Impacts of Blockchain Technology on the IFA Profession and Lessons Learned: An IFA's Guide to Understanding the Landscape, Investigative Approaches and Crypto Crime

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program

University of Toronto

Prepared by Nada Mohammed

June 9, 2023

For Prof. Leonard Brooks

Abstract

This thesis aims to evaluate the impact of the crypto industry on the Investigative Forensic Accounting (IFA) profession and, in the process, shine a light on the notion that users in the ecosystem are protected through a veil of anonymity. The industry, hereinafter referred to as "the crypto ecosystem," has a complex and intricate nature which will be untangled in this paper. It also delves into analyzing crimes perpetrated in the crypto ecosystem and the behaviours of the relevant offenders. In addition, it discusses a sample of successful investigations along with the tools used to trace illicit funds and uncover perpetrators' identities. By doing so, this thesis aims to provide practical recommendations for current and future IFA professionals who wish to excel in the domain of this disruptive technology. Due to it being a relatively new technology, the IFA field may have somewhat overlooked the crypto industry, and this thesis aims to bridge that gap and neutralize the threat of the ecosystem's wide adoption.

The crypto ecosystem has many honest users who generally trade in digital assets as investments and genuinely believe in the ecosystem's efficacy and potential. On the other hand, many remain wary and doubtful of its legitimacy and believe it to be a large-scale scam. While individuals on both ends of the spectrum may raise worthwhile points, it is crucial to emphasize that this paper does not delve into the legitimacy of the crypto ecosystem as a concept or advocate for or against its implementation. However, given that the crypto ecosystem's utilization and acceptance are expected to grow, regardless of its legitimacy, this paper focuses on how IFAs can contemplate ways to adjust to it.

Acknowledgment

I am deeply appreciative of the individuals who have assisted me in researching and writing my thesis. A special thank you goes to my mentor, Amrit Dev, for her unwavering support and encouragement throughout the research process. Despite her busy role as a senior manager at KPMG Canada's Forensic practice, she was always willing to discuss my research topic of Blockchain technology, even prior to my request for her mentorship. Her guidance was invaluable in helping me clarify my thoughts and directing me toward the right and relevant sources of information. I am also grateful for her comments on earlier drafts of the thesis, which helped me strengthen and improve the coherence of my research paper. Her generosity, expertise, and passion for the topic have been a true blessing and have inspired me to work harder toward my goals.

Table of Contents

1. A CHAIN REACTION TO THE FINANCIAL CRISIS

The 2008 Great Recession, a crisis triggered by a surge of subprime mortgages, led to the inflation of the housing bubble, ultimately resulting in a severe economic downfall once the bubble exploded. While many believed that the root cause of the crisis was solely due to the collapse of the subprime mortgage market, further research has revealed that the underlying factors were much more multifaceted. The crisis largely stemmed from significant shortcomings in financial regulation, oversight of corporate governance and risk management at the various levels of financial institutions. In fact, the Financial Crisis Inquiry Commission concluded in its 2011 report that this crisis was avoidable. According to the Commission, "The crisis was the result of human action and inaction, not of Mother Nature or computer models gone haywire."[1] The report indicated that the writing was on the wall. Still, government regulators and investors with an unsaturated appetite for risk completely disregarded the signs of impending doom. This resulted in a failure to safeguard a critical system that plays an essential role in the overall economic well-being of society.[2] The Washington Post reported that the United States lost approximately $9.8 trillion in public wealth as the value of Americans' homes crashed, and their retirement accounts vanished.[3] Thus, creating a catalyst for the loss of trust in traditional financial institutions among the public.

[1] The Financial Crisis Inquiry Report (p. 18).
[2] Ibid., 1.
[3] Merle, R. (2018, September 10). *A guide to the financial crisis - 10 years later*. The Washington Post. https://www.washingtonpost.com/business/economy/a-guide-to-the-financial-crisis--10-years-later/2018/09/10/114b76ba-af10-11e8-a20b-5f4f84429666_story.html

For some, the Great Recession served as a warning about the perils of investing, risk and the potential hazards of placing complete faith in financial experts, institutions and governments. However, for others, namely, an individual or group known under the pseudonym "Satoshi Nakamoto," this event demonstrated the perfect example of why the public needs to embrace an alternative method of conducting transactions that eliminate the need for intermediaries altogether, including financial institutions and governments.

Satoshi Nakamoto issued the whitepaper introducing Bitcoin in 2008. The introduction of the “Crypto Currency” concept also came about as a general response to the limitations and weaknesses of the fiat currency, its perceived monopolization by governments and its capacity to abuse that power.[4] The key distinguishing quality of a cryptocurrency is that it was meant to be purely a peer-to-peer (P2P) system, as opposed to the traditional one, which necessitates the involvement of an intermediary or a trusted third party to facilitate a transaction.[5] In the whitepaper, Nakamoto argues that the while the traditional system is functional, it has intrinsic limitations. These constraints are a direct result of intermediaries mandating access to sensitive personal details of customers, imposing exorbitant fees to execute transactions and mitigate their liabilities, in addition to the typical delays in execution and the chance of potential fraud faced by consumers as a cost of doing business.[6] Nakamoto envisioned the solution to these issues in Bitcoin (BTC). This cryptocurrency can be used for making instant transactions globally without invading

[4] Deane, S., & Fines, O. (2023, January 4). *Cryptoassets Beyond the Hype - An Investment Management Perspective on the Development of Digital Finance*. CFA Institute. (p. 7).
[5] Nakamoto, S. (2008, October 31). A peer-to-peer electronic cash system. Bitcoin. Retrieved April 29, 2023, from https://bitcoin.org/en/bitcoin-paper
[6] Ibid., 5.

users' privacies, all while not requiring a central entity to control it.[7] This is made possible through the use of blockchain, a technology that evolved from the concept of distributed ledger technology, both of which will be explored below.

Before we dive into how the crypto ecosystem works and what it means for the IFA profession, it is imperative to acknowledge two crucial aspects. First, while Nakamoto's vision of having one global currency through the blockchain seemed overambitious at the time, to say the least, it is arguably still more simplistic than the present crypto ecosystem, which has evolved to include coins, tokens, smart contracts, non-fungible tokens (NFTs), stablecoins, to name a few (together, referenced to as "crypto assets"). Although NFTs and stablecoins are growing in popularity among the crypto asset class, they are not explored in detail in this paper. Instead, this paper dives into the details surrounding coins, tokens and smart contracts as they form the foundations of the crypto ecosystem at the time of writing. Second, it is important to take a step back and expand on why this paper will not explore the legitimacy of cryptocurrency and blockchain as a concept. As discussed in the abstract of this paper, many remain rightfully skeptical of the crypto ecosystem and compare it to a global fraudulent scheme. The other majority strongly advocates for it and believes it to be a revolutionary financial system. However, regardless of legitimacy, the impact of the crypto industry is real and is felt by many. As of May 20, 2023, the total cryptocurrency market capitalization was around $1.1 trillion, and around $522 billion, or 46.4% of

[7] Ibid., 5.

which comprises Bitcoin's market capitalization.[8] Furthermore, in more recent years, multiple reputable business institutions have embraced crypto and accepted it as a form of payment, including Microsoft and Starbucks.[9] This gain of institutional interest was one of the many shifts made in favour of the crypto industry. As such, this paper aims to discuss the consequences of its current implementation and what IFAs should know and understand about it if this system continues to grow.

1.1 Satoshi Nakamoto's Whitepaper: Bitcoin

According to the whitepaper, Bitcoin is meant as an "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." The Bitcoin whitepaper envisioned the ability to replace intermediaries with a network of computers (or "nodes"), which perform computations for the purpose of verifying and recording transactions. The network timestamps transactions, thereby creating a record and then linking them to a continuous chain of prior transactions.[10] These records are meant to be permanent and immutable, as attempting to alter these transactions would require redoing the verification process performed by all the nodes in the network, which becomes near impossible as the chain becomes longer. Furthermore, a cost and benefit analysis shows

[8] *Global cryptocurrency market charts*. CoinMarketCap. https://coinmarketcap.com/charts Retrieved May 21, 2023
[9] Tuwiner, J. (2023, May 22). *9 major companies who accept bitcoin [spend crypto 2023]*. 9 Major Companies Who Accept Bitcoin [Spend Crypto 2023].
[10] Ibid., 5.

that the reaped benefit is not worth the time and computer power expensed to achieve this, which renders the proposed verification process secure.[11]

In order to understand how Bitcoin transactions are created, it is important to define the Distributed Ledger Technology (DLT) and Blockchain first. Generally defined, a DLT encompasses any system that involves more than one party, thereby eliminating the need for an intermediary or central operator.[12] This is complemented by the blockchain, which is a specialized implementation within the DLT framework. It is decentralized in nature as it broadcasts incoming transactions to authorized and distributed computers, i.e., nodes on its network, which in turn, perform the task of verifying the incoming transaction. The blockchain operates by utilizing a sequentially connected chain of data structures that house individual blocks of data. As each block is securely linked to the preceding one, it creates an immutable record that can be accessed and verified by the authorized parties.[13]

When applying these concepts to cryptocurrencies, the DLT can be described as a distributed digital ledger, which is the technology designed to verify and record transactions on a cryptocurrency blockchain network such as Bitcoin. The ledger is irreversible, meaning that it cannot be modified or tampered with, but it can only be appended with new transaction data.[14] Preserving and providing public access to

[11] Ibid., 5.
[12] Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2019, December 18). *Distributed Ledger Technology Systems: A conceptual framework*. SSRN.
[13] Ibid., 12.
[14] Ibid., 5.

cryptocurrency transaction records while maintaining the security and integrity of the data are some of the distinctive features that render the blockchain and DLT exceptionally transparent and reliable.[15] Such transparency is instrumental in establishing trust and accountability in the crypto ecosystem. With this broad conceptual framework, we further explore other essential concepts that play a crucial role in making this process possible. To start, we take a high-level look at how transactions are recorded in the blockchain. An illustration by Euromoney Learning, a reputable training platform under one of Europe's largest business and financial information companies, provides a helpful illustrative overview. It is recommended to keep this illustration in mind as we delve into these concepts:

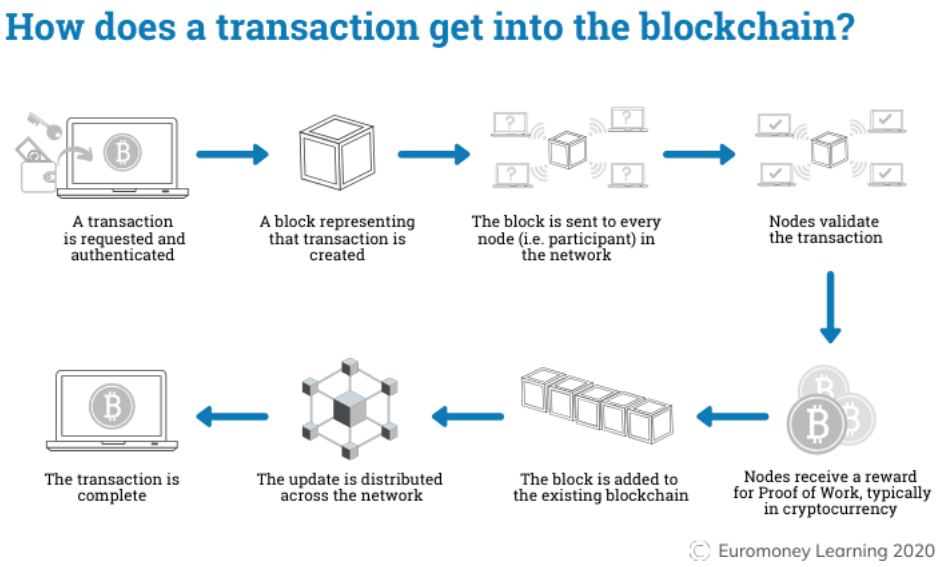

Figure 1.1[16]

[15] Ibid., 5.
[16] Euromoney. (n.d.). *How does a transaction get into the blockchain?*. Blockchain Explained: How does a transaction get into the blockchain? | Euromoney Learning. https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain

1.2 Cryptography

Cryptographic code adds additional layers of privacy and security to cryptocurrency transactions. It aims to maintain anonymity and obfuscate the linkage of wallet addresses to a specific individual or entity.[17] Before conducting a transaction, users must open a wallet with a wallet service provider. Users who wish to obtain a wallet address must first create a "private key," also referred to as "the digital signature." Through the application of complex mathematical functions called "elliptic curve multiplication," the private key is encrypted and used to derive an additional key, referred to as the "public key," providing the first privacy layer.[18] Furthermore, the public key then goes through an additional process of complex mathematical functions called "hashing," which shortens the public key and, as a result, derives what is referred to as the wallet address. The wallet address, comprising a string of 25 to 40 arbitrary alphanumeric characters, is what a receiver provides a sender in order to send funds, and this address, is what would appear on the distributed ledger[19].

