vulnerabilities in the regulations are exploited at an exchange level, it results in a systematic fraud and higher financial loss. Given the importance of monitoring such exchanges, this paper has focused on exploring factors that have resulted in cryptocurrency exchange related frauds to support formulation of strategies for their prevention.

To understand the underlying patterns and themes that have resulted in the conditions conducive for fraud, it is important to look at a sample that is representative of the players in the cryptocurrency industry, as well as have reliable information available for analysis. Hence, this paper has attempted to select cases that exhibit different characteristics to allow for an analysis of whether different factors influenced each case. Specifically, the following cases have been selected:

1. ***QuadrigaCX ("Quadriga")***

   Quadriga is the biggest cryptocurrency exchange-related fraud that has occurred in Canada. Hence, this case has been selected to analyze the root causes and factors in Canada that led to this scandal.

2. ***FTX Trading Ltd ("FTX")***

FTX has been one of the largest cryptocurrency exchange-related fraud that has occurred in the United States. This case has been chosen to understand the factors that led to perpetration of the fraud in the US, especially to understand if there are significant jurisdiction-specific reasons for this fraud and whether a fraud of this extent can happen in Canada.

3. ***ezBtc***

Occurring in Canada, ezBtc is a smaller cryptocurrency exchange-related fraud as compared to the above two cases. Nonetheless, it is still valuable to do an analysis of this case to assess if specific factors are associated with higher-magnitude frauds as compared to smaller ones. Analyzing a fraud of smaller magnitude can help us evaluate whether there are repeat patterns across the industry and pinpoint the issues to wider, systematic factors. Furthermore, even if different factors resulted in the fraud at a smaller magnitude, the number of players in the industry are significant enough that it becomes valuable to analyze the cause of such cases and implement measures to prevent them in the future.

4.2) Framework For Analysis: Fraud Diamond

This section outlines the rationale for selecting the specific framework used for the analysis of the selected cases.

To perform the analysis of the cases in a structured approach, it is important to select a consistent framework that can be applied across all selected cases. For the purposes of this paper, the cases have been analyzed through the lens of Fraud Diamond to provide a structured approach in analyzing the different factors that contributed to the execution of fraud.

Fraud Diamond is an extension of the Fraud Triangle, a model that is used to explain the factors that lead to a higher risk of fraud.[24] The three elements of a fraud triangle are pressure, opportunity and rationalization. The fraud diamond model adds the capability aspect to the fraud triangle model to demonstrate that if a fraud perpetrator does not have the ability to recognize the above three factors, the fraud will not happen.[25]

The cases are analyzed using the fraud diamond framework, instead of the fraud triangle framework, to emphasize and hone in on the specific features of the fraud preparators that allowed them to commit the frauds. This approach is used so that specific recommendations on preventing such frauds in the future can be provided.

---

[24] "The Fraud Triangle." National Whistleblower Center, accessed May 17, 2025. https://www.whistleblowers.org/fraud-triangle/.

[25] David T. Wolfe CPA and Dana R. Hermanson PhD, "The Fraud Diamond: Considering the Four Elements of Fraud," *The CPA Journal*, May 2024, https://www.cpajournal.com/2024/05/01/the-fraud-diamond-considering-the-four-elements-of-fraud/.

4.3) Elements of Fraud Diamond

This section explains the four factors of the fraud diamond in detail.

1. ***Opportunity***

   Any factors that pave the way for fraud perpetrators to be able to commit fraud is considered opportunity. The opportunity can be a result of weak processes that open the door for fraud.[26]

2. ***Pressure/Motivation***

   This refers to any factors, monetary or non-monetary, that encourage a person to perpetuate a fraud. The personal life and the psychological state of a perpetrator may play a significant rule in influencing this factor.

3. ***Rationalization***

   Rationalization refers to how a fraud perpetrator convinces themselves that it is acceptable to commit fraud. This can include denial, excuses or justification of the actions, among other things. Similar to pressure/motivation, this factor is also mainly related to the internal state of the perpetrator.

4. ***Capability***

   This factor recognizes that even if presented with the above three elements, a person will not commit fraud if he does not have the capability to recognize that there is an opportunity that can be exploited to commit fraud. This factor takes into account the specific traits and abilities of the fraud perpetrator.

[26] Ibid.

4.4) Other Considerations

Given that the focus of this paper is to recommend strategies to enhance governance in the cryptocurrency industry – primarily addressing external factors – a limited analysis has been performed on the motivation and rationalization areas. While the external governance strategies may have a minor impact on Rationalization and Pressure/Motivation, these two elements are largely influenced by the internal factors, as opposed to external. Hence, a more detailed analysis is performed on the Opportunity and Capability aspects to identify the prevalent external factors that result in cryptocurrency-related scams and to explore how such risks can be mitigated through regulatory measures.

5) Analysis of Cases

5.1) QuadrigaCX

a) QuadrigaCX: Summary

QuadrigaCX (Quadriga) was a Canadian cryptocurrency exchange that collapsed in 2019 after the death of its founder, Gerald Cotton. Per Ontario Securities Commission's (OSC) report on Quadriga, when the exchange collapsed and filed for creditor protection, over 76,000 clients were owed a combined $215 million CAD in assets and Quadriga's platform users had lost at least $169 million CAD.[27]

b) QuadrigaCX: Background

Quadriga was a cryptocurrency exchange platform, founded by Gerald Cotton and Michael Patryn in British Colombia in December 2013, at the time when cryptocurrency industry was at its' peak. The platform facilitated the buying, selling and trading of cryptocurrencies. Due to the growing popularity of cryptocurrency during this time, the platform got a lot of traction. The clients were able to use the platform to conduct trade and Quadriga was able to earn revenues by charging a percentage as fees on transactions that happened. Bitcoin was the major cryptocurrency that was traded on this platform, while Canadian dollar was the other major asset that was traded on this platform.[28]

---

[27] "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," *Ontario Securities Commission,* April 14, 2020, pg. 3, https://www.osc.ca/quadrigacxreport/web/files/QuadrigaCX-A-Review-by-Staff-of-the-Ontario-Securities-Commission.pdf.

[28] Ibid., pg. 9-10.

In December 2018, Cotton died while on a trip to India. Initially, after the death of Cotton, the immediate concern was that he was the only person with access to the passwords of the cold wallets of the virtual assets. This meant that without the passwords, these assets could not be accessed and were forever lost. However, a detailed investigation by the OSC revealed that this was not the case and Quadriga was indeed operating like a Ponzi scheme.[29]

c) QuadrigaCX: Fraud Scheme

During their investigation, OSC found that Gerald Cotton had multiple fake accounts on the platform, with either fake fiat currency or crypto assets balances. With these fake balances, Cotton engaged in real transactions with other customers on the platform. Additionally, the real crypto assets were moved off the Quadriga's platform on other crypto assets trading platform and Cotton engaged in trading them on the other platforms.[30] The trading losses incurred by Cotton on these other platforms resulted in a short-fall of assets that Quadriga had. In the event that Quadriga customers wanted to withdraw money, the deposits from other customers were used, an example of a classic Ponzi scheme. Per OSC's report, in its final months, Quadriga had almost no available assets and was operating like a "revolving door"—new client deposits were immediately re-routed to fund other clients' withdrawals.[31]

[29] Ibid., pg. 3.

[30] Ibid., pg. 14-15.

[31] Ibid., pg. 3-4.

d) QuadrigaCX: Fraud Diamond Perspective

i) Opportunity:

- The lack of any internal controls presented an opportunity for this fraud to occur, as Quadriga operated without having any proper internal controls over its operations.[32] Specifically, it can be pinpointed to lack of below controls:
    - The lack of internal controls around who has access to the wallet's passwords led to Cotton having the ultimate sole custody of the underlying assets. Due to the lack of security measures, Cotton was able to engage in fake trades using customers funds without any trouble.
    - The lack of internal controls around how the customers assets were to be held and safeguarded while they were on the platform allowed Cotton to move the funds as he saw fit. When trades occurred on Quadriga's platform, customer accounts were adjusted to reflect either the fiat currency balance or the cryptocurrency balance. However, the customer did not immediately get control/ownership of the crypto asset, which meant that the crypto assets that the customers would see on their account were not "theirs". In fact, they were what the customer could claim against Quadriga.[33] This meant that Quadriga was in charge of maintaining the custody of customer assets, but the lack of any proper controls around this process allowed Cotton to misuse customers' funds for other purposes.

[32] Ibid., pg. 7.

[33] Ibid., pg. 12.

- The lack of controls around the segregation of assets, as Quadriga did not maintain any boundaries between its own and customers' assets.[34] The comingling of funds led to putting the customers funds at risk, without their consent.
- The lack of proper bookkeeping or records[35] created an opportunity for Cotton to misrepresent the true financial position of Quadriga, giving him an opportunity to continue using customer funds as he wanted.

- There was a lack of internal governance and oversight.[36] Specifically, the following factors evidence the lack of governance:
  - All of the company's directors, other than Cotton resigned in 2016.[37] This is an indicator that after 2016, Cotton had full control of Quadriga and there was nobody to question Cotton's decisions, showing a lack of governance, oversight and accountability at Quadriga.
  - Another interesting factor to note is that the co-founder, Micheal Patryn, appeared to have a history of unethical activities. Per OSC's report, "Patryn had been convicted in 2005 in the United States of conspiracy to transfer identification documents in relation to an online money-laundering service under his prior name, Omar Dhanani."[38] This fact gives an indicator of what

[34] Ibid., pg. 14.

[35] Ibid., pg. 15.

[36] Ibid., pg. 3.

[37] Norton Rose Fulbright, "Quadriga Bankruptcy: C$190 Million May Have Turned into Digital Dust," *International Restructuring Newswire*, July 2019, https://www.nortonrosefulbright.com/en/knowledge/publications/168bc350/quadriga-bankruptcy.

[38] "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," pg. 9.

the tone at the top may have looked like, further demonstrating that Quadriga lacked appropriate corporate governance.

- The overall lack of any regulatory oversight gave an opportunity to perpetuate this fraud as well. Specifically:
    - As the platform was not regulated, Quadriga was able to make false claims without any detection. For example, as per Quadriga's website, Quadriga claimed to its' customers that it employs advanced security measures.[39] The lack of any measures or regulatory oversight to detect such false claims gave Quadriga an opportunity to lie to and defraud its' customers. Similarly, due to lack of any regulatory oversight, the fake trades that happened on the platform were not detected.
    - Per an article published in 2015 in Bitcoin Magazine that explored how Quadriga was planning on becoming a public entity in Canada, it was mentioned that "It will not, however, be trading in the United States, nor will it accept American investors at this time. The company is adopting a wait-and-see attitude for the moment until there is further regulation clarity south of the border."[40] This comment is an indicator of how the lack of regulations in Canada gave Cotton the confidence to perpetuate this fraud

[39] "About," QuadrigaCX, Archived March 17, 2015 at https://web.archive.org/web/20150317061558/https://www.quadrigacx.com/about.

[40] Christie Harkin, "Breaking: Canadian Exchange QuadrigaCX to Become World's First Publicly Traded Bitcoin Exchange," *Bitcoin Magazine*, March 3, 2015, https://bitcoinmagazine.com/business/breaking-canadian-exchange-quadrigacx-become-worlds-first-publicly-traded-bitcoin-exchange-1425421352.