These complex mathematical functions are all done in this specified order. In addition, they are immune to being reverse-engineered to obtain an individual's private key through their wallet address or public key. Doing so would put the ownership of the wallet's assets at risk of seizure and theft. To better grasp the concept of private keys,

---

[17] Team, E. (2021, August 15). *The keys to crypto kingdom: Wallet address, public and private keys explained*. Blocktrade. Retrieved May 17, 2023 https://blocktrade.com/wallet-addresses-public-and-private-keys-explained/
[18] Ibid., 17.
[19] Ibid., 17.

public keys and wallet addresses, BlockTrade, a crypto exchange platform, published the following illustration, which explains the flow as follows:

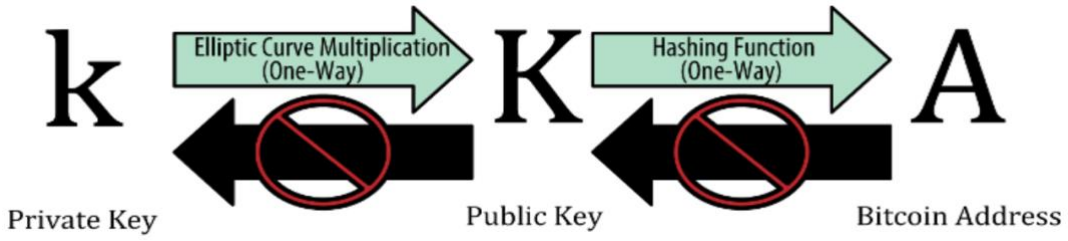

Figure 1.2[20]

To bring these concepts full circle in an investigative context, decrypting public keys or wallet addresses is possible when investigators obtain the private key. This is as the private keys grant control over the contents and value of the wallet address. However, where only the public key is available, possession of the wallet assets cannot be accomplished, making the seizure of illicit funds in a wallet extremely difficult unless the private key is obtained through traditional investigative methods of information gathering, such as interviewing the suspect, search and seizure of electronic devices[21].

To summarize how wallets operate in a purely transactional context for concept illustration purposes, let us assume a scenario where a customer wishes to pay a vendor 0.5 BTC for a service or commodity. The sender must enter the amount and the receiver's (i.e., the vendor's) wallet address which is derived from the public key. Before the transaction is sent out, it is digitally signed by the sender, where the signature is

[20] Ibid., 17.
[21] Kohler, C. (2022, March 13). *Can your bitcoin be seized by governments?*. The Bitcoin Manual. https://thebitcoinmanual.com/articles/can-bitcoin-seized/

generated using the private key. The signature proves that the wallet holder or owner has initiated a transaction on the DLT. Eventually, the transaction goes through the blockchain verifiers, and before the transaction is recorded on the blockchain, the verifiers must inspect and approve it. Blockchain verifiers are also referred to as miners, and their set of roles is further discussed in the next subsection.

1.3 Mining for Crypto Gold: Currency Creation

The blockchain is maintained by using cryptography, computer code and mining. The mining process serves as the primary means for regulating the creation of cryptocurrencies, in addition to authenticating and incorporating transactions into the blockchain network and maintaining its security.[22] There are multiple processes for validating transactions in the blockchain, the most ubiquitous process is the one referred to as "The Proof of Work (PoW)" consensus model. First, for a new currency to come into circulation, the process of Proof of Work (PoW) would involve the utilization of miners' computers that are connected to the network of a specific digital currency, those computers are called "nodes," as referred to in Figure 1.1. The nodes are responsible for generating complex solutions to intricate mathematical problems, also known as "hashes."[23] To achieve this, a considerable amount of real-world energy or computer power is expended as the computers employ brute force to guess the solutions to the hash. The first miner to accurately solve the hash is granted the privilege of ownership of a new

[22] Chainalysis Team. 2020. Who's Who on The Blockchains? The Chainalysis Guide to Cryptocurrency Typologies.
[23] Ibid., 22.

cryptocurrency by adding recently generated data blocks and transaction records to the blockchain.[24] This process is likened to gold mining by many.

1.4 Decentralized Auditing

The nodes (i.e., miners' computers on the blockchain network) function as the auditors for transactions through the Proof of Work (PoW) process. To illustrate, we build on the previously discussed example of the customer who needs to pay 0.5 BTC to a vendor. Before this transaction is processed and recorded on the public blockchain, the majority of nodes must first vote and reach a consensus on its validity[25]. Once an agreement is reached, the transaction is recorded, and the distributed ledger is updated to show this new entry. This mechanism ensures that the integrity of the blockchain is maintained and that transactions are thoroughly scrutinized by a decentralized network of nodes. The auditors, or nodes, in this case, would be paid for their work with cryptocurrencies.[26]

1.5 Alternative Coins, Tokens and Smart Contracts

Bitcoin brought the concept of cryptocurrency to mainstream attention, which brought about a substantial number of other cryptocurrencies referred to as "coins" or "alternative coins" into circulation. Alternative Coins or Altcoins refer to any

[24] Ibid., 22.
[25] Ibid., 16.
[26] Ibid., 16.

cryptocurrencies that are not Bitcoin and have their own blockchains. [27] As of June 2023, CoinMarketCap reported that there are roughly 25,400 cryptocurrencies or altcoins. [28]

Ether is the native cryptocurrency of the Ethereum blockchain and comes second in its market capitalization after Bitcoin.[29]. It is unique as it allows users to program the blockchain and utilize open-source platforms. It has grown in prominence due to its ability to create special features such as "Dapps," which we discuss further in Chapter 3, and "Smart Contracts."[30] Smart contracts grant users the ability to execute agreements and commands through written code of if/then statements[31]. Those functions would automatically be executed when certain conditions or terms agreed upon by the involved parties are fulfilled.[32] In the same vein as the DTL, these smart contracts do not require the existence of a third party to oversee execution and are supposedly secure. However, as we will discuss in Chapter 5 of this paper, they possess a significant weakness of being suspectable to hacking as they are essentially based on code.

What makes these smart contracts exceptional, or to some, concerning, is that, among many things, they allow everyday people, by using the blockchain, to fairly easily create what is called a "Token." Tokens are an embodied digital form of an asset or interest in an asset. This is because the alternative, crypto mining, has become an

---

[27] Team, T. E. (2021, July 23). *Altcoins vs Tokens: What is the difference?*. Trading Education. https://trading-education.com/altcoins-vs-tokens-what-is-the-difference
[28] Ibid., 9.
[29] Ibid., 22.
[30] Ibid., 22.
[31] Frankenfield, J. (2023, February 10). *What are smart contracts on the blockchain and how they work*. Investopedia. https://www.investopedia.com/terms/s/smart-contracts.asp
[32] Ibid., 22.

increasingly difficult, energy-consuming, and highly competitive process. A Token is a crypto asset created on top of an existing blockchain.[33] Tokens became increasingly prevalent in 2017 with the rise of Initial Coin Offerings (ICOs) as they were a way for blockchain-related businesses to raise funds for their projects. A business issues tokens to investors rather than traditional equity or debt instruments.[34] When the boom of ICOs, or what some may call the "ICO Mania," took place, the environment was and, to a large extent, remains unregulated, which creates the perfect opportunity for bad actors to create fraudulent ICOs, market them as legitimate, perform a quick and easy cash-grab and then disappear.[35]

Ponzi and Pump and Dump are also some of the fraudulent schemes which gained popularity with the rise of tokens. In 2019, a group of fraudsters in mainland China carried out a Ponzi scheme called PlusToken that defrauded victims out of an estimated $2.25 billion.[36] The scheme tricked investors into funding the development of cryptocurrency products by downloading an app and depositing funds, which were then converted into cryptocurrencies. Participants earned credit by recruiting others, and profits were distributed through PlutTokens, which were then reinvested in PlusToken. This scheme ended with affiliate investors being unable to withdraw their funds and the fraudsters posting a message that said, "We have run."[37] The fraudsters have been

[33] Ibid., 22.
[34] Pisa, M. (2018). Initial Coin Offering (ICO) mania and its implications for technology-led Social Enterprise.
[35] Ibid., 34.
[36] Leng, S. (2020, December 1). *Chinese cryptocurrency platform ringleaders jailed in US$2.25 billion scam*. South China Morning Post. https://www.scmp.com/economy/china-economy/article/3112115/chinese-cryptocurrency-scam-ringleaders-jailed-us225-billion
[37] Okta (2023, February 14). *The plustoken cryptocurrency scheme: Architecture and exposure*. Okta. https://www.okta.com/identity-101/plus-token/

arrested and sentenced to jail.[38] For Pump and Dump schemes, countless examples can be discussed, such as in the case of eight social media influencers posing as successful traders being charged by the U.S. Securities Exchange Commission (SEC) in December 2022 for securities fraud related to Pump and Dump schemes.[39] The schemes consist of exchangeable crypto asset holders who engage in deceptive practices encouraging the purchase of the held crypto asset by marketing it to unsuspecting investors, typically through social media platforms such as Twitter and Discord. This is done through the use of false and misleading statements, which play on an inexperienced investor's fear of missing out on profitable investment opportunities. Eventually, this causes the price of the asset to rapidly and artificially increase above its actual value as more investors buy in. The fraudsters who initiated the scheme then capitalize on the artificially inflated price by selling their asset at a significant profit, thereby dumping it, which causes the price to subsequently plummet and ultimately leave newer investors with a devalued asset.[40] Altcoins and tokens are considered the most popular assets for trading and transacting in the crypto ecosystem and can be utilized for illicit purposes, as discussed in the above cases. They, along with smart contracts, are key concepts for the IFA to understand crime in the crypto world since they make popular tools for criminals to utilize for illicit gain.