- The widespread enthusiasm and interest in cryptocurrency drew customers to Quadriga's trading platform,[41] creating an opportunity for Cotton to misuse their funds for his personal benefit. Furthermore, the lack of awareness among the people who used Quadriga gave Cotton an opportunity to exploit their trust. One of the victims of the fraud, Tong Zou in the documentary to Netflix said "I guess I trusted (Quadriga) a lot…I did some research on Reddit. They said: 'Oh it's going to take a while but you always get your money. It's not a scam'."[42] The OSC report also identified that many clients "approached Quadriga from a perspective of trust and believed there were safeguards in place similar to those applicable to regulated financial institutions."[43] This lack of knowledge and awareness among the customers led to this fraud since if the customers had been more knowledgeable regarding crypto trading platforms or risks associated with them, they may have not placed so many assets for a longer period of time in the platform.

ii) Capability:

- Quadriga was not registered with any securities regulator[44] due to the absence of any regulations or guidelines at this time regarding registration requirements for cryptocurrency exchanges. This meant that no regulator was overseeing its'

[41] "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," pg. 10.

[42] David Mercer, "Man lost £500,000 life savings in crypto exchange scam after trader died with password to funds," *Sky News*, March 30, 2022, https://news.sky.com/story/man-lost-500-000-life-savings-in-crypto-exchange-scam-after-trader-died-with-password-to-funds-12577397

[43] "QuadrigaCX: A Review by Staff of the Ontario Securities Commission," pg. 10.

[44] Ibid., pg. 30.

business operations. This gave Cotton the capability to engage in trading with the customer funds, without their permission.

- Cotton was in sole control of Quadriga's operations, as he was the only director of business and had control over the fiat and crypto assets.[45] Having this full control gave him the capability to commit this fraud.

iii) Motivation:

- The prospect of earning significant profits from the trading may have been the main motivation to engage in this scheme. However, as the scheme only unravelled after Cotton had died, there is no information available to analyze or comment on what exactly motivated him to commit this fraud.

iv) Rationalization:

- Similar to above, we may never be able to get answer to some questions like how Cotton rationalized this fraud. A potential rationalization might be the classic "borrowing" justification, i.e. the assets were used to engage in trading on other platforms but the profit earned from that trading would have been returned to the original customers. However, this remains purely speculative and may never be definitely answered.

[45] Ibid., pg. 10.

5.2) FTX

a) FTX: Summary

Within the US, FTX has been one of the biggest cryptocurrency-related scandals in recent years. FTX was a cryptocurrency exchange that filed for bankruptcy in 2022. The CEO of FTX, Samuel Bankman, was sentenced to 25 years in prison and $11 billion in penalties for the fraud.[46] According to the US Department of Justice, SBF defrauded FTX investors of more than $1.7 billion and defrauded the lenders of Alameda Research of more than $1.3 billion.[47]

b) FTX: Background

FTX Trading Ltd. was an international cryptocurrency exchange that was founded in 2019 by Samuel Bankman-Fried (SBF), Gary Wang, and Nishad Singh. Before FTX was founded, SBF was also involved in co-founding Alameda Research LLC., which was a cryptocurrency trading firm that managed and traded digital assets.[48] Customers were able to have accounts of FTX platform, and were able to trade cryptocurrency on it. During 2019, FTX also launched their own token "FTT".[49]

---

[46] U.S. Department of Justice, Office of Public Affairs, "Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes," March 28, 2024, https://www.justice.gov/archives/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes.

[47] Ibid.

[48] U.S. Securities and Exchange Commission, "Complaint, SEC v. Samuel Bankman-Fried, No. 22-cv-1050." S.D.N.Y., filed Dec. 13, 2022, para. 13-14, https://www.sec.gov/files/litigation/complaints/2023/comp25616.pdf.

[49] BDO Canada, "A complex scheme: The rise and demise of FTX" *BDO Canada*, accessed May 31, 2025, https://www.bdo.ca/insights/fraud-deconstructed-ftx-cryptocurrency.

FTX was able to quickly rise to growth due to cryptocurrency being a hot industry, as well as having a marketing strategy with endorsements from celebrities. For example, in 2022, Larry David appeared in a Super Bowl FTX commercial,[50] and in 2021, FTX were able to purchase the rights to name Miami Heat Arena, the FTX Arena.[51]

During 2022, an article was published by CoinDesk, a media outlet that specifically covers cryptocurrency industry, that noted that majority of Alameda's $14.6 billion of assets, consisted of FTT token.[52] This raised concerns because it showed that Alameda was heavily reliant upon FTT, which led to concerns about liquidity and solvency of Alameda. This was further fueled by announcement of Binance's CEO, Changpeng Zhao (CZ), about liquidating their investment of $580 million in FTT tokens.[53] This triggered the selloff of FTT, where customers started to withdraw their investment in FTT and leaving FTX in a liquidity crisis. There was a minor relief to FTX, as Binance reached a deal to acquire FTX, however, the deal was later cancelled by Binance after "…corporate due diligence, as well as the latest news reports regarding mishandled customer funds and alleged US agency

[50] "FTX Super Bowl Don't Miss Out with Larry David," YouTube, February 14, 2022, https://www.youtube.com/watch?v=hWMnbJJpeZc.

[51] Cheyenne Ligon, "Miami HEAT Arena Balks at FTX Naming Rights, Ending 19-Year Deal Early," *CoinDesk*, November 11, 2022, https://www.coindesk.com/business/2022/11/12/miami-heat-arena-balks-at-ftx-naming-rights-ending-19-year-deal-early/

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

[53] Max Zahn, "A Timeline of Cryptocurrency Exchange FTX's Historic Collapse," *ABC News*, March 28, 2024, https://abcnews.go.com/Business/timeline-cryptocurrency-exchange-ftxs-historic-collapse/story?id=93337035.

investigations…"[54]. Eventually, as a result of not being able to meet customers' withdrawal requests, both FTX and Alameda filed for bankruptcy in November 2022.[55]

c) FTX: Fraud Scheme

In their complaint, the Securities and Exchange Commission alleged that SBF engaged in a scheme to defraud the investors of FTX by diverting the customers' deposits in FTX to Alameda and using the investors' money to make undisclosed investments and using it for personal use. FTX provided misleading information to their investors, including claims that the customer funds were kept separate and safely and were not being used by FTX. These claims were found to be untrue as the customers funds were channeled to Alameda for various purposes, either directly by telling customers to deposit funds in Alameda's bank accounts or by the way of having special features on the FTX platform that allowed Alameda to obtain funds from FTX.[56] John J. Ray III (Ray) was appointed as the CEO of FTX after its collapse to lead FTX's restructuring efforts.[57]

[54] Binance (@binance). "As a result of corporate due diligence, as well as the latest news reports regarding mishandled customer funds and alleged US agency investigations, we have decided that we will not pursue the potential acquisition of http://FTX.com." *Twitter (now X),* November 9, 2022. https://x.com/binance/status/1590449161069268992.

[55] "Complaint, SEC v. Samuel Bankman-Fried, No. 22-cv-10501," para. 5.

[56] Ibid., para. 32.

[57] John J. Ray III, "Declaration in Support of Chapter 11 Petitions and First Day Pleadings, FTX Trading Ltd., et al., Case No. 22-11068 (JTD)", U.S. Bankruptcy Court for the District of Delaware, November 17, 2022, para. 1, https://s3.documentcloud.org/documents/23310507/ftx-bankruptcy-filing-john-j-ray-iii.pdf

d) FTX: Fraud Diamond Perspective

i) Opportunity:

- The lack of internal controls at FTX provided a huge opportunity for this fraud to occur. After John J. Ray III was appointed CEO, in his declaration in support of Chapter 11 bankruptcy filing, Ray mentioned that "Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here"[58]. Specifically, the following lack of internal controls were identified:
    - Lack of cash management procedures. For example, there was lack of controls around the cash disbursement procedures. In his declaration, Ray noted that "For example, employees of the FTX Group submitted payment requests through an on-line 'chat' platform where a disparate group of supervisors approved disbursements by responding with personalized emojis".[59] The declaration also notes that the corporate funds of FTX were used to make personal purchases by employees and advisors.[60] This further gave FTX an opportunity to comingle funds.
    - There was a lack of centralized control of cash and a lack of accurate list of bank accounts and signatories.[61] Due to a lack of an accurate tracking of cash, there was no tracking of customer funds, which gave FTX the opportunity to comingle customer funds with Almeda. Additionally, this

[58] Ibid., para. 5.

[59] Ibid., para. 62.

[60] Ibid., para. 63.

[61] Ibid., para. 50.

also meant that FTX did not keep track of the cash balances required to meet customers' withdrawal requests, eventually leading to the liquidity crisis.

  - There was a lack of record keeping and security related to the digital assets.[62] This gave an opportunity to commit this fraud and allowed Alameda to move the funds from FTX freely.

- The lack of regulations in the cryptocurrency industry allowed FTX to comingle customer funds with Alameda. The deposits by FTX customers were deposited into bank accounts that were controlled by Alameda.[63] However, this was not flagged by any regulator, primarily because majority of FTX entities were not regulated. The following are examples of things that could have been identified if the regulations were stringent:
  - It was revealed in Nishad Singh's testimony that he created a custom software code that allowed Alameda to have an unlimited line of credit with FTX. [64]
  - None of the FTX external auditors provided an opinion on the internal controls, as FTX was not required to comply with certain provisions of Sarbanes-Oxley Act of 2002 (SOX), which would have ensured stronger

[62] Ibid., para. 65.

[63] "Complaint, SEC v. Samuel Bankman-Fried, No. 22-cv-10501," para. 32.

[64] Securities and Exchange Commission, "Complaint: Securities and Exchange Commission v. Nishad Singh, Civil Action No. 23-cv-1691," U.S. District Court for the Southern District of New York, February 28, 2023, para. 60. https://www.sec.gov/files/litigation/complaints/2023/comp25652.pdf.

internal controls at FTX.[65] Hence, FTX got away with limited to no internal controls.

- FTX made a number of claims on its websites that its' customers relied on but were later proven to be false. There was no monitoring of these claims and FTX could openly lie to customers.[66] For example, FTX claims related to customer deposits being held in custody and segregated from its own funds were made on Terms of Conditions and public documents.[67] No regulatory body identified if the claims made by FTX to the customers were valid or not, providing it another opportunity to defraud customers.
- Overall, there was a lack of corporate governance at FTX. In his declaration, John J, Ray specifically mentioned that many entities in the FTX Group never had board meetings.[68] Board meetings are a key corporate governance tools that allows for stakeholders to be able to decide upon the strategic direction of a company. This just shows one aspect of lack of corporate governance. By having an overall lack of corporate governance, FTX had the opportunity to use customer funds as they wished, leading to the downfall of the company. Another example of lack of

[65] "The IIA Calls Upon Congress to Require Cryptocurrency Exchanges Operating in the U.S. to Strengthen Corporate Governance," *The Institute of Internal Auditors*, December 5, 2022, https://www.theiia.org/en/content/communications/press-releases/2022/december/the-iia-calls-upon-congress-to-require-cryptocurrency-exchanges/.

[66] "Complaint, SEC v. Samuel Bankman-Fried, No. 22-cv-10501," para. 28.

[67] Ibid., para. 48-49.