[38] Ibid., 37.
[39] SEC. (2022, December 14). *Press release - SEC Charges Eight Social Media Influencers in $100 Million Stock Manipulation Scheme Promoted on Discord and Twitter*. SEC Emblem. https://www.sec.gov/news/press-release/2022-221
[40] Team, C. (2023, February 16). *Crypto pump and dump schemes make up 24% of new tokens*. Chainalysis. https://blog.chainalysis.com/reports/2022-crypto-pump-and-dump-schemes/

Conclusion

The concepts covered in this chapter are all elements of the crypto ecosystem. While not an exhaustive list, this chapter provides IFAs with an introduction to how disruptive the blockchain is and how its accessibility creates an opportunity for exploitation by criminals. Blockchain is an emerging technology that is undergoing development and is far from mature. Even some of the terms used in this paper may develop and change with time. However, it has garnered enough interest and attention for IFAs to see the importance of being cognizant of its fundamentals if they hope to approach scrutinizing it. As such, IFAs must be well-informed of the challenges, opportunities and risks it offers.

To summarize how the crypto ecosystem may affect the IFA professionals, the potential challenges and opportunities of the crypto ecosystem using an IFA lens are listed below:

Challenges:

- Given the rapidly evolving landscape of the crypto ecosystem, it poses a challenge for regulators to implement regulations and hold bad actors accountable.
- The complexity of the ecosystem can be overwhelming, potentially dissuading IFAs from entering the industry. However, their unique skills and services in enhancing fraud prevention, detection, and investigation efforts, can make the technology safer, which directly correlates to a smaller pool of victims who may join the industry based on the advice of bad-faith actors who may exploit them.

- The decentralized aspects of the blockchain dissipate regulators' sense of responsibility globally, posing the following questions "Who enforce the regulations, and how?".
- With the crypto ecosystem being an uncharted territory, it lacks regulation and offers criminals a prime lawless environment to commit crimes by exploiting vulnerabilities in the system. In addition, it provides them free reign to innovate ways of increasing anonymity and obfuscating money sources, making it challenging for regulators and investigators to keep pace.
- The blockchain's anonymity provides a shield for protecting the identities of malicious actors. However, the blockchain's privacy may be subject to change as the environment evolves.

Opportunities:

- Blockchain provides permanent and immutable records, resulting in accurate records that investigators can scrutinize and rely on. This also decreases the risk of records being manipulated by bad actors.
- The blockchain's ability to provide easy access to transaction records enhances transparency and streamlines the data extraction process for IFAs. This can also eliminate delays that occur when records are difficult to find or obtain when being retained by clients.
- Accessing public records permits auditing procedures by all users. In addition, accountability is promoted, and honesty is incentivized during the transaction verification procedures.

- Being an uncharted territory, the crypto ecosystem permits the building of innovative tools and protocols, offering regulators and investigators a unique chance to create ground-breaking investigation and enforcement tools which may enhance traditional investigative procedures.
- The enhanced privacy the blockchain provides promotes honest users' experiences by protecting their identities from malicious actors.

Lastly, as we started this chapter by introducing Satoshi Nakamoto's vision, it is appropriate to remind the reader that the crypto ecosystem is far from the original vision introduced in 2008. The current environment shows that the blockchain and DLT concepts have taken a life of their own. The first cryptocurrency exchange was introduced in 2010, opening the floodgates to many more.[41] However, these exchanges play a pivotal role in distorting the decentralization, security, and privacy principles of the blockchain as they are centralized by the entity or individual overseeing the exchange. In addition, the custody of the crypto assets is held by a central entity which meant that funds were exposed to internal misuse and theft by the exchange controllers or external hackers. While these risks are now better mitigated with increased regulatory oversight, implementation of safeguards and enhanced controls such as Know Your Customer (KYC) or Customer Due Diligence (CDD) requirements, it remains true that centralized exchanges are controlled by a central entity and custodian. As centralized exchanges are perceived to be moving away from Nakamoto's vision[42], developers sought to restore it

[41] Protocol, T. B. (2019, May 14). *The evolution of the Decentralized Exchange: A brief history*. Medium. https://theblocknetchannel.medium.com/the-evolution-of-the-decentralized-exchange-a-brief-history-888ee0ce1803
[42] Ibid., 41.

by introducing the “Decentralized Finance” application, which also provides a different set of challenges and opportunities for IFAs, as will be discussed in the following chapter.

2. DECENTRALIZED FINANCE

Decentralized finance (DeFi) emerged as a subset of the broader crypto ecosystem. DeFi pertains to all crypto protocols, services and instruments that operate under the purest form of decentralization. The DeFi paradigm is commonly used to describe the intersection of blockchain, digital assets, and financial services, according to the paper *DeFi Beyond the Hype - The Emerging World of Decentralized Finance*, published by the Wharton School of the University of Pennsylvania (UPenn) in collaboration with the World Economic Forum (WEF).[43] DeFi’s use is confined to decentralized applications, referred to as “Dapps.” These offer financial services on a blockchain settlement layer, such as payments, lending, trading, investments, insurance, and asset management. In the spirit of upholding Nakamoto’s philosophy, DeFi doesn't require centralized intermediaries or institutions. As such, any individual or entity can have access to these financial services without any KYC or CDD requirements. DeFi utilizes open protocols which permit flexible combinations of services that are customized through programming.[44]

[43] Gogel, D., Taylor, T. B., Cloots, A. S., Forster, B., Gustave, J. L., Schär, F., & Sokolin , L. (2021). *DeFi beyond the hype - Wharton Initiative on Financial Policy and Regulation*. University of Pennsylvania. https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf?ref=tokendaily
[44] Ibid., 43.

UPenn's paper summarizes the nine key building blocks of DeFi as being: blockchain, digital assets, wallets, smart contracts, DApps, governance systems, decentralized autonomous organizations (DAOs), stablecoins and oracles [45]. Some of these concepts were discussed in Chapter 1 of this paper as part of the overall crypto ecosystem. These, along with the new concepts, are the key to enabling the overall DeFi ecosystem (refer to Appendix for detailed definitions of each building block).

2.1 DeFi Characteristics and Service Categories

As demonstrated in the introduction of this chapter, there is some overlap of concepts with the overall crypto ecosystem. However, not all blockchain applications can be categorized as DeFi applications, even ones that allow the use of financial services. For example, smart contracts can be applied to both decentralized and centralized systems this is because identical criteria and implementation can be utilized in centralized settings. This indicates that there are defining criteria that constitute DeFi protocols as follows:[46]

1- DeFi protocols must facilitate the transfer and exchange of value directly without any intermediaries. They operate on a Peer-to-Peer (P2P) philosophy in its truest form.

2- To ensure trust-minimized operation and settlement, DeFi protocols must be anchored on transactions recorded based on DeFi protocol rules.

[45] Ibid., 43. (p.3-4)
[46] Ibid., 43.

3- DeFi protocols are non-custodial in principle, which provides users full control and protects their assets from being seized by regulators or changed by third parties, including service providers. Thus, it creates a critical distinction between centralized and decentralized crypto exchanges, where the former has custody of users' assets, rendering them non-DeFi platforms. This is further discussed in Chapter 3 of this paper.

4- DeFi protocols have an open-source code for public programming and architecture, allowing for the development of financial instruments. The Wharton paper demonstrates an example of a stablecoin that can be used as the basis for a derivative, which is then utilized as collateral for a loan and covered under an insurance contract.

Services which operate under this set of principles fall under the DeFi ecosystem. This is not an exhaustive list, but significant service categories include stablecoins, exchanges, credit, derivatives, insurance and asset management.[47]

Conclusion

This relatively simplistic overview of DeFi signifies the extremely rapid developments brought about through blockchain technology. Through DeFi's increased access to capital markets, it opened doors for a plethora of financial services which focus on shedding the traditional system of trusted third parties and centralized authority. While this promotes increased innovation in the financial industry, it also raises various

[47] Ibid.,43.

concerns due to its facilitation of financial crime. A summary of these concerns is provided below to demonstrate why it is important to set the foundational understanding of these new concepts if IFAs hope to combat crimes in this ecosystem.

- As DeFi facilitates the use of open-source programming, users can create innovative financial services and tools. However, this feature also facilitates the building of decentralized protocols used for enhancing privacy and obfuscating trails of funds for money laundering, making detection and tracing efforts further challenging. An example of which would be cryptocurrency mixers. Those are discussed in detail in Chapter 5 of this paper.
- DeFi provides global access and round-the-clock availability of services. However, unlike traditional banking systems, it does not safeguard the environment with bank account requirements or demand users' personal information.[48] It offers unrestricted access to all users, including high-risk participants and cybercriminals, making it a double-edged sword feature for the crypto ecosystem.
- There is continuous debate within the DeFi community about the degree of centralization within DeFi. Many argue that the decentralization component in DeFi is inherently fictitious. This stems from the fact that DeFi protocols rely on central data feeds known as Oracles, which are controlled by a select few anonymous individuals with admin keys. Also, there is a disproportionate allocation of governance tokens and voting rights, which tip the scales of

[48] Ibid., 43.

decision-making in favour of one party over the other.[49] This issue has become a point of contention, and as many question the true decentralization of DeFi, regulators must answer even more difficult questions, such as "who is held accountable" as they attempt to regulate the space.

With this in mind, we delve further into how the concepts discussed translate in the form of centralized and decentralized exchanges and how these exchanges play a role in combating or facilitating crime in the crypto ecosystem.

3. ECONOMIC EXCHANGES

Exchanges play a large role in investigative blockchain crimes, and this chapter aims to clarify that role. Traditional exchanges have and continue to facilitate the trading of securities and are a well-developed and regulated service industry globally. Regulatory authorities, such as the SEC in the U.S. and the Canadian Securities Administrator (CSA), enforce regulations to ensure fair trading. Prior to discussing how centralized and decentralized exchanges can help in investigations, it's important to understand the criteria that define each as they have undergone changes with the introduction of crypto. This overview aims to help IFAs become well aware of the features and issues they need to consider when approaching investigative work in the crypto ecosystem.

3.1 Centralized and Decentralized Exchanges

[49] SCHÄR, F. (2022, September). *Defi's promise and pitfalls - IMF*. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/Fandd/Article/2022/September/Schar.ashx

Both centralized and decentralized exchanges facilitate the same services of buying/selling assets, but they operate under different principles. Centralized exchanges refer to models that rely on a trust-based system employing intermediaries to manage users' funds and crypto assets. They publish accurate price data, pair up buyers and sellers, finalize trades through settlements, and oversee transactions.[50] This definition has evolved to include all exchanges that are centralized, including those which strictly deal in fiat, such as the New York Stock Exchange, and those that facilitate trades between fiat and digital assets, such as Binance. These exchanges are considered centralized as they are intermediated, custodial in principle, do not allow open-source coding and do not minimize trust.[51]

For decentralized exchanges, we build on prior concepts discussed in Chapter 2 of this paper. Decentralized exchanges are non-custodial in nature, as they utilize non-custodial wallets, which allow users to retain full control and possession of their wallet content. In addition, they are accessed programmatically, determine prices through algorithms and settle transactions through smart contracts against a capital pool.[52] Obvious issues with decentralized exchanges stem from its name - decentralization dissipates accountability, which poses challenging questions for regulators on how to hold a distributed network accountable. In addition, the private nature can be a strong facilitator to laundering proceeds of crime. On the one hand, they may arguably live up to the transparency feature of blockchain, as all transactions and governing smart contracts

[50] Ibid., 43.
[51] Ibid., 43.
[52] Ibid., 43.

are viewable and publicly available, providing easy access to users and investigators. On the other hand, this transparent nature, when exploited by illicit actors, can be the very reason DeFi becomes vulnerable and insecure. For example, hackers and other illicit actors are able to scan the DeFi code of a decentralized exchange to detect weaknesses and launch timely and calculated attacks that allow them to steal as much as possible.[53]

3.2 Role of Crypto Exchanges

Exchanges, specifically ones permitting the exchange of digital assets, have become increasingly pivotal in regulating and investigating the blockchain landscape in recent years. Centralized exchanges represent an important tool during the stages of the money laundering process. This is done by criminals who place their illicit cryptocurrency funds in a centralized exchange and exchange these funds for fiat. The process of exchanging cryptocurrency for fiat is commonly referred to as "fiat-off ramp." While cybercriminals may use other methods to launder money, centralized exchanges remain the most popular for criminals. Chainalysis reported that in 2022, centralized exchanges received just under 50% of nearly $23.8 billion in illicit cryptocurrencies, making them the number one choice for money laundering.[54] On the other hand, decentralized exchanges are also growing in use by hackers who exploit DeFi protocol weaknesses to steal funds. Once a protocol is hacked and emptied of its funds, hackers can place these funds in a decentralized exchange and exchange them for a cryptocurrency that is more likely to be stable. Once the exchange is complete, hackers

[53] Chainalysis. (2023). *Chainalysis 2023 Crypto Crime Report* . Chainalysis. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
[54] Ibid., 53.

can transfer these funds into a centralized exchange and off-ramp to fiat.[55] These schemes are discussed in more detail in Chapter 5 of this paper.