[68] "Declaration in Support of Chapter 11 Petitions and First Day Pleadings, FTX Trading Ltd., et al., Case No. 22-11068 (JTD)," para. 46.

corporate governance is that there was no discussion around the liquidity and solvency risk posed by the lending practices of Alameda and FTX.

- There was a lack of trustworthy financial information, which meant that Alameda's borrowings from FTX were not properly accounted for, [69] and as a result no tracking of how much funds have been borrowed occurred. This further gave the opportunity to comingle funds, leading to the eventual fall of FTX.

ii) Capability:

- Due to his capacity as the co-founder of Alameda, as well as due to his holdings in FTX and Alameda entities, SBF was the ultimate controller of all of these entities. He was the ultimate decision-maker at Alameda, even after other individuals were appointed as co-CEOs in 2021.[70] Having the ultimate decision-making power meant that the lines between the corporate entities were blurred and gave SBF the capability to easily comingle the customers deposits with Alameda.
- In his declaration, John J,. Ray specifically mentioned that there was concentration of control in a very small group of people.[71] This led to the group making decisions in their own best interests and not necessarily to maximize the value for all stakeholders. This power gave them the capability to exploit the weaknesses in the internal controls.

---

[69] "Complaint, SEC v. Samuel Bankman-Fried, No. 22-cv-10501.", para. 51.

[70] Ibid., para.18.

[71] "Declaration in Support of Chapter 11 Petitions and First Day Pleadings, FTX Trading Ltd., et al., Case No. 22-11068 (JTD)," para. 5.

- The co-founders of FTX controlled access of the digital assets of the main businesses in the FTX Group.[72] This gave them the capability to have control over the assets and move them freely.

iii) Motivation:

- As in most embezzlement cases, the motivation behind these actions appears to stem from personal gain and self-interest. Peter Easton, an accounting professor at University of Notre Dame who testified regarding the collapse of FTX, corroborated in his testimony that the customer funds were spent for investments, real estate, political donations, and charity.[73]

iv) Rationalization:

- Some of the interviews of SBF clearly show a "denial of responsibility" rationalization where the fraud perpetrator maintains that he has been a victim of the situation. For example, in one interview with, SBF said "I didn't knowingly commingle funds…. But I wasn't trying to commingle funds."[74] This may suggest that there is a need for improved messaging regrading responsibilities of exchanges with regards to customers' deposits so that it is easier to hold them accountable.

---

[72] Ibid., para. 65.

[73] Jacquelyn Melinek, "FTX Misused Customer Funds, Accounting Expert Who Assisted in Enron Prosecution Testifies," *TechCrunch*, October 18, 2023, https://techcrunch.com/2023/10/18/ftx-misused-customer-funds-accounting-expert-who-assisted-in-enron-prosecution-testifies/

[74] New York Times Events, "Sam Bankman-Fried Interviewed Live About the Collapse of FTX," YouTube video, 9:38-10:06, November 30, 2022. https://www.youtube.com/watch?v=IyoGdwVIwWw

5.3) ezBtc

a) ezBtc: Summary

ezBTC was a crypto asset trading platform that was dissolved in 2022. In British Columbia Securities Commission (BCSC) Findings decision, dated November 27, 2024, the BCSC found that ezBtc and its founder, David Smillie, perpetrated a fraud resulting in a financial loss to the customers of $13 million.[75] In their decision, BCSC ordered Smillie and his company ezBTC to pay a total fine of $18.4 million for committing the fraud.[76]

b) ezBtc: Background

Per the BCSC Findings decision regarding ezBtc, 1081627 B.C. Ltd, operating as ezBtc, was a crypto asset trading platform that was incorporated in 2016 and dissolved in 2022. Per the corporate registry, David Smillie was the incorporator and sole director of ezBtc. ezBtc operated as a crypto asset exchange, allowing customers to trade cryptocurrency. Customers were able to open accounts on the platform and deposit either fiat currency or cryptocurrency to a wallet address that was held by ezBtc for the customer. Similar to other crypto exchanges, ezBtc charged a fee for deposits, withdrawals and trades

[75] British Columbia Securities Commission, "B.C.-based Crypto Trading Platform Defrauded Customers of $13 Million," *British Columbia Securities Commission*, August 12, 2024, https://www.bcsc.bc.ca/about/media-room/news-releases/2024/74-bc-based-crypto-trading-platform-defrauded-customers-of-13-million.

[76] Proctor, Jason, "B.C. crypto fraudster fined $18.4 million for gambling away clients' cash," *CBC News*, December 02, 2024, https://www.cbc.ca/news/canada/british-columbia/bitcoin-fraud-sanction-smillie-1.7399003.

conducted on the platform, which were revenues for ezBtc. If customers wanted to make a withdrawal, they could submit an online withdrawal form to the platform. [77]

c) ezBTC: Fraud Scheme

Upon receiving complaints that some customers have been unable to withdraw the funds or cryptocurrency from the platform, BCSC hired a forensic data analytics firm to investigate the exchange. The firm conducted an analysis of the cryptocurrency that was supposed to be kept in ezBtc' s cold storage and their investigation revealed that a majority of the assets were transferred to either Smillie's personal accounts or gambling websites.[78]

d) ezBTC: Fraud Diamond Perspective

i) Opportunity:

- Per the archived website of ezBTC, on January 15, 2018,[79] ezBTC claimed to customers "99% Cold Storage" and that "Your coins are safe". However, as later evidenced by BCSC investigation, these claims were not accurate.[80] The lack of any monitoring of the claims that were made by ezBTC allowed ezBtc to make fake

[77] British Columbia Securities Commission, "Re Smillie, 2024 BCSECCOM 348." August 7, 2024, para. 12-26, https://www.bcsc.bc.ca/-/media/PWS/New-Resources/Decision-and-Orders/Decisions/2024/2024-BCSECCOM-348.pdf.

[78] Ibid., para 27, 39-42.

[79] ezBtc, "Welcome to Canada's most innovative and personalized Digital Asset Exchange," archived January 15, 2018, Internet Archive Wayback Machine, https://web.archive.org/web/20180115205447/https://www.ezbtc.ca/

[80] "Re Smillie, 2024 BCSECCOM 348." August 7, 2024, para. 39-42.

or exaggerated promises to customers, attracting them to the platform and giving it an opportunity to defraud them.

- Similarly, per the archived website of ezBTC on January 15, 2018[81], ezBTC claimed that customers can "Save your Bitcoin and earn 9% in annual commission. Paid daily". There appears to have been no monitoring of if this claim was accurate or not.

ii) Capability:

- Smillie was able to misuse the customer funds as he was the sole director of ezBtc and the only authorized signatory of ezBtc' s bank accounts.[82] This meant that he was able to divert the customer funds for personal use without any hurdle.
- BCSC report found that the staff at ezBTC needed Smillie to move crypto assets from cold storage and that there was no other person at ezBTC who had the same level of authority and involvement as Smillie.[83] This meant that there was nobody to hold ezBTC accountable for the investors, giving him the capability to commit this fraud.

iii) Motivation:

- There has been a lack of available information that would allow to assess and make commentary on the underlying motivations for Smillie's actions.

---

[81] "Welcome to Canada's most innovative and personalized Digital Asset Exchange"

[82] "Re Smillie, 2024 BCSECCOM 348," para. 14.

[83] Ibid., para. 131.

iv) Rationalization:

- A “denial of facts” (perpetrator denying specific parts of the crime) and “denial of guilt” (perpetrator denying that an action is a crime) rationalization can be seen in this case again. Per BCSC Decision, “Smillie concedes that ezBtc was improperly managed and operated negligently, but denies that he or ezBtc perpetrated a fraud”.[84] This suggests that Smillie acknowledges that the actions committed by him were negligence and not right, however he did not accept them to be fraud. This suggests that the definitions of fraud should be expanded to explicitly encompass cryptocurrency-related schemes, which exploit regulatory gaps and weaknesses to evade accountability.
- The “borrowing” justification can also be seen. Per BCSC findings “Smillie asked us to infer that the crypto assets transferred to gambling websites were done on behalf of customers”.[85] This can imply that Smillie may have used the justification that these assets will be returned to customers eventually.

[84] Ibid., para. 95.

[85] Ibid., para. 120.

6) Key Findings

This section summarizes the key findings and patterns that emerge as common themes across the three cases analyzed above. These are as follows:

1. ***Lack of internal controls at the cryptocurrency exchanges***

   The above cases demonstrate that there was a lack of required internal controls, making it easier to perpetrate fraud. The absence of a comprehensive regulatory oversight contributed to an environment where these organizations were able to operate without any internal controls.

2. ***Lack of governance internally within the cryptocurrency exchanges***

   The organizations lacked proper governance structure, with control concentrated in the hands of a very small group—or in some cases, a single individual. This significantly increased the risk of fraud and made it easier for it to occur undetected. Similar to above, the absence of a strong regulatory governance led to an environment where these organizations were able to operate without having a proper governance structure in place.

3. ***Lack of education and awareness of the investors***

   It has been noted that the customers who used the above cryptocurrency exchanges were not fully aware of the operations and technicalities of how the cryptocurrency exchanges are operating, making it easier for the perpetrators to deceive the customers.

4. ***Denial rationalizations for crypto related crimes***

   Another interesting theme that emerges from the above cases is that the fraud perpetrators showed “denial of guilt”, “denial of facts” and “denial of

responsibility" rationalization, which may imply that these acts are not seen as fraud by the perpetrators.

5. ***Lack of industry regulations***

There is an overall lack of oversight and monitoring at the industry level, primarily due to ambiguity over which authorities hold the responsibility to regulate these entities. However, this area is constantly evolving as regulators draw lessons from past cases and are working to strengthen oversight. For example, in Canada, following the collapse and investigation of Quadriga, regulators introduced guidelines to govern these exchanges, as further discussed in Section 7. The following additional themes have been noted, which eventually stem from a lack of regulations:

a. ***Liquidity Issues***

Cryptocurrency exchanges have been noted to be at risk of having liquidity issues and facing a "bank run" i.e. a situation where customers want to withdraw their funds and there are not enough cash to meet the withdrawal request. Cryptocurrency exchanges are not meant to operate like banks by leveraging customer assets. Hence, absence of regulation in this area has led to this problem.

b. ***Lack of oversight over claims made by the cryptocurrency exchanges***

It has been noted that the fraud perpetrators made false claims to customers and were able to solicit investments from them. There were lack of regulatory oversight in place to detect or monitor whether the claims made by the perpetrators were true or not.

c. Comingling and lack of segregation of the customer funds

The fraud perpetrators comingled the customers deposits either with other corporations or for their personal use. As a result, customer funds were not safe at the exchanges, which resulted in eventual financial loss to customers.

7) Regulatory Landscape

7.1) Overview Of Section

Since the occurrence of major cryptocurrency exchange related fraud cases have been discovered, many regulations have come into effect in both the United States and Canada. The purpose of this section is to provide an overview of the current state of the regulatory landscape as it pertains to cryptocurrency exchanges. As the main discussion around regulating cryptocurrency exchanges is focused on whether they need to be regulated by the way of securities regulation, the below section looks at the specific securities landscape in Canada and the US, as well as what the specific cryptocurrency exchanges specific guidelines are.

7.2) Current Canadian Regulatory Landscape

Cryptocurrencies are not legal tender in Canada, which means that they are not issued or overseen by a central authority.[86] While cryptocurrencies are not regulated, the channels through which they are traded are regulated, mostly by the way of securities law due to the heightened risk posed to the investors by this asset class. This section specifically looks at the securities legislations that are applicable to cryptocurrencies and cryptocurrency trading platforms.

In Canada, securities regulation is under the responsibility of provincial and territorial regulators such that each province and territory have a securities regulator. Specifically, there are 13 local securities regulators in Canada. However, all of these regulators also fall under an umbrella organization called Canadian Securities Administrators (CSA) that aims to provide an overarching guidance and harmony in the ways the Canadian capital markets are regulated.

To address the debate around whether cryptocurrency platforms need to comply with the securities regulations, CSA, in collaboration with Canadian Investment Regulatory Organization (CIRO) issued guidance in March 2021 to stakeholders clarifying when the securities law will apply to them. This guidance is called "Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Staff Notice 21-329 Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements".[87]

---

[86] "Crypto Assets."

[87] Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, "Joint CSA/IIROC Staff Notice 21-329: Guidance for Crypto-Asset Trading Platforms: Compliance with

In summary, the notice provides guidance on how the securities regulations apply to crypto asset trading platforms. Per the guidance, the trading platforms need to evaluate the underlying substance of the asset to determine the applicable securities requirements. Specifically, guidance is provided for cryptocurrency trading platforms (CTPs) to determine if they operate as a Dealer Platforms or a Marketplace Platforms.

If a CTP only facilitates primary distribution of security tokens, and the interaction is only between the CTP and the customer (i.e. no interaction between customers), it is a dealer platform (Section 3 – Part a). In this case, the dealer platform would need to comply with the dealer registration requirement. If a CTP brings together different buyers and sellers to trade the crypto assets, it will be marketplace platform (Section 3 – Part b). In this case as well, the platforms must register with the securities regulator as a marketplace. In addition to above, platforms that are located outside of Canada but provide service to Canadians must also be registered to comply with the regulatory rules.

Overall, the above guidance provides more clarity to crypto assets trading platforms regarding the application of the current securities regulations. Being registered with the securities regulator will allow to mitigate many risks such as providing transparent, accurate and complete information to the investors, as well as enforcing the crypto platforms to have controls in place to protect the crypto assets. For example, for an exchange to be recognized under OSC, it needs to have a corporate governance structures, rules, policies, and financial viability among other things.[88]

Regulatory Requirements," March 29, 2021, https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/JointCSAIIROCNotice21-329(March29_2021).pdf.

[88] "Exchanges," Ontario Securities Commission, accessed May 17, 2025, https://www.osc.ca/en/industry/market-regulation/marketplaces/exchanges.

Additionally, to further protect the investors, CSA introduced a pre-registration undertaking in 2023 for platforms that are still in the process of obtaining registration. The goals of this pre-registration undertaking are for the CTPs to adhere to expectations regarding custody and segregation of crypto assets, a prohibition on offering margin, credit, or other forms of leverage to any Canadian client.[89] Additionally, the CTPs need to maintain a chief compliance officer and audited financial statements, as well as prohibiting risky services.[90]

[89] "Canadian Securities Regulators Strengthen Oversight, Enhance Expectations of Crypto Asset Trading Platforms Operating in Canada," Canadian Securities Administrators, February 22, 2023, https://www.securities-administrators.ca/news/canadian-securities-regulators-strengthen-oversight-enhance-expectations-of-crypto-asset-trading-platforms-operating-in-canada/.

[90] "Crypto Regulation and Illicit Finance in Canada," *TRM Labs*, April 29, 2025, https://www.trmlabs.com/resources/reports/crypto-regulation-and-illicit-finance-in-canada.

7.3) United States Regulatory Landscape

In the United States, similar to Canada, cryptocurrency is not legal tender and are not issued or overseen by a central authority. In the US, trading of crypto assets are regulated under many different agencies based on the nature of the underlying asset. It is important to note that there is no particular set of rules specific to crypto that have been developed. As a result, the extent of the regulation has been to provide guidance to businesses on how the current regulations apply to the crypto businesses.

In the US, there are two main federal bodies that are involved in regulating investments: the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). The SEC is a federal body that is responsible for regulating the securities market, while the CFTC is a federal regulatory body that oversees the derivatives market in US. While the SEC regulates at the federal level, each state in the US also has a local securities regulator. However, there are no state-specific derivatives market regulator.

In the US, much of the debate about cryptocurrency regulation pertains to whether they are classified as a security (regulated by SEC) or as a derivate (regulated by CFTC).[91] To clarify this, the SEC has provided guidance to the stakeholders that help them determine whether the crypto asset is a security. If the defined criteria is met, the asset is regulated as a security under the SEC regulations and the exchange is required to comply with certain

[91] Dragos Cernescu, "Regulating Crypto in a Post-FTX World – Initiatives and Timelines," *The Paypers*, March 20, 2023, https://thepaypers.com/expert-opinion/regulating-crypto-in-a-post-ftx-world-initiatives-and-timelines--1261881

requirements. For example, if an exchange is registered under SEC, it is required to establish measures for investor protection and upholding market integrity.[92]

Similarly, if the crypto asset is classified as a commodity, it will be regulated by the CFTC. Being regulated by the CFTC will allow for the crypto exchanges to operate with integrity and without any manipulative or disruptive market activity, in accordance with the CFTC's mission.[93]

Overall, similar to Canada, the regulations in the US around cryptocurrency are focused on providing guidance to how the current laws and regulations apply to the cryptocurrency exchanges.

[92] "Statutes and Regulations," U.S. Securities and Exchange Commission, accessed May 17, 2025, https://www.sec.gov/rules-regulations/statutes-regulations.

[93] Commodity Futures Trading Commission. "About the CFTC." Accessed May 31, 2025. https://www.cftc.gov/About/AboutTheCommission.

7.4) Gaps In Current Frameworks

Based on the above discussion, the following are some of the overarching gaps noted in the current regulatory landscape as it pertains to cryptocurrency exchanges:

- Regulators in both Canada and US, have not introduced new regulations for cryptocurrency exchange platforms, but have concentrated on providing guidance on how the existing regulations apply to them. This leads to the possibility that specific risks that may only be relevant to cryptocurrency exchanges will be left unaddressed. For example, although the pre-registration undertaking in Canada addresses some cryptocurrency exchange specific concerns (like segregating client assets), by not focusing on providing crypto specific rules, some risks can be left unaddressed. For example, as identified in European Securities and Markets Authority's (ESMA) Advice on Initial Coin Offerings and Crypto-Assets,[94] the specific risks associated with cryptocurrency exchange platforms can include risks that are specific to the underlying technology like cybersecurity risks, risks related to territoriality and jurisdiction due to the distributed nature of blockchain and risks related to centralized platforms taking control of customers assets unlike traditional trading platforms.
- The guidance and regulations that have been introduced by the regulators has been reactive, rather than proactive. For example, in Canada, the Notice 21-329 Guidance for Crypto-Asset Trading Platforms was issued after the Quadriga

[94] European Securities and Markets Authority, "Advice on Initial Coin Offerings and Crypto-Assets", January 9, 2019. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

scandal. If regulators do not take a proactive approach to managing the fraud risk in the industry, the industry will continue to suffer from such frauds.

- The lack of any one specified framework leads to ambiguity, which can lead to higher instances of non-compliance. The guidance issued by CSA and IROC attempts to regulate CTPs by educating them to register with a regulator, however, as evidenced by the example of ezBtc, there still appears to be a lack of monitoring regrading the CTPs, resulting in the scandal. This is similar in US as well, where there are many different bodies that may have jurisdiction over the cryptocurrency exchanges, which may lead to confusion among businesses regarding which rules to comply with. This can also increase the operational costs of a business, leading to inhibiting innovation and growth.

8) Fraud Risk Management Framework

8.1) Background

An effective fraud risk framework provides guiding principles to detect prevalent fraud risks and developing strategies to deal with those risks in an attempt to prevent fraud. Under COSO/ACFE 2016 Fraud Risk Management Guide,[95] there are five main components of a fraud risk management framework – fraud governance, fraud risk assessment, preventative and detective fraud controls, fraud investigations and ongoing monitoring. The following is a detailed explanation of these components:

1. ***Fraud Risk Governance***

   Fraud Risk Governance relates to establishing corporate governance and an internal control environment for an organization. This includes establishing a tone at the top that communicates to all the stakeholders that there is no tolerance for fraudulent behavior in an effort to enforce a culture of high integrity, as well as maintaining fraud governance policies.

2. ***Fraud Risk Assessment***

   Fraud Risk Assessment component involves an ongoing and regular assessment of potential fraud schemes and the likelihood of their occurrence so that current controls can be evaluated and actions can be taken to address fraud risks completely. It is critical for this process be ongoing and regular so that any new risks identified can be addressed in the entity's fraud risk management program.

[95] "Fraud Risk Management Guide – Executive Summary,"

3. ***Fraud Controls***

   This component involves establishing specific controls to prevent (preventative fraud controls) and detect the fraudulent events from happening (detective fraud controls).

4. ***Fraud Investigations***

   The fourth component of a fraud risk management framework is establishing specific activities to take action against fraudulent activities when they are reported or discovered. It is crucial to have these in place so that any fraudulent events identified can be investigated in a proper and timely manner.

5. ***Monitoring***

   Monitoring involves establishing an ongoing monitoring program of the fraud risk management program that monitors if all the above-mentioned factors are present and effective.

8.2) Framework for Cryptocurrency Industry

While fraud risk management frameworks are typically used by an organization to detect and respond to fraud risk internally, this framework is specifically written as a guidance for the industry regulators. As the fraud cases analyzed earlier in this paper related to fraudulent organizations (they were not victims of fraud, but the perpetrators) this framework is written for the regulators to assist in minimizing the risk of such fraudulent crypto organizations in the industry.

This framework aims to provides broad principles that can be used by regulators to ensure effective regulations are in place to respond to and detecting fraud risk. Based on the insights from the above analysis of cases, this fraud risk framework aims to address the factors that can be controlled and provides guidelines on preventive measures. The next section lists out the recommendations and measures that can taken to ensure that such frauds and scandals can be avoided for the future. Please also refer to ***Figure D*** included in Appendix for the mapping of the below proposed recommendations to the Key Findings in Section 6.

8.3) Recommendations: Fraud Risk Governance

1. ***Defined structure and responsibilities to maintain effective oversight***

   A very important factor in establishing fraud risk governance is to establish structure, with defined roles and responsibilities. Having defined roles and structure ensures that there is no ambiguity for the stakeholders, as well as it ensures that the responsible body can be held accountable. An effective oversight over crypto-related matters cannot be established if there is ambiguity among the regulatory bodies regarding whose role it is to regulate the crypto exchanges.

   Recommendation 1*: Regulators can consider forming a crypto-specific body that maintains oversight over the crypto-related exchanges. As discussed earlier, since cryptocurrency exchanges are the common platform for cryptocurrency trading, it is important that these are governed.*

   It is critical that one body can be defined so that there is no ambiguity and effective oversight can be implemented. The specific authority and responsibilities of this body can be further specified, and this body can be responsible for developing rules that are specific for the crypto exchanges and provide further guidelines.