When crypto exchanges were first created, they were expected to uphold the privacy, security, decentralization, and accessibility principles of the blockchain. As a result, many were hesitant to work with law enforcement agencies by either sharing information or enforcing strict KYC procedures that combat money laundering and terrorist financing efforts. However, regulatory and law enforcement authorities have successfully exerted pressure on these crypto exchanges, leading to a shift in their approach toward compliance. As a result, exchanges are now more amenable to cooperating with law enforcement and have strengthened their KYC and regulatory compliance requirements.

In November 2022, the CSA announced that it would strengthen its oversight of crypto trading platforms. This includes expanding current requirements and expecting greater commitment from platforms operating in Canada as they seek registration.[56] In an attempt to resolve jurisdictional issues, the CSA considers platforms accessible by Canadians, even if located outside of Canada, to be operating within Canada for the purpose of this regulation.[57] Key terms and conditions require platforms serving Canadian clients to hold those clients' assets with a regulated custodian in countries like

[55] Ibid., 53.
[56] CSA. (2022, December 12). *CSA provides update to crypto trading platforms operating in Canada*. Canadian Securities Administrators. https://www.securities-administrators.ca/news/csa-provides-update-to-crypto-trading-platforms-operating-in-canada/
[57] Ibid., 56.

the US, Canada, or similar jurisdictions that have a supervisory regime for conduct and financial regulation. Moreover, these assets must be kept separate from the platform's proprietary business.[58] This CSA's approach will render all platforms centralized if they comply, which contradicts the principles of DeFi and, as such, is expected to face resistance from decentralized exchanges. Additionally, it appears that as of this announcement, the CSA has not explicitly issued guidance or regulation that pertains to decentralized exchanges.[59] However, in an effort to show their commitment to these regulations, the CSA has set a deadline for platforms to submit pre-registration undertakings (PRUs) as evidence of their adherence to these regulations. Failure to do so could result in a ban in Canada. If necessary, the CSA may even take enforcement action to ensure compliance with securities law.[60] Interested readers can find an updated source of all platforms which have registered with the CSA or provided PRUs, along with the CSA or principal regulator's decision.[61] As a result of increased regulatory requirements, numerous other platforms are presently facing the prospect of being non-compliant within their respective jurisdictions, thus posing a threat to their existence in those countries. In order to remain operational in countries like the US and Canada, centralized exchanges have realized the importance of adhering to regulatory protocols.

---

[58] Ibid., 56.
[59] Stein, L., & Sorell, R. (2022, November 11). *Retail investment limits under the Canadian Crypto Asset Trading Platform (CTP) regulatory regime*. McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/techlex/retail-investment-limits-under-canadian-crypto-asset-trading-platform-ctp-regulatory-regime
[60] CSA. (2022a, August 15). *Canadian securities regulators expect commitments from crypto trading platforms pursuing registration*. Canadian Securities Administrators.
[61] CSA. (2023, June 2). *CSA regulatory sandbox / crypto asset trading platform decisions*. Canadian Securities Administrators. https://www.securities-administrators.ca/resources/regulatory-sandbox/decisions/#CTPDecisions

Consequently, many exchanges have begun to collect vital customer information, including government-issued identification and IP addresses. This practice enables them to provide valuable information to law enforcement agencies during official investigations, which can aid in tracking funds and identifying the identities of perpetrators of criminal activities.

Conclusion

Exchanges continue to be a highly frequented stop for money laundering by illicit actors. However, through increased cooperation and enhanced due diligence measures, law enforcement agencies across the globe can effectively coordinate and collaborate with cryptocurrency exchanges in the event of a necessary freezing of funds. These measures allow law enforcement to seize funds to provide restitution to victims who have suffered damages from illicit activities. Such efforts not only bolster integrity in the cryptocurrency industry but also support the broader goals of justice and security.

Furthermore, while increased regulation and oversight are crucial, IFAs must equip appropriate and relevant investigative techniques that complement the current environment. As we will discuss in Chapters 4 and 5, these tools will allow IFAs to better investigate and identify illicit activities. By doing so, IFAs can support regulators' efforts in cementing the perception that illicit activity in the crypto ecosystem is not far from the hands of prosecution and ensure that the cryptocurrency ecosystem has the potential to become a secure space for honest users.

4. INVESTIGATING CRYPTO CRIMES

As previously noted, a key feature of cryptocurrency that has garnered significant attention is its purported anonymity. For some time now, there has been a widely held belief that the privacy and anonymity of users' identities in the crypto ecosystem render it an elusive and challenging entity to track or regulate. Nevertheless, this perception is undergoing changes, thanks to the remarkable advancements of competent cryptographers, investigators, researchers and analysts. Experts have successfully debunked the myth that tracing crypto is an insurmountable challenge. As a result, it is becoming increasingly evident that crypto is more amenable to regulation and tracking than previously assumed and that the blockchain should more accurately be described as pseudo-anonymous rather than anonymous, as described by many.

4.1 Clustering Heuristics Rules

The endeavour to scrutinize and trace cryptocurrency transactions dates back to as early as late 2012. While many efforts were concentrated on this issue, this paper highlights efforts by Sarah Meiklejohn and her team, presently a Professor in Cryptography and Security at the esteemed University College London (UCL) and a Staff Research Scientist at Google[62], who was pursuing her Ph.D. studies at the University of California in late 2012. Meiklejohn's research marked a pivotal moment in the history of cryptocurrency as it introduced the conceptual framework used in the development of various tracing tools and investigative techniques today. Hence, her contribution to the

[62] Meiklejohn, S. (n.d.). Sarah Meiklejohn. https://smeiklej.com/

field has been highly regarded and continues to inspire contemporary studies in the domain.

To test the limits of the anonymity feature in Bitcoin, Meiklejohn returned to Satoshi Nakamoto's whitepaper to analyze it. In the whitepaper, Nakamoto states [63], "As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner." Whether inadvertently or otherwise, this statement proves that specific analysis techniques could be applied to collapse some addresses into single identities, which laid the groundwork for Meiklejohn's research into "Clustering Heuristics Rules."

The First Clustering Heuristic Rule:

First, to break down Nakamoto's words, we need to expand on the concept of "inputs" briefly. If we assume a scenario wherein an individual "A" has possession of two separate wallets with 2 BTC in each, along with their respective private keys, and "A" needs to transfer a total of 4 BTC to another individual, "B." Instead of conducting two separate transactions of 2 BTC each, "A" can send 4 BTCs at once to "B" as the software will automatically combine the amounts in one transaction listing two inputs, wallet 1 and 2. The input will show the wallet addresses used to send the payment, i.e., wallets 1 and

[63] Ibid., 5. (P. 6)

2, and the output will list the receiving wallet address owned by "B."[64] Through this analysis, Meiklejohn, her research team and others who performed similar analyses to the whitepaper were able to formulate and infer the first clustering heuristic rule. The first rule states that if two addresses appear as input for the same transaction, they are more likely than not to be controlled or owned by the same user.[65]

The Second Clustering Heuristic Rule:

Building off the first heuristic rule, we need to deconstruct another concept and introduce "Change Wallets." If a number of BTCs in a wallet are spent, the whole amount must leave the wallet, this is a rule in the blockchain that is automatically executed once a transaction is initiated. We illustrate this with another example to clarify, where "A" has a wallet that contains 5 BTCs and needs to send only 4 BTCs to "B." "A" will perform the transaction normally as they would any other transaction, but behind the scenes in the blockchain protocol, all 5 BTCs will leave the sender's wallet. Only 4 BTCs will go to "B," and the one remaining BTC will be deposited in a new wallet called a "change wallet" created for "A."[66] This is likened to breaking a piggy bank, where once the bank is broken, the coins not used will need to be deposited in a new piggy bank.[67] The following figure, published by the Institution of Research and Technology, provides a simplistic illustration of how change wallets come to be. The example assumes 5 BTCs need to be sent to a receiver (i.e., Address 4) and 0.1BTC as the transaction fee:

---

[64] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, December). *A fistful of bitcoins: Characterizing payments among men with no names*. University of California San Diego. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf
[65] Ibid., 64.
[66] Ibid., 64.
[67] Greenberg, A. (2023). *Tracers in the dark: The global hunt for the Crime Lords of Cryptocurrency*. Knopf Us.

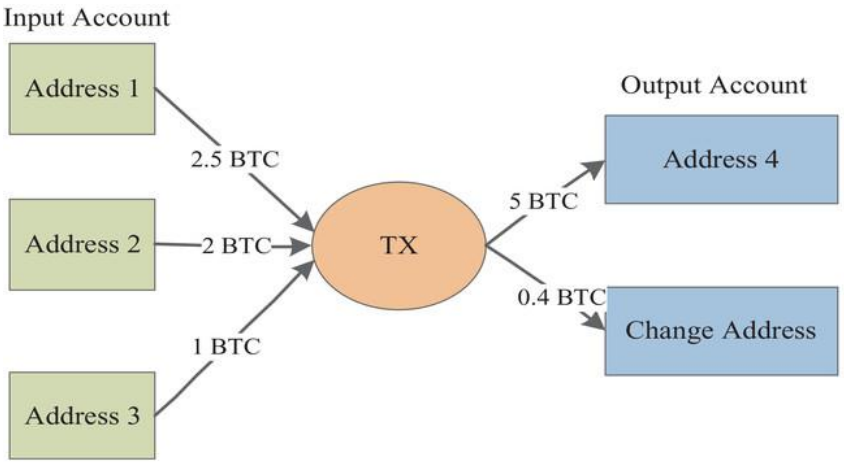

Figure 1.3[68]

This protocol helped Meiklejohn and her team deduce the second heuristic rule, which stated that if a change address is created, it is more likely than not to belong to the sender.[69] However, on a surface level, there were no particularly unique identifiers that distinguished change addresses from normal transaction addresses, which required an additional layer of analysis. Through pattern analysis, first, it was understood that the change wallet process occurs automatically on the backend of the Bitcoin protocol, sometimes even unknowingly by the user. Second, the primary transaction wallet will remain functional and frequently used by the user. This meant that change wallets would typically be used only in two instances, first, to deposit the change and second, to move out the change when making a second payment or transfer.[70]

To add a layer of safeguarding, suspected change wallets were observed for a duration of a week to ensure they were infrequently used. Following these sets of rules,

[68] He, X., He, K., Lin, S., Yang, J., & Mao, H. (2022, May 31). *Bitcoin address clustering method based on multiple heuristic conditions*. Institution of Research and Technology. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12014
[69] Ibid., 64.
[70] Ibid., 64.