   It is worth noting that that this role can also be taken up by the existing regulatory bodies. However, the current regulatory bodies were established before the widespread emergence of cryptocurrency and their regulations may not be suited to regulating trading of cryptocurrency. This misalignment can contribute to their limited proactivity in asserting clear regulatory authority over the space. Hence, it may be more beneficial to form a separate body for governance of cryptocurrency exchanges.

2. ***Clear guidelines for industry participants***

Having clear guidelines is another important aspect of fraud risk governance as it can provide clear guidance to the participants on what regulations need to be followed, overall resulting in more clarity. Without clear guidelines, the ambiguity can lead to non-compliance.

Recommendation 2*: Regulators (or the specified body) needs to establish clear guidelines for crypto related organizations so that the exchanges are aware of which body they need to register with and what rules they need to comply with. This will be an important step in removing any ambiguity among the industry participants.*

3. ***Whistleblower line***

Setting a whistleblower line is an important factor in fraud risk governance, as it shows commitment to prevent fraud by encouraging the people with first hand experience of fraud to report it.

Recommendation 3: *Regulators should establish an anonymous whistleblower line to be able to empower the industry stakeholders to report any suspicious behavior regarding any business. It is worth noting that traditional regulatory bodies, including securities regulators, already have such measures in place.*

More importantly, an efficient process must be maintained to react to such reports on a timely basis, as discussed in Section 8.6.

4. ***Code of conduct or best practices***

Establishing a code of conduct that outlines the best practices or clearly outlines the unethical practices ensures that stakeholders are aware of proper practices in an organization. Additionally, mandating declarations by the relevant parties ensures their commitment to adhering to the specified code of conduct.

Recommendation 4*: Regulators should establish a code of conduct/best practices document that clearly highlights the unethical or unacceptable behaviors. Additionally, it should be mandatory for the exchanges to adhere to those specified practices by the way of declarations. This can be particularly useful in inhibiting the "denial of crime" rationalization, as well as encourage organizations to have internal controls and proper governance in place.*

5. ***Fraud risk management guidance***

Establishing an overall fraud risk management policy is a critical component as it provides a defined framework to manage the fraud risk.

Recommendation 5: *Regulators should consider developing a crypto-specific fraud risk management guidance that specifies, among other things, the below key components for the industry participants:*

- *What constitutes fraud specifically in the context of crypto exchanges. One observation from the analyzed cases is that fraud perpetrators may use the "denial of guilt" or "denial of crime" rationalization. This may be avoided if regulators can develop and communicate clear guidelines to public on what constitutes a fraud, specifically in the context of cryptocurrency industry.*

Although this will be the same as what is considered fraud in conventional context, adapting the terminology to incorporate cryptocurrency fraud can communicate the message more effectively.

- *What the consequences of the fraud are and define the specific fraud penalties. Explicit messaging on penalties can encourage organizations to be more proactive in implementing proper controls and governance.*
- *Specific procedures listed for clients and investors to follow if they believe that something is a fraud.*

6. Tone at the top

Setting an overall ethical tone at the top is a critical element of fraud risk governance. This tone at the top is set by effective action by management against fraud, as well as by the actions of management. In the context of an entire industry, regulators need to set an effective tone at the top to prevent fraudulent exchanges from happening.

Recommendation 6*: Regulators need to be proactive in communicating to the stakeholders what actions they are taking to combat fraud. This will create an expectation of honest behavior from the industry participants and also encourage them to improve their internal governance.*

8.4) Recommendations: Fraud Risk Assessment

1. An effective fraud risk assessment

An effective fraud risk management program is not possible without an effective fraud risk assessment. A fraud risk assessment ensures that an organization is able to identify the potential fraud risks, assess the likelihood and significance of those risks to manage priority and ultimately determine measures to control those risks. Having an effective fraud risk assessment ensures that an organization is able to be proactive and prevent fraud from happening.

Recommendation 7*: Regulators (or specified body) need to be involved in performing regular fraud risk assessments for cryptocurrency exchanges to identity the prevalent crypto related fraud risks and their common indicators. Additionally, these risks need to be assessed based on the likelihood of occurrence, as well as the significance of the risks so that they can be dealt with in a priority manner. This risk assessment needs to be focused on the crypto industry so that specific crypto risks can be identified.*

Recommendation 8*: For the above recommendation to be successful, regulators need to educated on the new crypto related topics so they can provide proactive guidelines to relevant stakeholders. For example, in the case of Quadriga (which was not registered with any securities regulator), regulators published guidelines after the discovery of fraud. An effective fraud risk assessment will allow the regulators to be proactive instead.*

8.5) Control Activities

To run an effective fraud risk management program, regulators need to design, implement and monitor effective controls that address the specific risks identified in the fraud risk assessment step. While the Governance and Fraud Risk Assessment stages offer recommendations on how regulatory bodies can influence and evaluate industry practices, the Control Activities stage identifies specific controls that should be present within regulated entities, based on the key findings from the cases analyzed earlier in this paper. The following are some examples of preventive and detective fraud controls that can be imposed by regulators to ensure that risk factors that appear prevalent in crypto exchanges are addressed.

8.5.1) Recommendations: Preventative Fraud Controls

1. An observation from the above cases has been that the crypto exchanges faced liquidity problems, resulting in a run for cash by the customers.

   Recommendation 9: *Regulators should consider enforcing the requirement of a liquidity risk management program for crypto exchanges. For example, they can consider defining the percentage of assets that an entity can have in cryptocurrency. This will lead to these organizations having stricter focus on meeting customer demand of redemption, and to prevent a run.*

   Recommendation 10: *Another key control that can be placed is that a reserve should be maintained by crypto exchanges, similar to a bank, to ensure that it can meet the customers' withdrawal requests. The reserve to be maintained should be indicative of*

the risk of withdrawals by customers. Regulators can consider mandating auditing of such reserves to ensure compliance.

2. In the above cases, once the crypto exchange was bankrupt, the investors lost money as there was no insurance. For financial institutions in Canada, Canada Deposit Insurance Corporation (CDIC) insures eligible deposits, so that even if banks run out of money, the customer's money will be protected. Given that a crypto exchange is similar to a bank in this regard, this can offer further customer protection.

   Recommendation 11: *Regulators can consider imposing a requirement of a deposit insurance for crypto exchanges to prevent or mitigate the losses in cases of bankruptcy. Currently in Canada, cryptocurrencies are not eligible for this under CDIC.*[96]

3. In the case of Quadriga, the passwords to the crypto wallets were lost resulting in loss of the funds. This is a risk that is faced by every crypto exchange where if the private key to a crypto wallet is lost, the funds are lost forever.

   Recommendation 12: *Regulators should consider imposing requirements of specific disaster recovery procedures, that outline procedures that crypto platforms can follow in the case of losing the wallets or keys to the wallets. There should be specified processes developed by the exchanges as a backup to access the wallets. This may also entail having specific requirements for business continuity planning and multiple signatures for the storage wallets.*

[96] Canada Deposit Insurance Corporation, "What's Covered," *CDIC*, accessed May 24, 2025, https://www.cdic.ca/depositors/whats-covered/.

4. Another theme noted from the above cases is the lack of awareness among customers regarding the management of investments by the exchanges. This is in line with the general trend observed within the public as well. Per the Crypto Asset Survey 2023, Canadians who buy crypto conducted research primarily based on information from friends, family and colleagues (34%), followed by social media influencers (23%).[97] This lack of education makes the investors more vulnerable to fraud.

   Recommendation 13: *Education and awareness among investors regarding the operations of crypto exchanges and common red flags can be an important preventive tool that allows investors to be more mindful of their investment decisions.*

5. In the above cases, we can see a pattern of use of customer funds by the company for other purposes, resulting in comingling of funds and eventually a loss of those customer funds.

   Recommendation 14: *Regulators should enforce specific segregation of customer funds practices on these exchanges. This can be potentially implemented by requiring an exchange to show effective segregation of customer fund procedures as part of the registration, and annual declarations to be in compliance with the rules set.*

6. We also note that the crypto exchanges made many claims to customers that later turned out to be untrue. The false claims by the exchanges were able to give investors a false impression of the security of their investments, effectively misleading them.

[97] Ontario Securities Commission, "Crypto-Asset Survey 2023." November 29, 2023, 9, https://www.osc.ca/sites/default/files/2023-12/inv-research_20231129_crypto-asset-survey-2023.pdf.

7. ***Recommendation 15:*** *Regulators may consider having specific oversight regulations for marketing claims for crypto exchanges. This would be similar to how it is done for financial product advertising.*[98] *For example, there can be more stringent requirements to disclose the risk that is associated with the exchanges.*

8. In the case of FTX, we noted that the primary asset making up the balance sheet of FTX was the crypto assets, leading to the solvency crisis.

   Recommendation 16: *Regulators should impose requirements of having actual assets back-up the value of the exchange. Alternatively, regulations can focus on preventing exchanges from having the cryptocurrency they trade, as their sole asset backing, since this creates a dependency on a value that is generated by the exchange itself.*

9. The wallet addresses were controlled by one person, who maintained exclusive control over the transactions. This results in a risk that one person has exclusive control over transactions, and concentrates the control in one person.

   Recommendation 17: *Regulators should enforce specific rules regarding which individuals have the responsibilities and authority over the wallets, as they are the key underlying asset for the crypto exchanges. For example, they can consider specifying that a third-party with no direct affiliation to cryptocurrency exchange could be given the authority over wallets, under a strict and enforceable contract, to prevent abuse of customer funds.*

[98] Dana Lawrence, "Marketing Compliance in Financial Services," *Wolters Kluwer*, December 4, 2024, https://www.wolterskluwer.com/en/expert-insights/marketing-compliance-in-financial-services.

8.5.2) Recommendations: Detective Fraud Controls

1. We note that there was a lack of transparency by the crypto exchanges regarding the activities undertaken by them. In addition to this, there was an overall lack of internal controls, record keeping and corporate governance at the exchanges which the customers were unaware about this.

   Recommendation 18: *Regulators should consider mandating financial and internal control audits for crypto exchanges to ensure compliance with the rules set, including having sufficient internal control, bookkeeping and governance structure. Additionally, this should include the exchanges providing disclosure to customers about the crypto investments and other factors. Although an audit only provides reasonable assurance, it will be an effective tool in ensuring that exchanges are not blatantly lying to customers and it will also encourage the implementation of internal controls and governance.*

2. We note that in the above cases, customer funds were being diverted for other purposes, most notably in the case of ezBtc, where such transfers happened immediately after the customer funds were deposited on the platform. [99]

   Recommendation 19: *Blockchain analytics tools should be utilized by regulators and auditors to audit and monitor the cryptocurrency exchanges. Utilizing such tools will be critical in identifying if customers funds are being misused by the platform.*

[99] "Re Smillie, 2024 BCSECCOM 348," para. 41.

8.6) Recommendations: Fraud Investigations

1. *Defined investigation protocol*

Establishing fraud investigation and response protocol is a critical component of fraud investigations as it allows for investigations to happen in an efficient manner, that can mitigate losses.

Recommendation 20: *Regulators should implement specific crypto fraud investigation and response protocol that includes the following, among other thing:*

- *Clear structure and established authority for the investigation team*
- *Have a dedicated fraud investigation team, that have the required skills and experience to conduct crypto specific investigations. This includes experience with blockchain transaction analytics tool to trace transactions, as well as digital forensic experts who can extract and retain digital evidence, in a way that is appropriate for court proceedings.*
- *Develop procedures to stop the bleeding i.e. take immediate steps to try to recover the crypto assets when the allegations of fraud are first discovered.*

2. *Communicate investigation findings*

A theme that has been noted is that many same issues are noted across the cases analyzed, even after some cases have been heavily prosecuted.