Meiklejohn and her team started tagging change wallets and applying this heuristic rule to wallets on the Bitcoin blockchain. The result showed that out of a sample of 12 million public keys on the Bitcoin blockchain, there were only 3.3 million clusters. They also tested the heuristic rule's ability to trace criminal activity and have successfully mapped out the movement of a large number of bitcoins from "The Silk Road," a popular darknet market which operated in 2012, to various exchanges.[71]

4.2 Inherent Transparency

The research conducted by Meiklejohn and other experts has demonstrated that the blockchain infrastructure is, in fact, inherently transparent. This is an important milestone toward developing effective investigation and tracing techniques for cryptocurrencies. Since the publication of Meiklejohn's paper in 2013, there have been many technological advancements, such as enhanced machine learning, analysis and decryption programs. It is widely recognized that these technologies will only continue to improve over time. In addition, many other tools and blockchain analysis firms have since emerged with blockchain analysis tools with high success rates in investigating and tracing illicit funds or activities.

Conclusion

It is also important to note that criminals have fully embraced blockchain technology due to a belief in its anonymity and privacy features which resulted in an onslaught of criminal activity on its services and platforms. However, as the

[71] Ibid., 64.

understanding of the crypto ecosystem the blockchain technology grows, IFAs can identify ways to analyze criminals' methods, schemes and patterns of behaviour, including their hidden connections to other seemingly unrelated criminal organizations, which can provide insight into the extent and scale of their illicit operations. In a practical investigative context, this can be done by obtaining detailed records of not just one suspicious transaction but the entire transaction history of the suspected wallet in the public ledger. This includes any associated wallets that may relate to the wallet holder's activities, regardless of their location. This gives IFAs, a reason to be cautiously optimistic about the ability to investigate the blockchain landscape by combining highly analytical skills with these advanced technologies. With this view and understanding, we delve into the current environment of illicit activity in the crypto ecosystem in the next Chapter.

5. CRYPTO-RELATED CRIMES

Equipped with a fundamental understanding of how the blockchain's transparency can be a powerful tool in the IFA's arsenal to combat and investigate crime. This chapter delves deeper into analyzing both the current blockchain crime environment and the efforts and tools used by regulators, investigators and blockchain analysts to fight against it.

The crypto ecosystem is still very much in its infancy, and it is well known that the lack of regulations makes it a fertile ground for illicit activity. Specifically, throughout the last year, many scandals have erupted in the crypto ecosystem, from crypto exchange owners defrauding their investors to using crypto as a means of payment in darknet

markets. Still, nonetheless, interest and demand did not subside, and on the same level, illicit activities in the crypto ecosystem have maintained an upward trajectory[72]. With the institutional interest of large organizations such as Microsoft and Starbucks, it becomes more difficult to deny impacts and disruptions happening as a result of blockchain technology. As such, some governments grew concerned and took extreme positions by cracking down on the industry and making dealing in crypto illegal. However, other governments, such as the U.S. and Canada, have started to increase regulations on the industry and, particularly in the case of the US, enforce sanctions on some DeFi services and protocols through designation by the Office of Foreign Assets Control (OFAC).

Nonetheless, until regulations are codified and successfully enforced, criminals will always choose the path of least resistance. It is believed that as long as the crypto industry exists, with the expectation of anonymity, which is consistently being challenged, criminals will continue to find it an attractive avenue to funnel and obtain illicit funds.

5.1 On-chain Crimes and Combatting Efforts

On-chain crimes pertain to all illicit dealings occurring on the blockchain, which, as discussed, are, for the most part, recorded on the blockchain. Many would agree that they provide more transparency than off-chain crimes, which denotes any financial crimes not recorded on the blockchain, an example of which is a case of misstatement of financial records by a non-blockchain entity. Another example is a

[72] Ibid., 53.

cryptocurrency exchange that defrauds its customers. As this chapter delves into analyzing crime in the crypto ecosystem, it's important to note two things. First, this chapter's focus will be exclusively on on-chain crimes. While off-chain crimes that occur in a crypto environment are extremely relevant to IFAs' work, they have unique components that require a different analysis than the one provided in this paper. As such, it is more appropriate to research them separately to avoid the risk of not providing an applicable in-depth analysis. Second, to ensure the accuracy and relevance of the data used in this research with respect to the IFA field, this chapter will rely on insights provided by Chainalysis, an industry leader in blockchain analysis. The *Chainalysis 2023 Crypto Crime Report* published by the firm will serve as our primary reference for several reasons.[73] As early as 2014, Chainalysis established itself as a reliable source of blockchain investigative tools and, since, has been widely recognized for its expertise in analyzing blockchain transactions. Its credibility is further evidenced by its various successful collaborations with U.S. government projects and investigations, making it the preferred blockchain analysis firm for government contracts.[74]

The 2023 report stated that 2022 had the largest volume to date in illicit transactions in crypto. The total cryptocurrency value received by illicit addresses totalled $20.6 billion, representing a 14% increase from the prior year's value of $18.1 billion.

[73] Ibid., 54
[74] Nelson, D. (2023, May 9). *Inside chainalysis' multimillion-dollar relationship with the US Government*. CoinDesk . https://www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government/

These figures are considered lower-bound estimates but still provide clear evidence of the rapid growth of crypto crime. This is a cause for concern to IFA professionals, regulatory bodies and the public who might find themselves victims of crypto scams. According to the report, the crimes with the highest value received in 2022 were categorized based on their prominence. The OFAC-sanctioned entities topped the list, followed by scams, stolen funds, darknet money and ransomware. While this is not an exhaustive list, the next subsections of this paper will dive deeper into each one of these crimes as they resulted in the highest impact in terms of losses. The discussion on sanctions will be discussed last in the following subsections due to their unique nature of enforcement. For a more high-level look at all values obtained through on-chain crime in the crypto ecosystem, the below figure is presented:

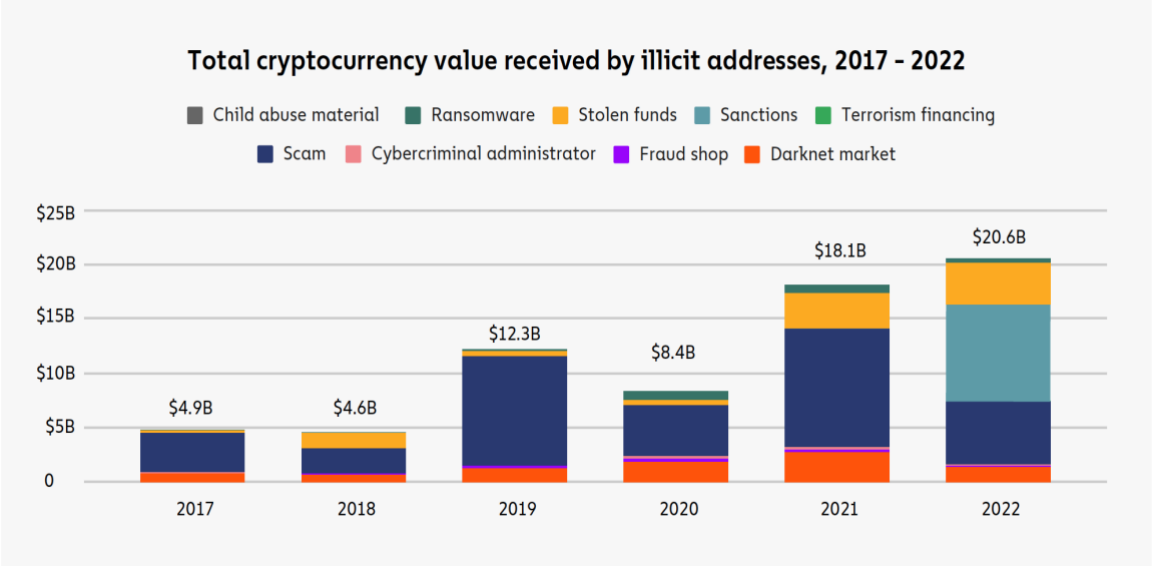

Figure 1.4[75] (Note: *graph represents lower bound estimate*)

[75] Ibid., 53.

Illicit activities in blockchain services and platforms may seem familiar to those in traditional environments. However, blockchain's added transparency allows for insights that were previously unavailable in traditional avenues. With this as background, we begin to delve into the selected sample of crimes in the crypto ecosystem.

5.1.1 Scams

Chainalysis' report [76] provides valuable insights to IFA investigators combating scams in the crypto ecosystem. Such insights would be difficult to quantify in traditional markets outside of the blockchain. However, due to the added transparency provided by the blockchain, it is possible to observe the flow of illicit funds from one wallet to another and analyze which wallet received the illicit fund; this, therefore, aids in ascertaining the address belonging to the perpetrator of a scam. Through analysis of the trends in scam-related addresses, it appears that depending on the type of scam fraudsters are attempting to inflict, a scam's success rate is either positively or negatively correlated with the volatility of the market. This analysis indicates that scammers may switch tactics based on crypto prices and market conditions. In 2022, a year that is particularly turbulent for the crypto industry, scam revenues fell to $5.9 billion from $10.9 billion in the prior year. It is also generally believed that the numbers reported by Chainalysis and other sources are underestimated due to various reasons. One reason is that not all addresses performing scams have been identified. This reason is specific to Chainalysis and other blockchain analysis firms whose method of reporting is the tracing of illicit addresses

[76] Ibid., 53.

associated with a crime.[77] Another reason, supposedly more relevant to law enforcement authorities, is the nature of this crime and its psychological impact on victims. Scams are specifically underreported as many victims feel embarrassed or humiliated that they fell for scammers' deception, and many prefer to bite the bullet than face the humiliation. The report also provides an overview of the different types of scams in the industry:[78]

Giveaway scams:

Scammers often deceive people by using the likeness of a famous person to make false promises of rewards. They may ask victims to send them cryptocurrency in exchange for these rewards.

Impersonation scams:

Fraudsters use the fear component to deceive victims and impersonate government employees or ones in positions of authority, such as agents from the CRA or IRS. They claim that victims must send cryptocurrencies to rectify a problem and avoid fines or charges. Impersonation scams are positively correlated with particularly upward market conditions and cryptocurrency prices, specifically Bitcoin. We can infer that this may play a part in tempting victims with possible rewards.

Investment scams:

Fraudsters advertise a fake investment company or service that promises unusually high returns. These scammers often use social media and online platforms to promote fake

[77] Ibid., 53.
[78] Ibid., 53.

testimonials of successful clients. Investment scams are especially positively correlated with Bitcoin prices. Fraudsters find it particularly appealing when the market conditions are on the rise, as this perpetuates their scheme's promise of high returns.

NFT scams:

Scams exist where fraudsters deceive victims into purchasing counterfeit non-fungible tokens (NFTs) that resemble well-known and rare collections. NFTs are digital assets that represent art pieces that are impossible to replicate.

Romance scams:

Involve fraudsters who feign interest in a romantic relationship with the victims. They typically find their targets through social media or online dating platforms. The goal is to extort money from victims through guilt or deception. Some fraudsters may spend months building a trusting relationship with their victims. These scams may also involve "pig butchering scams," which combine aspects of romance and investment scams. Scams involving romance are particularly underreported due to their sensitive nature. These scams are also not affected by market conditions, as victims are tricked into giving money to help a loved one rather than for investment purposes. This reveals how fraudsters may shift to romance scams during uncertain market conditions, which supports why they might be willing to build a relationship which takes time and effort rather than focusing on quick financial gain.

Investigating Scams on the Blockchain:

Through a combination of advanced blockchain analysis (i.e., on-chain analysis), which looks for connections between illicit addresses held by scammers, and traditional investigative tools (i.e., off-chain analysis) of cross-referencing information available online, such as fake customer testimonials and street addresses, Chainalysis found indicators that suggest a large percentage of scam work is perpetrated by only a few large players representing scam networks. To gather necessary evidence, there are other tools that rely on clustering heuristic rules, such as the ones discussed in Chapter 4 of this paper. An analysis can be conducted to determine if two scammers have used the same wallet address to deposit their ill-gotten gains. This may indicate that one person or entity is behind both scams or that the overlapping address relates to a nested service for money laundering.[79]

To conclude the subsection on scams, we summarize a number of key takeaways for IFAs, given the rise in scams.

Lessons Learned:

1- Public education plays a vital role in the prevention of scams. The blockchain allows for unique opportunities in this regard, as authorities have the capability of publicizing wallet addresses associated with scams to the public without the need

[79] Ibid., 53.

to release a scammer's personal identifying information. This can allow potential victims to spot these addresses before sending funds to a scammer.

2- As discussed, central exchanges can play a vital role in regulating and safeguarding the cryptocurrency landscape as they represent an important stop in the path that criminals take to exchange their illicit cryptocurrency funds into tangible cash, a process referred to as “fiat-off ramp.” One measure that exchanges can take is to warn unsuspected victims as they transfer funds to high-risk wallet addresses suspected of scams and other crimes in the form of an alert. IFAs who are equipped with a deep understanding of cyber security measures can provide consultation and risk assessment services on how these measures can be implemented to reduce liabilities on exchanges.

3- IFAs must be cognizant of market conditions and their influence on the behaviour of cybercriminals to focus their crime-combatting efforts efficiently and effectively. It is also crucial to stay up to date with DeFi and blockchain products, protocols, and services. As an example, Chainalysis has observed that scammers are moving from soliciting payments in Bitcoin to stablecoins as a means of hedging against a possible cryptocurrency market crash.

4- Blockchain analysis firms have developed software such as Chainalysis’ “Reactor” with the capability of tracing funds on wallet addresses and mapping millions of addresses to their corresponding off-chain entities, businesses, and individuals. Identifying businesses and individuals behind an address is done by utilizing automated traditional investigative methods such as scanning the wallet

address through social media, crypto forums and darknet markets.[80] These tools have proven to be useful in successful investigations and money-tracing efforts carried out by law enforcement authorities. The below figure represents an example of the Reactor tool that can show the movement of funds stolen from a hacked exchange and ultimately deposited into another exchange:

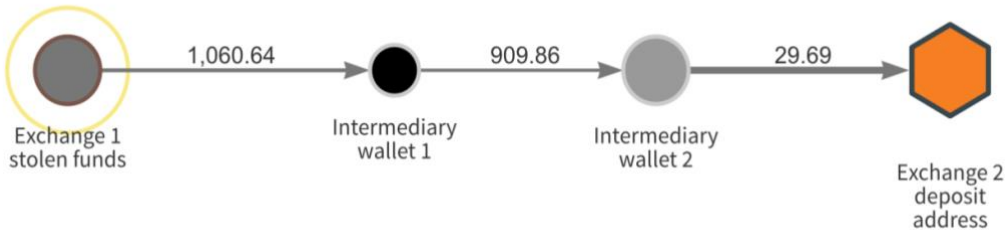

Figure 1.5[81]

5- Excluding Sanctions, scams account for a significant amount of money lost. However, the crypto scamming industry may be smaller than originally anticipated, as the funds seem to be linked to a few criminals or scam networks. Understanding the reach, behavioural and digital patterns of scammers is important to efficiently concentrate investigative efforts made towards fighting and tracing criminal activity. This deduction was only possible through monitoring and analyzing the movements of funds on the blockchain, and IFAs can be valuable contributors in this aspect as they possess the necessary analytical and accounting skills.

[80] Chainalysis. (2023b, June 5). *Cryptocurrency investigation software - chainalysis reactor*.
[81] Team, C. (2022, May 20). *Why you can't trace funds through services using blockchain analysis (and why you don't need to anyway)*. Chainalysis.

5.1.2 Stolen Funds

Crypto criminals usually acquire stolen funds through hacking. According to Chainalysis, hackers' focus has shifted from targeting centralized cryptocurrency services between 2016 and 2020 to targeting decentralized finance (DeFi) protocols in the past two years (2021-2022), where out of all the $3.8 billion in cryptocurrency stolen in 2022, DeFi protocols made up 82% or $3.1 billion.[82]

One particularly attractive DeFi protocol for hackers is the "Cross-chain Bridge." This protocol, using smart contracts, allows users to move digital assets from one blockchain to another. For example, if a user has 5 Stablecoins in their wallet on the Ethereum blockchain, they can lock this asset into a smart contract where it would be held as collateral. Once the protocol bridges to another currency's chain, such as a currency called "Polygon," the user is given funds in the form of an equivalent asset on Polygon's chain.[83] Cross-chain bridges are perceived to become as important as "Automated Clearing Houses" for banking institutions. [84] However, they are certainly not as secure and more susceptible to hacking which poses a real threat to the adoption of the blockchain's technology as a result of this vulnerability.[85] They are particularly attractive to hackers as users lock significant amounts of digital assets in these smart contracts,

[82] Ibid., 53.
[83] Team, C. (2022b, August 10). *Cross-chain bridge hacks emerge as top security risk*. Chainalysis. https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/
[84] Rosenberg, E. (2023, February 28). *What are cross-chain bridges?*. Investopedia. https://www.investopedia.com/what-are-cross-chain-bridges-6750848
[85] Ibid., 83.

where if a weak spot is found in the smart contract's code, they can be hacked and emptied out of the locked funds.[86]

The types of stolen assets are typically illiquid assets such as tokens, which can be issued by legitimate or illegitimate crypto projects but are not listed on centralized exchanges.[87] In order to launder their illicit goods in the blockchain, hackers usually resort to decentralized exchanges. These exchanges enable the trading of illiquid tokens for more liquid ones.[88] Another popular money laundering measure taken by hackers and other criminals is to place these stolen funds into a DeFi tool referred to as "Mixers."[89] As the name suggests, mixers are a privacy service that mingles the cryptocurrencies of numerous users for the purposes of concealing the source of funds. Criminals deposit the stolen funds from their illicit purposes wallets into mixers, and once mixed, they receive the obfuscated funds in another "clean" wallet which can be exchanged on a centralized exchange.[90]

As we conclude the subsection on stolen funds, below are a number of takeaways for IFAs to keep in mind.

Lessons Learned

[86] Ibid., 53.
[87] Ibid., 53.
[88] Ibid., 53.
[89] Ibid., 53.
[90] Team, C. (2023b, April 5). *Crypto Mixers and AML compliance*. Chainalysis. https://blog.chainalysis.com/reports/crypto-mixers/#:~:text=A%20crypto%20mixer%20is%20a,and%20owners%20of%20the%20funds.

1- DeFi services and protocols have a lot of work to do in terms of enhancing security measures if it hopes to become a trustworthy and widely used service.[91] During an interview with Chainalysis, David Schwed, who is the COO of Halborn - a reputable blockchain security firm with a proven track record - suggested that DeFi developers can learn a lot from proven security measures implemented by traditional financial institutions and that conducting "DeFi code auditing" could be a possible solution to address security vulnerabilities in DeFi. To enhance security measures, he suggested testing DeFi protocols by conducting controlled attacks to identify any security loopholes. Additionally, it is important to continuously monitor suspicious activities on smart contracts and implement circuit breaks that can pause transactions in the event of a hacker attack to mitigate potential damages.[92]

2- Although there are legitimate uses for mixers, the development of this protocol and its accessibility by bad actors is indeed concerning. However, just as criminals use technology to their advantage, IFA and law enforcement authorities can do the same with the support of blockchain analysis and security firms. With respect to mixers, there has been the development of tools with the ability to unmix some transactions to reveal their hidden origins. The development of these de-mixing tools is still in its early stages, and the specific method is intentionally kept undisclosed. However, Chainalysis and another prominent Blockchain

[91] Ibid., 53.
[92] Ibid., 53.

analysis firm, “Elliptic”[93], confirmed its existence and its successful application.[94] This, along with other previously discussed tools, enforces the belief that the crypto ecosystem is inherently transparent.

5.1.3 Darknet Markets

Darknet Markets are online stores located on the dark web and can be accessed through anonymity networks like “Tor,” which help hide the user's identity while browsing the internet. Darknet Markets typically connect illegal vendors with customers interested in purchasing a variety of illegal products and services. These can include drugs, fake documents, weapons, stolen data like credit cards, stolen items, and even child exploitation materials. In terms of services, these can entail hacking and hiring hitmen. All transactions on these platforms are conducted using cryptocurrency and are managed by cybercriminal administrators who conduct administrative tasks such as maintaining the website’s security, resolving users' technical difficulties and processing transactions.

Law enforcement agencies from various jurisdictions have successfully taken down and seized various Darknet Markets by executing coordinated operations and using blockchain tracing and analysis tools. A number of successful investigations are discussed below:

---

[93] Khatri, Y., & Copeland, T. (2022, February 23). *A look at Chainalysis’ claim to track bitcoin through mixing service coinjoin*. The Block. https://www.theblock.co/post/135148/a-look-at-chainalysis-claim-to-track-bitcoin-through-mixing-service-coinjoin

[94] Shin, L. (2022, February 23). *Exclusive: Austrian programmer and ex crypto CEO likely stole $11 billion of ether*. Forbes. https://www.forbes.com/sites/laurashin/2022/02/22/exclusive-austrian-programmer-and-ex-crypto-ceo-likely-stole-11-billion-of-ether/?sh=7e5f457f7f58

AlphaBay:

The darknet market, AlphaBay, was the largest of its kind at the time of the operation[95], perceived as the successor of a prior darknet market, "The Silk Road," which was also taken down by law enforcement.

In 2017, the FBI led a joint operation involving the cooperation of law enforcement agencies from Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, along with Europol.[96] The operation aimed to seize AlphaBay's servers and is arguably one of the most sophisticated joint operations at this scale. The website's creator, Alexandre Cazes, 25 years old at the time, was a Canadian citizen who was living in Thailand prior to his arrest by Thai authorities on behalf of the United States.[97] A quote from the FBI's article describes the investigation as follows "FBI and its partners used a combination of traditional investigative techniques along with sophisticated new tools to break the case and dismantle AlphaBay."[98] A statement by FBI Special Agent Chris Thomas states, "The message to criminals is: Don't think that you are safe because you're on the dark web. There are no corners of the dark web where you can hide." [99]

[95] FBI. (2017, July 20). *Alphabay takedown*. FBI. https://www.fbi.gov/news/stories/alphabay-takedown
[96] Ibid., 95.
[97] Ibid., 95.
[98] Ibid., 95.
[99] Ibid., 95.