Recommendation 21: *Regulators should communicate the investigation results to the industry stakeholders so that they are aware of any issues applicable to them. This will ensure that the fraud perpetrators cannot use a "denial of guilt" rationalization to justify their actions.*

8.7) Recommendations: Monitoring

1. Frequent monitoring

It is critical for monitoring to occur at an appropriate frequency so that any changes that are required to the program can be made in a timely manner.

Recommendation 22: *Regulators should consistently monitor the steps performed above to ensure that their fraud risk management program meets the ongoing risks in the crypto space. As the crypto space is constantly evolving, it is critical that regulators are constantly updating their program as well. Regulators should also consider incorporating the lessons from ongoing crypto investigations into the program so that the repeated instances can be avoided.*

9) Applicability to IFAs

Up until this point, the focus of this paper has been to provide guiding principles and recommendations to prevent the possibility of fraud in the cryptocurrency space in the future. This section explores the various roles that forensic accountants can play in this space to assist in building a more fraud resistant cryptocurrency ecosystem.

Investigative and Forensic Accountants (IFAs) are professionals who integrate their accounting knowledge and investigation skills together, to effectively assist in areas of litigation support and accounting investigations.[100] These roles extent beyond fraud investigations, as IFAs' experience with dealing with fraud uniquely positions them to identify areas of weaknesses where fraud can occur, as well as makes them capable to identify common fraud schemes and the indicators of such scheme. As such, IFAs are extremely relevant in the context of developing a fraud management framework for the cryptocurrency space. Their roles can extend beyond fraud investigations to risk assessments, education, and policy and regulations development. Specifically:

- As discussed above, the educational and practical experience of an IFA allows them to have the skill set to properly identify the fraud risks, gaps in the internal controls, as well as other red flags. As evidenced by the above cases analyzed, the fraud perpetrators commonly use the same fraud scheme, such as perpetrating a Ponzi scheme, but with new tools. Hence, IFAs can utilize their experience and knowledge of fraud schemes to effectively identify the fraud scheme that can be utilized by perpetrators on a proactive basis and take measures to address them

[100] "Forensic Accountant." Association of Certified Fraud Examiners, accessed May 17, 2025. https://www.acfe.com/career/career-paths/career-path-accounting/career-path-detail-forensic-accountant.

before any damage occurs. These skills can be used by IFAs to conduct a thorough fraud risk assessment for the cryptocurrency space and identify specific fraud risk factors.

- Similarly, IFAs can recommend the controls that can be implemented at the industry level to mitigate the identified risks. IFAs through their experience have a deep understanding of common reasons for failures of controls, as well as the common vulnerabilities.
- IFAs can play a critical role in fraud investigations in the cryptocurrency space, as they can be well versed with blockchain analytics tools that can be used to trace cryptocurrency transactions.
- Aside from conducting fraud investigations, IFAs can provide insight to the internal investigation team regarding best practices to perform an investigation in a timely manner.
- Additionally, IFAs can play a crucial role in educating the relevant stakeholders regarding the types of investment frauds prevalent in the cryptocurrency space, to enhance investor education, enabling them to make sound investment decisions and enhancing the integrity of the cryptocurrency market. This can make an overall ethical “tone at the top” at industry level.
- IFAs can also play an important role in developing the ethical polices and code of conduct for the industry. Such a code can clearly communicate to the stakeholders what would include fraudulent behavior and can reinforce ethical behavior from the industry participants.

- Lastly, IFAs can play a critical role within the monitoring component as well. IFAs can perform holistic review of the policies and provide recommendations on their sufficiency in preventing the fraudulent schemes. Such a review that is performed on a regular basis can be an effective tool in addressing the changes that are occurring in the crypto space and evolving the policy/regulatory structure on a timely basis.

Overall, the unique skill set of IFAs can be used by the industry to make the cryptocurrency industry less susceptible to fraud, enhance investor confidence, and encourage more innovation.

10) Conclusion

Over the past few years, interest in the cryptocurrency space has surged dramatically. This growing interest, while fostering technological innovation, has also given rise to novel forms of crime. While many view cryptocurrency as inherently secure due to its foundation in blockchain technology, this is a misleading perception and recognising that no financial system is immune to fraud is the first step in developing a more resilient cryptocurrency ecosystem.

The current state of the regulations in the cryptocurrency space is not preventive, but rather reactive. The response of the regulators is mostly reactive as regulations in the cryptocurrency space are primarily a result of the frauds that have been discovered. Regulators need to be proactive in implementing regulations that foresee the potential risks of fraud in the space, so that the frauds can be avoided.

The industry can benefit from following a structured fraud management program as it provides overarching principles that can be followed by the regulators to enhance the effectiveness of their governance. As the cryptocurrency ecosystem continues evolving with emerging technology and new features, it is crucial for regulators to adopt a flexible approach that allows for regular updates to the regulatory framework. The principles-based recommendations provided in this paper aims to provide such an adaptive guidance.

11) Limitations & Other Research Questions

This section outlines some limitations of this research paper, as well as other research topics that can provide further valuable insight into fraud prevention strategies for cryptocurrency ecosystem.

Due to the limited timeframe within which this research paper has been written, the analysis has been limited. Additionally, although a fraud diamond framework has been used, as reinforced throughout this paper, there have been limited insights and commentary made on the rationalization and motivation aspects of the frauds. Lastly, the regulatory landscape for the cryptocurrency industry has been constantly evolving with many moving pieces. As such, there have been new updates and regulatory changes that did not exist at the time of the specific case and/or this analysis, but have since been introduced by the regulatory bodies.

This research paper has been limited to three specific cryptocurrency exchanges fraud cases that have been analyzed. There can be additional insights derived if further cases are analyzed. For example, the recommendations provided in the fraud control activities section of this paper are limited to those findings derived from the cases analyzed. If further cases are analyzed, we can get insight into further themes and risks that crypto exchanges face and different control recommendations may be applicable to address those risks.

There may be additional insights that can be developed if the cases are analyzed from a Fraud Pentagon or Fraud Hexagon lens. Such an analysis can explore other factors

such as arrogance and justification of the fraud perpetrators and may allow us to explore other measures to prevent such frauds from happening in the future.

There may be further insights that can be derived from analyzing the fraud cases in different jurisdictions. For example, Bermuda, Australia, and Panama are examples of countries that are becoming crypto-friendly[101] and have developed frameworks and guidelines for companies to follow. There is value in exploring what the impact of these guidelines have been on the fraudulent activity and what, if any, frauds have been noted despite these regulatory restrictions.

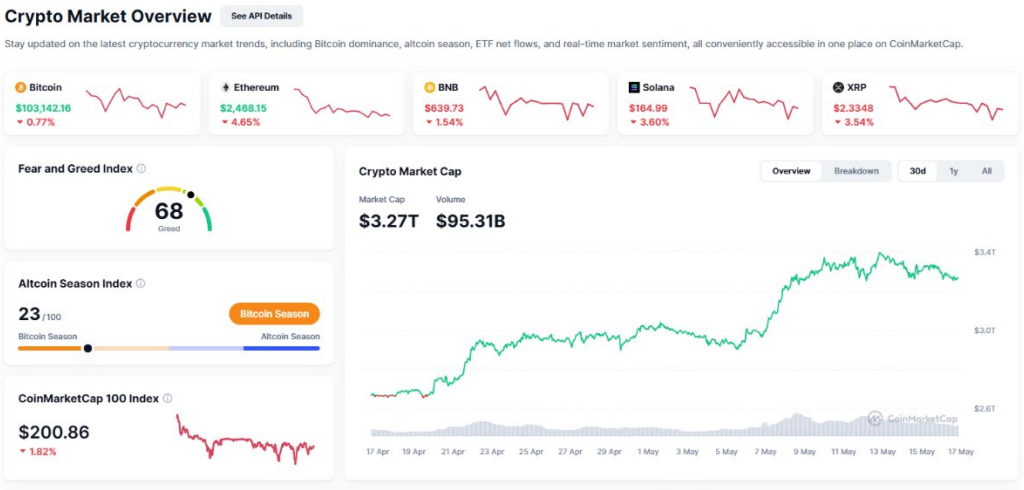
Overall, the cryptocurrency space is constantly evolving and further research into the above listed topics can provide further insights that can be helpful in regulating this space, while maintaining flexibility and innovation.

[101] Alisa Abramova, "The Top 10 Crypto-Friendly Countries (2025)," *Sumsub*, February 11, 2025, https://sumsub.com/blog/crypto-friendly-countries/.

12) Appendix

Figure A[102]*: Partial screenshot of the global cryptocurrency market cap charts webpage from CoinGecko, an independent cryptocurrency data aggregator, as of May 17, 2025*

Figure B.1[103]***:*** *Screenshot of the Crypto Market Overview webpage from CoinMarketCap, a cryptocurrency data and insights provider, as of May 17, 2025.*



[102] "Global Cryptocurrency Market Cap Charts."

[103] "Cryptocurrency Charts & Market Data."

Figure B.2[104]*: Screenshot of the Cryptocurrencies tracked webpage from CoinMarketCap, a cryptocurrency data and insights provider, as of May 17, 2025.*

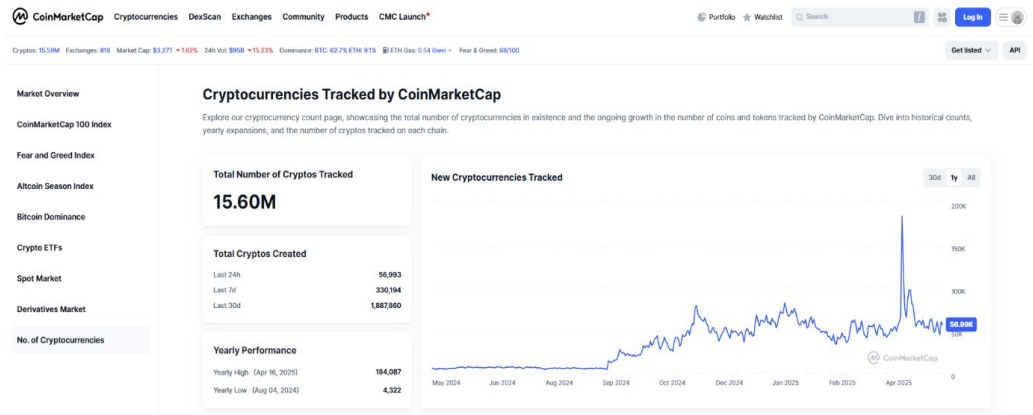


Figure C[105]*: Screenshot of the original post by user "dwdollar" on January 15, 2010 regarding launching a bitcoin exchange*

[104] "Number of Cryptocurrencies Tracked." CoinMarketCap. Accessed May 17, 2025, https://coinmarketcap.com/charts/number-of-cryptocurrencies-tracked/.

[105] "New Exchange (Bitcoin Market)."