A key breakthrough in the AlphaBay investigation, not talked about very publicly, involved the efforts of IRS agent Tigran Gambaryan and Chainalysis' co-founder Jonathan Levin, who played a significant role behind the scenes. They were able to track AlphaBay's server IP address through blockchain surveillance, which helped the FBI in their seizure of the server.[100] While the exact method of how it was accomplished remains a trade secret, it is speculated that this was done by placing nodes on the blockchain which listen to the incoming broadcasted transaction during the verification process discussed in Chapter 1 of this paper. These nodes appear to be able to overhear and record the IP addresses behind those transactions. The method behind the technology has not been confirmed, but its desired purposes were demonstrated to be achievable, contrary to the commonly held assumption that it was impossible to obtain identifiable information through the blockchain.[101]

Welcome to Video:

The dark net market solely dealt with child sexual exploitation material and was the largest of its kind in terms of volume.[102] The investigation and arrest of the perpetrators involved a joint effort between various entities, including the Internal Revenue Service – Crime Investigation Unit (IRS-CI), Homeland Security Investigations

[100] Ibid., 67.
[101] Ibid., 67.
[102] DOJ. (2020, December 7). *South Korean national and hundreds of others charged worldwide in the takedown of the largest darknet child pornography website, which was funded by Bitcoin*. The United States Department of Justice. https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

(HIS), the National Crime Agency in the United Kingdom, and Korean National Police in South Korea.[103]

Jong Woo Son, the South Korean citizen who is serving his jail sentence in South Korea, was 23 years old at the time of the indictment in 2018. He masterminded the website, which transacted in Bitcoin for purchasing the materials. IRS-CI Chief Don Fort stated in a quote, "Through the sophisticated tracing of bitcoin transactions, IRS-CI special agents were able to determine the location of the Darknet server, identify the administrator of the website and ultimately track down the website server's physical location in South Korea."[104] Chainalysis later came out later to confirm that it assisted in the investigation by using the "Reactor" tool discussed in subsection 5.1.1.[105]

Thanks to all the various collaboration efforts by cross-jurisdictional law enforcement, blockchain analysis firms and exchanges who divulged identification information about the suspected wallets which had funds tying them back to WTV, the website's server was successfully seized.[106] This enabled them to share server data with other law enforcement agencies worldwide, helping to identify and prosecute international customers of the site. As a result, 23 minors in the United States, Spain, and the United Kingdom who were being actively exploited by the website's customers have

[103] Ibid., 102.
[104] Ibid., 102.
[105] Team, C. (2022a, May 20). *Chainalysis in action: DOJ announces shutdown of largest child pornography website*. Chainalysis. https://blog.chainalysis.com/reports/chainalysis-doj-welcome-to-video-shutdown/
[106] Ibid., 102.

been rescued. Furthermore, leads were provided to 38 countries, which led to the arrest of 337 subjects in the U.S. and around the globe.[107]

As we conclude the subsection on darknet markets, we summarize a number of key takeaways for IFAs, given the continuous emergence of these markets.

Lessons Learned:

1- Due to the decentralized nature of blockchain transactions and its accessibility worldwide, individuals involved in a particular scheme can be spread across the globe. This can make investigations and enforcement action by one jurisdiction quite challenging. However, cross-jurisdictional collaborations and globally organized investigations can be an effective remedy to this issue, especially if countries have extradition laws or have good relationships with each other.

2- Traditional forensic investigative techniques such as the ones employed in the above cases have proven to be effective, especially when coupled with new technologies, they can be even more powerful.

3- Darknet Markets will always exist. AlphaBay and various other markets after it came as successors to prior darknet markets that were shut down. It does seem that as law enforcement stops one fire, another one starts in a different location. Chainalysis' analytics indicate that when a market shuts down, the admins create a new market and direct the previous market's vendors and customers to it.[108] This

[107] Ibid., 102.
[108] Ibid., 53.

indicates that IFAs must be acutely aware of how these markets operate and stay vigilant by monitoring administrators' activities as they move to a new market after one is shut down. IFAs must also be well-informed of new technologies that aid the investigative process.

4- The techniques used by Tigran Gambaryan and Chainalysis' co-founder Jonathan Levin to trace IP addresses through blockchain surveillance prove that the blockchain analytics might even be more transparent than initially believed. More so, it hints that as tracing and analysis technology advances, referring to the blockchain as anonymous might become obsolete.

5.1.4 Ransomware

In 2022, ransomware attackers extorted approximately $456.8 million from victim entities, which is lower compared to the prior year's total of around $765.6 million.[109] It is important to reiterate that numbers reported by Chainalysis are lower bound estimates due to the same reasons mentioned in the 5.1.1 subsection.

It is well known that ransomware attacks have been widely employed in the past few years by various illicit actors, such as in the case of Colonial Pipeline, a major American oil pipeline that suffered a ransomware attack that brought its systems to a halt. Ransomware attacks typically involve infecting an entity's system or infrastructure with malware, which denies access to computers or compromises sensitive data servers.

[109] Ibid., 53.

Attackers require a ransom, typically in the form of cryptocurrency, in return for the safe release of the data or the computers that are held, hostage. The analysis of blockchain transactions draws a clear picture of how ransomware attackers work. The business model is based on a win-win agreement involving two key players: ransomware developers and affiliates. The developers create the mechanisms behind the malware, and they permit affiliates to deploy it on victims in exchange for a portion of the ill-gotten gains.[110]

The decline in ransomware revenue appears to be a result of enhanced security measures taken by targeted companies. More importantly, a growing trend shows that targeted businesses are outright refusing to pay attackers.[111] This is a healthy sign that businesses are learning from prior mistakes made when cyber security and its infrastructure were not met with the seriousness they required.

As we conclude the subsection on ransomware, below are a number of key takeaways for IFAs.

Lessons Learned:

1- The data obtained through "address overlap" analysis tools and the technical analysis of ransomware code suggest that, just like scamming networks, the ransomware ecosystem might be much smaller than originally perceived. The data shows that affiliate and administrators' wallet addresses overlap in different types

[110] Ibid., 53.
[111] Ibid., 53.

of ransomware software. In other words, while there may be various types of ransomware, the people or groups responsible for them could be the same. These insights obtained thanks to the blockchain's transparency can help concentrate investigation and seizure efforts on the biggest players.

2- As discussed, victim entities are refusing to pay ransoms. There are two major reasons for this change in behaviour. First, upon pressure from regulators, entities have become more hesitant to pay as they may face legal consequences. Regulators in the U.S., such as OFAC, have warned against making such payments, as the funds may end up in the hands of sanctioned entities or individuals.

Second, cyber insurance firms have implemented stricter underwriting requirements to allow ransom payment coverage which had a significant impact on this shift. In a conversation with Chainalysis, Michael Phillips, a Chief Claims Officer of a cyber insurance firm called "Resilience," stated, "Today, companies have to meet stringent cybersecurity and backup measures to be insured for ransomware coverage. These requirements have proven to actively help companies bounce back from attacks rather than pay ransom demands. An increased focus on underwriting against factors that contribute to ransomware has led to lower incident costs for companies and contributed to a decreasing trend in extortion payments."[112]

5.1.5 Money Laundering

[112] Ibid., 53.

Laundering of cryptocurrencies is a rite of passage for every type of cybercriminal. Money laundering in cryptocurrency is a large concern. Cybercriminals' aim is to transfer funds to addresses where their criminal origin cannot be traced. The goal is to convert the cryptocurrency into cash, likely through exchanges, where it can be used without detection.[113] The practice of converting ill-gotten cryptocurrencies into tangible cash severs its connection to the blockchain, which also breaks off the trail investigators can follow. Without effective Anti-Money Laundering measures in place, the motivation for engaging in cybercriminal activities involving cryptocurrency will persist.

Money Laundering typically falls under two main entities and service categories[114]:

Intermediary services and wallets:

As previously discussed in this chapter, cybercriminals have found tools to hide the movement of illicit funds from one wallet to another through the use of DeFi protocols such as mixers and darknet markets. In some cases, more sophisticated DeFi protocols and, particularly, decentralized exchanges are also used. However, their increased transparency proves they are a less effective obfuscation measure.

Fiat Off-ramps:

[113] Ibid., 53.
[114] Ibid., 53.

As discussed, these refer to services that allow the conversion of cryptocurrencies to fiat money. It is an attractive tool for cybercriminals and is commonly utilized through centralized exchanges. Even though there are other options available, centralized exchanges remain the popular choice for criminals. As mentioned in Chapter 3, nearly half of the $23.8 billion laundered in 2022 was traced back to centralized exchanges. Cybercriminals' use of these services can raise some concerns for investigators. First is the previously discussed severance of the digital trail if the illicit funds are exchanged into fiat and eventually integrated into the economy. Second, if funds are deposited into an exchange, they're held in pools which co-mingle all deposits that are only visible to those exchanges making the tracing ability less effective.[115] The second issue highlights the crucial role that exchanges play in implementing measures such as KYC and customer due diligence, in addition to their cooperation with law enforcement and regulators, which can provide effective remedies in an investigation setting. This is because when criminals attempt to launder funds through regulated and complaint exchanges, those exchanges can provide the required information that helps investigators detect and identify launderers.

As we conclude the subsection on money laundering, below are a number of key takeaways for IFAs to keep in mind, given the prevalence of this activity in the crypto ecosystem.

Lessons Learned:

[115] Ibid., 81.

1- Centralized exchanges are an important stop for cybercriminals hoping to launder money. However, prior to placing illicit funds in exchanges, cybercriminals may use intermediaries such as mixers or DeFi protocols. Those tools are used to add a layer of privacy as they obfuscate the sources of funds to make them harder to trace.[116] As such, special care must be taken by IFAs as they attempt to trace mixed funds.

2- In the case of mixers, de-mixers can be used. While the technology is still quite complex and not widely used, it exists and is expected to develop further as technology evolves.[117] In terms of DeFi protocols, their key feature is that they are accessible on the blockchain. An example is decentralized exchanges, where cybercriminals typically exchange illiquid digital assets such as tokens for more liquid assets such as stablecoins to eventually exchange them at centralized exchanges for fiat. The movement from decentralized exchanges to a centralized exchange is possible to trace as it would be on the blockchain.[118]

3- In the case of centralized exchanges, investigators are not without options. If investigators need to trace the movements of illegal funds in a service deposit address, such as in a regulated, centralized exchange, they can collaborate with the compliance teams of the services involved as they track the KYC information behind wallet addresses. It is advisable for investigators to contact these services to gather information on where a user has transferred funds after depositing them.

[116] Ibid., 53.
[117] Ibid., 53.
[118] Ibid., 53.

In other cases, investigators working with law enforcement may also obtain this information by issuing a subpoena.[119]

5.1.6 Lessons from OFAC Sanctions

Government agencies such as the Office of Foreign Assets Control (OFAC), which effect sanctions against targeted countries, individuals, or entities that pose a threat to national security and foreign policy, have begun to shift their attention to sanctioning these threat sources in the crypto ecosystem. The effectiveness of these sanctions was initially met with skepticism, but we will discuss their success below.

Historically, traditional sanctions enforcement relied on financial institutions, however, with the emergence of the blockchain, threat actors shifted their activities there as it allowed them to circumvent these traditional intermediaries. In 2022, OFAC designated what is considered the largest number of cryptocurrency services to date, targeting a wider array of service types for various reasons. Centralized crypto exchanges were less of a challenge to implementing sanctions and have demonstrated that sanctions can be enforced in the crypto world.[120] This is likely due to the existence of a central entity or individual to sanction.