Figure D: *Mapping of proposed Recommendations in Section 8.3 – 8.7 to Key Findings in Section 6.*

Key Finding	Recommendation
Key Finding 1: Lack of Internal Controls	Recommendation 4
	Recommendation 5
	Recommendation 12
	Recommendation 17
	Recommendation 18
Key Finding 2: Lack of Internal Governance	Recommendation 4
	Recommendation 5
	Recommendation 6
	Recommendation 18
Key Finding 3: Lack of Industry Regulations	Recommendation 1
	Recommendation 2
	Recommendation 3
	Recommendation 4
	Recommendation 5
	Recommendation 7
	Recommendation 8
	Recommendation 20
	Recommendation 22
Key Finding 4: Lack of Investor Education/Awareness	Recommendation 13
Key Finding 5: Denial of Guilt	Recommendation 4
	Recommendation 5
	Recommendation 21
Key Finding 6: Liquidity Issues	Recommendation 9
	Recommendation 10
	Recommendation 11
	Recommendation 16
Key Finding 7: Lack of Oversight over Specific Claims	Recommendation 15
	Recommendation 19
Key Finding 8: Comingling & Lack of Funds Segregation	Recommendation 14

13) Bibliography

1. "1. Who Regulates Banking and Financial Services in Your Jurisdiction? Global Financial Services Regulatory Guide." *Baker McKenzie Resource Hub*. Accessed May 17, 2025. https://resourcehub.bakermckenzie.com/en/resources/global-financial-services-regulatory-guide/north-america/canada/topics/who-regulates-banking-and-financial-services-in-your-jurisdiction

2. Abramova, Alisa. "The Top 10 Crypto-Friendly Countries (2025)." *Sumsub*, February 11, 2025. https://sumsub.com/blog/crypto-friendly-countries/.

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

4. Amure, Tobi Opeyemi. "Hot Wallet vs. Cold Wallet: What's the Difference?" *Investopedia*. Updated April 21, 2024. https://www.investopedia.com/hot-wallet-vs-cold-wallet-7098461.

5. Anglejan-Chatillon, Alix d', Ramandeep K. Grewal, Éric Lévesque, and Antonin Lapointe. "Blockchain & Cryptocurrency Regulation 2025: Canada." *Stikeman Elliott LLP*. Accessed May 17, 2025. https://stikeman.com/-/media/files/kh-general/blockchain-and-cryptocurrency-2025-stikeman-elliott-canada.ashx.

6. Association of Certified Fraud Examiners. "Forensic Accountant." Accessed May 17, 2025. https://www.acfe.com/career/career-paths/career-path-accounting/career-path-detail-forensic-accountant.

7. Bathgate, Benjamin M., Jessica Stansfield and Natalie Bravo. "Cryptocurrency 'Regulation by Enforcement' as Hot as Ever: What's to Come from Securities Regulators in 2024?" *WeirFoulds LLP*, February 5, 2024. https://www.weirfoulds.com/cryptocurrency-regulation-by-enforcement-as-hot-as-ever-whats-to-come-from-securities-regulators-in-2024.

8. BDO Canada. "A Complex Scheme: The Rise and Demise of FTX." *BDO Canada*, Accessed May 17, 2025. https://www.bdo.ca/insights/fraud-deconstructed-ftx-cryptocurrency.

9. Bharadwaj, Chirag. "Custodial Vs. Non-Custodial Wallets: Understanding the Difference Points." *Appinventiv*, February 19, 2025. https://appinventiv.com/blog/custodial-vs-non-custodial-wallets/.

10. Binance (@binance). “As a result of corporate due diligence, as well as the latest news reports regarding mishandled customer funds and alleged US agency investigations, we have decided that we will not pursue the potential acquisition of http://FTX.com.” *Twitter (now X),* November 9, 2022. https://x.com/binance/status/1590449161069268992.

11. Bitcoin Forum. “New Exchange (Bitcoin Market)”. Accessed on May 17, 2025. https://bitcointalk.org/index.php?topic=20.0.

12. Board of the International Organization of Securities Commissions. “Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms.” *International Organization of Securities Commissions,* February 2020. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf.

13. British Columbia Securities Commission. "B.C.-based Crypto Trading Platform Defrauded Customers of $13 Million." *British Columbia Securities Commission*, August 12, 2024. https://www.bcsc.bc.ca/about/media-room/news-releases/2024/74-bc-based-crypto-trading-platform-defrauded-customers-of-13-million.

14. British Colombia Securities Commission. “Cease Trade Order 2016 BCSECCOM 69”. *Sedarplus*, March 8, 2016. https://www.sedarplus.ca/csa-party/viewInstance/view.html?id=0c11f8b7998bcd96b075c3ea16dca2e70e8952019b83c214&_timestamp=701955346059362.

15. British Columbia Securities Commission. “Re Smillie. 2024 BCSECCOM 348”. August 7, 2024. https://www.bcsc.bc.ca/-/media/PWS/New-Resources/Decision-and-Orders/Decisions/2024/2024-BCSECCOM-348.pdf.

16. Canada Deposit Insurance Corporation. “What’s Covered.” *CDIC*. Accessed May 24, 2025. https://www.cdic.ca/depositors/whats-covered/.

17. Canadian Securities Administrators and Alberta Securities Commission. “Investor’s Guide: Cryptocurrencies.” Accessed May 17, 2025. https://www.securities-administrators.ca/wp-content/uploads/2022/08/CSA-Investors-Guide-Cryptocurrencies.pdf.

18. Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada. “Joint CSA/IIROC Staff Notice 21-329: Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements”. March 29, 2021. https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/JointCSAIIROCNotice21-329(March29_2021).pdf.

19. Canadian Securities Administrators. "Canadian Securities Regulators Strengthen Oversight, Enhance Expectations of Crypto Asset Trading Platforms Operating in Canada." *Canadian Securities Administrators*, February 22, 2023. https://www.securities-administrators.ca/news/canadian-securities-regulators-strengthen-oversight-enhance-expectations-of-crypto-asset-trading-platforms-operating-in-canada/.

20. Cernescu, Dragos. "Regulating Crypto in a Post-FTX World – Initiatives and Timelines." *The Paypers*, March 20, 2023. https://thepaypers.com/expert-opinion/regulating-crypto-in-a-post-ftx-world-initiatives-and-timelines--1261881.

21. Chambers, Richard. "On The Frontlines: The Hard Lessons of FTX." *AuditBoard*. January 25, 2023. https://auditboard.com/blog/on-the-frontlines-the-hard-lessons-of-ftx

22. CoinGecko. "Global Cryptocurrency Market Cap Charts." Accessed May 17, 2025. https://www.coingecko.com/en/global-charts.

23. CoinLedger. "Centralized vs Decentralized Crypto Exchanges: What's the Difference?". Accessed May 24, 2025. https://coinledger.io/learn/centralized-vs-decentralized-crypto-exchanges.

24. CoinMarketCap. "Cryptocurrency Charts & Market Data." Accessed May 17, 2025, https://coinmarketcap.com/charts.

25. CoinMarketCap. "Number of Cryptocurrencies Tracked." Accessed May 17, 2025. https://coinmarketcap.com/charts/number-of-cryptocurrencies-tracked/.

26. Committee of Sponsoring Organizations of the Treadway Commission. "Fraud Risk Management Guide – Executive Summary." *Committee of Sponsoring Organizations of the Treadway Commission,* September 2016. https://www.coso.org/_files/ugd/3059fc_02c01fde6552479196535bcfee8ea60e.pdf.

27. Commodity Futures Trading Commission. "About the CFTC." Accessed May 31, 2025. https://www.cftc.gov/About/AboutTheCommission.

28. Commodity Futures Trading Commission. "The CFTC's Role in Monitoring Virtual Currencies." Accessed May 17, 2025. URL not available.

29. Cryptohopper. "What was the First Crypto Exchange". Accessed on May 17, 2025. https://www.cryptohopper.com/blog/what-was-the-first-crypto-exchange-449

30. “Crypto Regulation and Illicit Finance in Canada.” *TRM Labs*, April 29, 2025. https://www.trmlabs.com/resources/reports/crypto-regulation-and-illicit-finance-in-canada.

31. Delfabbro, Paul, Daniel L. King, and Jennifer Williams. “The Psychology of Cryptocurrency Trading: Risk and Protective Factors.” *Journal of Behavioral Addictions* 10, no. 2 (June 19, 2021): 201–7. https://doi.org/10.1556/2006.2021.00037

32. Edwards, John. “Bitcoin's Price History.” *Investopedia*, January 23, 2025. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.

33. European Securities and Markets Authority. “Advice on Initial Coin Offerings and Crypto-Assets.” January 9, 2019. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

34. ezBtc. “Welcome to Canada's most innovative and personalized Digital Asset Exchange.” Archived January 15, 2018. Internet Archive Wayback Machine. https://web.archive.org/web/20180115205447/https://www.ezbtc.ca/.

35. Financial Consumer Agency of Canada. “Crypto assets”. *Government of Canada*, December 16, 2024. https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html

36. FINRA.org. “Crypto Assets - Risks,” Accessed May 17, 2025. https://www.finra.org/investors/investing/investment-products/crypto-assets/risks

37. “FTX Super Bowl Don't Miss Out with Larry David.” YouTube. February 14, 2022. https://www.youtube.com/watch?v=hWMnbJJpeZc.

38. Fuke, Daniel, Julie He. “FTX Aftermath from a Canadian Securities Law Perspective.” *Fasken*, January 5, 2023. https://www.fasken.com/en/knowledge/2023/01/ftx-aftermath-from-a-canadian-securities-law-perspective

39. Garnett, Allie Grace. “Centralized vs. decentralized crypto exchanges – which should you choose?” *Britannica Money.* Accessed May 24, 2025, https://www.britannica.com/money/centralized-vs-decentralized-crypto.

40. “Global Crypto Policy Review & Outlook 2023/24.” *TRM Labs*. Accessed May 17, 2025. https://uploads-ssl.webflow.com/6082dc5b67056233213587a4/6597f1953f85d02072d9a5e2_TRM%20Global%20Crypto%20Policy%20Review%20%26%20Outlook%202023-24.pdf.

41. “Global Crypto Policy Review & Outlook 2024/25.” *TRM Labs*, December 12, 2024. https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/679bc2e15f2c7d48854bdd21_TRM_Global-Crypto-Policy-Review-Outlook-2024-25.pdf.

42. Harkin, Christie. "Breaking: Canadian Exchange QuadrigaCX to Become World’s First Publicly Traded Bitcoin Exchange." *Bitcoin Magazine*, March 3, 2015. https://bitcoinmagazine.com/business/breaking-canadian-exchange-quadrigacx-become-worlds-first-publicly-traded-bitcoin-exchange-1425421352.

43. Hermanson, Dana R., PhD, and David T. Wolfe CPA. “ICYMI | The Fraud Diamond.” *The CPA Journal*, October 2024. https://www.cpajournal.com/2024/10/30/the-fraud-diamond-2/

44. Hetler, Amanda. “FTX Scam Explained: Everything You Need to Know.” *TechTarget,* January 2, 2025. https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know.

45. Investopedia Team. “Cryptocurrency Wallet: What It Is, How It Works, Types, and Security”. *Investopedia*, November 25, 2024. https://www.investopedia.com/terms/b/bitcoin-wallet.asp

46. “Is Owning a Crypto Exchange Profitable? An In-Depth Analysis” *WeAlwin*, Accessed May17, 2025. https://www.alwin.io/crypto-exchange-business-profitable

47. Jimenez, Alison. “Cryptocurrency Traceability: Unraveling underlying assumptions.” *Dynamic Securities Analytics, Inc.,* February 1, 2024. https://securitiesanalytics.com/cryptocurrency_traceability

48. Kovalenko, Nazar. “Balancing Innovation and Regulation: The Future of Cryptocurrency in the Global Financial Landscape.” *Assas Legal Innovation Journal,* January 12, 2025. https://assaslegalinnovation.com/2025/01/12/balancing-innovation-and-regulation-the-future-of-cryptocurrency-in-the-global-financial-landscape

49. KPMG. “The Collapse of FTX: Lessons and Implications for Stakeholders in the Crypto Industry.” *KPMG*. November 2022. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2022/11/the-collapse-of-ftx.pdf

50. Lawrence, Dana. "Marketing Compliance in Financial Services." *Wolters Kluwer*, December 4, 2024. https://www.wolterskluwer.com/en/expert-insights/marketing-compliance-in-financial-services.

51. Ligon, Cheyenne. “Miami HEAT Arena Balks at FTX Naming Rights, Ending 19-Year Deal Early.” *CoinDesk*, November 11, 2022. https://www.coindesk.com/business/2022/11/12/miami-heat-arena-balks-at-ftx-naming-rights-ending-19-year-deal-early/.

52. McCarty, Becky. “Considerations for Fraud Risk Assessment: COSO Principle 8.” *Linford & Company LLP*, August 24, 2024. https://linfordco.com/blog/fraud-risk-assessment-coso-principle-8

53. Melinek, Jacquelyn. "FTX Misused Customer Funds, Accounting Expert Who Assisted in Enron Prosecution Testifies." *TechCrunch*, October 18, 2023. https://techcrunch.com/2023/10/18/ftx-misused-customer-funds-accounting-expert-who-assisted-in-enron-prosecution-testifies/

54. Mercer, David. "Man Lost £500,000 life savings in crypto exchange scam after Trader died with password to funds." *Sky News*, March 30, 2022. https://news.sky.com/story/man-lost-500-000-life-savings-in-crypto-exchange-scam-after-trader-died-with-password-to-funds-12577397.

55. Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System”. *Bitcoin*. October 31, 2008. https://bitcoin.org/bitcoin.pdf

56. Nallapaneni, Dhiraj. “The FTX Collapse: A Complete Guide.” *CoinLedger*.” Accessed May 17, 2025. https://coinledger.io/learn/the-ftx-collapse

57. New York Times Events. “Sam Bankman-Fried Interviewed Live About the Collapse of FTX.” *YouTube video,* November 30, 2022. https://www.youtube.com/watch?v=IyoGdwVIwWw

58. Norton Rose Fulbright. “Quadriga Bankruptcy: C$190 Million May Have Turned into Digital Dust.” *International Restructuring Newswire*, July 2019. https://www.nortonrosefulbright.com/en/knowledge/publications/168bc350/quadriga-bankruptcy.

59. Oliverethan. “How Cryptocurrency Exchanges Generate Revenue: A Look Into 2025.” *Nasscom Community,* January 27, 2025. https://community.nasscom.in/communities/blockchain/how-cryptocurrency-exchanges-generate-revenue-look-2025.

60. Oliverethan. “What Was the First Crypto Exchange?” *Nasscom Community,* November 9, 2024. https://community.nasscom.in/communities/blockchain/what-was-first-crypto-exchange.

61. Ontario Securities Commission. “Crypto-Asset Survey 2023.” *Ontario Securities Commission,* November 29, 2023. https://www.osc.ca/sites/default/files/2023-12/inv-research_20231129_crypto-asset-survey-2023.pdf.

62. Ontario Securities Commission. "Exchanges." Accessed May 17, 2025. https://www.osc.ca/en/industry/market-regulation/marketplaces/exchanges.

63. Ontario Securities Commission. “QuadrigaCX: A Review by Staff of the Ontario Securities Commission.” *Ontario Securities Commission,* April 14, 2020. https://www.osc.ca/quadrigacxreport/web/files/QuadrigaCX-A-Review-by-Staff-of-the-Ontario-Securities-Commission.pdf

64. “Overview Report – Quadriga CX” Assessed May 17, 2025. https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/246%20-%20Overview%20Report%20-%20Quadriga%20CX%20Final.pdf

65. Proctor, Jason. "B.C. crypto fraudster fined $18.4 million for gambling away clients' cash." *CBC News*, December 02, 2024. https://www.cbc.ca/news/canada/british-columbia/bitcoin-fraud-sanction-smillie-1.7399003.

66. “Proposed Legislative Text for Enhancing Corporate Governance at Cryptocurrency Exchanges.” *The Institute of Internal Auditors,* May 4, 2023. https://www.theiia.org/globalassets/site/iia-letter-to-congress_5.4.23.pdf

67. PwC. “Making Sense of Bitcoin, Cryptocurrency and Blockchain.” Assessed May 17, 2025. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

68. Q.Ai. "What Happened To Crypto Giant FTX? A Detailed Summary of What We Actually Know Here." *Forbes*, December 13, 2022. https://www.forbes.com/sites/qai/2022/12/13/what-happened-to-crypto-giant-ftx-a-detailed-summary-of-what-we-actually-know-here/

69. QuadrigaCX. "About." Archived March 17, 2015. Accessed May 17, 2025. https://web.archive.org/web/20150317061558/https://www.quadrigacx.com/about.

70. “QuadrigaCX – Blockchain and Bankruptcy.” *Appleby*, May 15, 2019. https://www.applebyglobal.com/publications/quadrigacx-blockchain-and-bankruptcy.

71. Ray, John J. "Declaration in Support of Chapter 11 Petitions and First Day Pleadings. FTX Trading Ltd., et al., Case No. 22-11068 (JTD)." *U.S. Bankruptcy Court for the District of Delaware*, November 17, 2022. https://s3.documentcloud.org/documents/23310507/ftx-bankruptcy-filing-john-j-ray-iii.pdf.

72. Reserve Bank of Australia. "Digital Currencies". Assessed May 17, 2025. https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html

73. Singh, Neetu, and Anjali. "Integration of Forensic Accounting with Corporate Governance: A Weapon to Combat Financial Frauds." *World Journal of Advanced Research and Reviews* 16, no. 3 (December 2022): 299–307. https://doi.org/10.30574/wjarr.2022.16.3.1323

74. Sbf. "FTX Pre-Mortem Overview." *SBF's Substack*, January 12, 2023. https://sambf.substack.com/p/ftx-pre-mortem-overview

75. Securities and Exchange Commission. "Complaint: Securities and Exchange Commission v. Nishad Singh, Civil Action No. 23-cv-1691." U.S. District Court for the Southern District of New York, February 28, 2023. https://www.sec.gov/files/litigation/complaints/2023/comp25652.pdf.

76. Shishkanov, Alexander. "How Do Crypto Exchanges Make Money? – An In-Depth Look" *B2Broker*, November 11, 2024. https://b2broker.com/news/how-do-crypto-exchanges-make-money-an-in-depth-look/

77. Siripurapu, Anshu, Noah Berman. "The Crypto Question: Bitcoin, Digital Dollars, and the Future of Money." *Council on Foreign Relations*, January 17, 2024. https://www.cfr.org/backgrounder/crypto-question-bitcoin-digital-dollars-and-future-money.

78. Skavysh, Vladimir, Jacob Sharples, Sofia Priazhkina and Salman H. Hasham. "Market Structure of Cryptoasset Exchanges: Introduction, Challenges and Emerging Trends." *Bank of Canada Staff Analytical Note* 2024. February 2, 2024. https://www.bankofcanada.ca/wp-content/uploads/2024/01/san2024-2.pdf

79. "The 2025 Crypto Crime Report*." Chainalysis,* February 2025. https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf.

80. "The Bitcoin Whitepaper Simply Explained." *Bitpanda*. Accessed May 17, 2025. https://www.bitpanda.com/academy/en/lessons/the-bitcoin-whitepaper-simply-explained/

81. “The Ever-Shifting Landscape of U.S. Crypto Regulation.” *O’Melveny,* October 18, 2024. https://www.omm.com/insights/alerts-publications/the-ever-shifting-landscape-of-us-crypto-regulation.

82. "The IIA Calls Upon Congress to Require Cryptocurrency Exchanges Operating in the U.S. to Strengthen Corporate Governance." *The Institute of Internal Auditors*, December 5, 2022. https://www.theiia.org/en/content/communications/press-releases/2022/december/the-iia-calls-upon-congress-to-require-cryptocurrency-exchanges/.

83. The National Whistleblower Center. “The Fraud Triangle.” Accessed May 17, 2025. https://www.whistleblowers.org/fraud-triangle/

84. U.S. Department of Justice, Office of Public Affairs, "Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes," March 28, 2024, https://www.justice.gov/archives/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes.

85. U.S. Securities and Exchange Commission. “Complaint, SEC v. Samuel Bankman-Fried. No. 22-cv-10501.” S.D.N.Y. Filed December 13, 2022. https://www.sec.gov/files/litigation/complaints/2023/comp25616.pdf

86. U.S. Securities and Exchange Commission. “Crypto Task Force.” Accessed May 15, 2025. https://www.sec.gov/about/crypto-task-force.

87. U.S. Securities and Exchange Commission. “Cyber, Crypto Assets And Emerging Technology.” Assessed May 17, 2025. https://www.sec.gov/about/divisions-offices/division-enforcement/cyber-crypto-assets-emerging-technology

88. U.S. Securities and Exchange Commission. "Statutes and Regulations." Accessed May 17, 2025. https://www.sec.gov/rules-regulations/statutes-regulations.

89. “What Is Cryptocurrency and How Does It Work?”. Kaspersky. Accessed May 17, 2025. https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

90. “What Is the Fraud Diamond? Explaining the Motivations for Fraud.” *McGowan.* August 8, 2024. https://www.mcgowanprofessional.com/resources/what-is-the-fraud-diamond-explaining-the-motivations-for-fraud/.

91. “Why You Can’t Trace Funds Through Services Using Blockchain Analysis (And Why You Don’t Need to Anyway).” *Chainalysis Blog*. October 9, 2020. https://www.chainalysis.com/blog/blockchain-analysis-trace-through-service-exchange/.

92. Wolfe, David T., and Dana R. Hermanson PhD. “The Fraud Diamond: Considering the Four Elements of Fraud.” *The CPA Journal*, May 2024. https://www.cpajournal.com/2024/05/01/the-fraud-diamond-considering-the-four-elements-of-fraud/

93. Woodbury, Richard. “Creditors of Fraudulent Cryptocurrency Platform QuadrigaCX Can Get 13% of Their Money Back.” *CBC*, May 16, 2023. https://www.cbc.ca/news/canada/nova-scotia/creditors-of-fraudulent-cryptocurrency-platform-quadrigacx-can-get-13-of-their-money-back-1.6845113

94. Yahoo Finance. "Bitcoin USD Price (BTC-USD) Historical Data." Accessed May 17, 2025. https://finance.yahoo.com/quote/BTC-USD/history/.

95. Zahn, Max. "A Timeline of Cryptocurrency Exchange FTX's Historic Collapse." *ABC News*, March 28, 2024. https://abcnews.go.com/Business/timeline-cryptocurrency-exchange-ftxs-historic-collapse/story?id=93337035

END