However, we discuss an example of the first DeFi protocol to be sanctioned by OFAC for facilitating the money laundering of funds stolen by hackers linked with North

[119] Ibid., 81.
[120] Ibid., 53.

Korea, Tornado Cash. This is a DeFi-based cryptocurrency mixer that can obscure currency movement. Unlike in a centralized service, the challenge with sanctioning a DeFi protocol is that there is no overseeing person or organization that controls it, which raises the question of would be held accountable. The answer to this question lies with the users of Tornado Cash. As a global service, Tornado Cash had many users who could face the consequences of violating U.S. sanctions or being cut off from other services if their wallets exhibited exposure to Tornado Cash. As a result, sanctions against decentralized services acted as a deterrent to using rather than cutting off usage completely. In this case, Chainalysis reported a 68% decrease in inflows in the 30 days following Tornado Cash's designation. This is significant because mixers become less effective for money laundering the fewer funds they receive overall.[121] Although to a limited degree, this shows that sanctions can be an effective tool against threat sources on the blockchain.

5.2 The Crypto Fraud Diamond:

Through the research performed for this paper, several trends were observed. These trends can assist IFAs in better understanding why cybercriminals and at least a portion of traditional criminals have chosen to engage in criminal activities within the crypto ecosystem. Studies show that understanding the components which drive people to commit fraud is a key factor in strengthening prevention, deterring and detection efforts

[121] Ibid., 53.

performed by IFAs.[122] For this purpose, the fraud triangle was developed and widely adopted as a pivotal tool in the IFA's arsenal. The fraud triangle's framework consists of three components, pressure to commit fraud, an observed opportunity and finally, a way for the offender to rationalize their behaviour and justify it to themselves to alleviate guilt.[123]

In 2004, Kennesaw State University published a paper titled *The Fraud Diamond: Considering the Four Elements of Fraud* by David T. Wolfe, a CPA and founder of Glasgow Forensic Group and Dana R. Hermanson, a Ph.D. and professor of accounting in the Coles College of Business at Kennesaw State University at the time the paper was issued.[124] Their research suggested including a fourth component to the fraud triangle, which is "capability." The authors argue that for fraud to occur, it is important to have the right person with the necessary abilities in the appropriate position.[125] The argument of the "capability" component can be appropriately applied to fraudsters in the crypto ecosystem.

Throughout history, there have always been individuals who attempt to deceive others through fraudulent means. However, when it comes to the crypto ecosystem, not all fraudsters possess the knowledge and skillset necessary to successfully carry out

[122] Wolfe, D. T., & Hermanson, D. R. (2004). *The fraud diamond: Considering the four elements of fraud*. Kennesaw State University . https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs
[123] W. Steve Albrecht. (2014). *Iconic Fraud Triangle endures*. Fraud Magazine. https://www.fraud-magazine.com/article.aspx?id=4294983342

[124] Ibid., 122.
[125] Ibid., 122.

financial crimes within it. For these reasons, to conduct the analysis for this research, the fraud diamond framework has been adopted, as demonstrated in Figure 1.6 below.

It is also worth establishing that although this assumption remains that not many people can proficiently use blockchain technology, this doesn't mean that only a select few can access it or generally use it. In fact, almost anyone with an internet connection can use blockchain technology, and there are plenty of free resources available online to learn more about it. However, this paper assumes that mastering these skills can be a complex and lengthy process and that individuals mastering it would typically be already technologically inclined. Additionally, not all users of the crypto ecosystem engage in it for fraudulent reasons, as it has already been long established that the ecosystem has various legitimate uses for investors and other types of users.

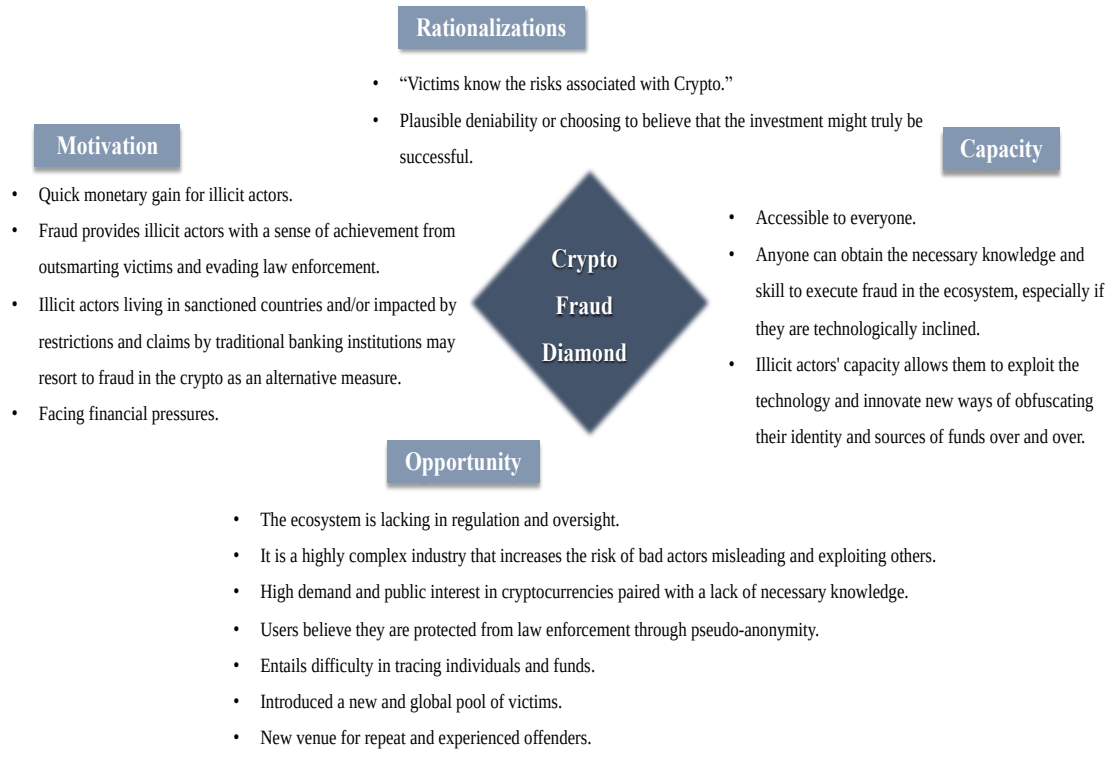

Figure 1.6

The crypto fraud diamond provides valuable insights for IFAs to better understand the drivers of crime in the crypto ecosystem. Having this foundation can serve as a background when shaping more effective prevention and detection measures for clients of the IFA.

Conclusion

In this chapter, we have discussed several of the prominent financial crimes in the crypto ecosystem, but it's important to remind the readers that this is not an exhaustive list and that, as the technology evolves, it is expected to see the same schemes taking different forms. In addition, we delved into a sample of successful crypto investigations and analyzed the blockchain analysis tools which aided in their success. Further to their success in tracing funds for a specific investigation, a feature that is only expected to improve with time, blockchain analysis tools have proved their ability to provide insights which can aid future investigations. An example of this includes the indicators of large-scale scams being potentially done by a small group of scam networks. The same applies to ransomware attacks, where the same small group of affiliates may be changing the ransomware software, giving the impression that they are a different hacker. These insights can also further help us understand cybercriminals' motivations, capabilities, and the opportunities they seek to perform their crimes.

CONCLUSION

This research aimed to demystify the crypto ecosystem from an IFA perspective and, in the process, question the myth of anonymity behind the blockchain. With these key statements in mind, this paper demonstrated how obtaining a deeper understanding of the crypto ecosystem can provide valuable benefits and insights for IFAs in terms of implementing better investigative techniques, strategies, and tools. In addition, understanding the crypto ecosystem's fundamentals can provide valuable data into the trends and behavioural patterns taken by criminals to obtain and launder illicit funds. This data can be used for the analysis of how prevention and safeguarding measures can be effectively implemented.

The DLT encompasses any system that operates without a central authority. The blockchain utilizes the DLT technology to link, verify and record transactions in a secure and decentralized manner. It is transparent in the sense that transactions are publicly recorded and available. This transparency is key to any investigative approach or method the IFAs undertake to investigate crime in the crypto ecosystem. Many of the tools crafted for the purposes of monitoring and tracing funds on the blockchain at the time of writing this paper have been based on this fundamental trait. Investigators and regulators must have a deeply rooted awareness of the blockchain's transparency. The clustering heuristic rules developed by Sarah Meiklejohn and other researchers were one of the earliest investigative techniques rooted in the ability to see transactions on the blockchain. These rules have been engaged as early tools for analyzing data on the blockchain and have proved to be effective in identifying patterns and relationships

between different transactions. By proving that wallet addresses can be tied to owners of other addresses, we are able to take steps to follow the money and analyze behaviour taken by criminals in an effort to hide the sources of funds by moving them from one wallet to another. In addition, since the time Meiklejohn issued her paper in 2012, many advanced blockchain analysis tools have been developed and adopted in investigations where they have been proven to be effective in tracing funds and identifying cybercriminals and their pattern of behaviour.

While this paper decrypted various fundamental concepts in the crypto ecosystem and the role they play in enabling and combating crime to better assist IFAs, this is not an exhaustive list. The crypto ecosystem is still in its infancy and continues to develop rapidly in complexity. New concepts appear to constantly emerge, and some of the terms used in the ecosystem also continue expanding to encompass other tools, protocols and services. In addition, crypto crime remains on an upward trajectory, and cybercriminals continue to uncover novel ways of exploiting the ecosystem for their personal gain. However, this paper contends that the view of investigating, regulating and implementing enforcement action in the crypto ecosystem is not bleak and that IFAs and regulators should maintain a cautiously optimistic perspective in order to find innovative methods to keep pace with the prevalent crimes and effectively harness the power of blockchain technology to combat illicit activities. It is also highly recommended that further research be conducted on the crypto ecosystem as it develops to continuously assess its impact on the IFA profession.

Bibliography

a16z crypto. (2022, December). *De-Anonymization in Bitcoin with Sarah Meiklejohn | a16z crypto research talks*. YouTube. https://www.youtube.com/playlist?list=PLjQ9HCQMu_8yPGgfvsscHgt1w1KJkx8BN

Beyond the Hype. Retrieved April 29, 2023, from https://www.cfainstitute.org/-/media/documents/article/industry-research/Crypto_Fiduciaries-and-Institutional-Investors.pdf

Chainalysis. (2023). *Chainalysis 2023 Crypto Crime Report* . Chainalysis. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

Chainalysis. (2023b, June 5). *Cryptocurrency investigation software - chainalysis reactor*. Chainalysis. https://www.chainalysis.com/chainalysis-reactor/?utm_source=google&utm_medium=cpc&utm_campaign=%7Bcampaign%7D&utm_term=chainalysis&utm_content=579138555250&gclid=CjwKCAiA_vKeBhAdEiwAFb_nrXnYyHoYLdS0cw7yZ5cKMaE4oKDRB2a8iLNNmvfmVLz298CmQLq63BoC3hQQAvD_BwE

Chainalysis Team. (2020, February 4). *Who's Who on The Blockchains? The Chainalysis Guide To Cryptocurrency Typologies*. Typologies Report. Retrieved April 30, 2023, from https://go.chainalysis.com/rs/503-FAP-074/images/Typologies-Report-final.pdf

Coinbase. (n.d.). *What is a fork?*. Coinbase. https://www.coinbase.com/learn/crypto-basics/what-is-a-fork

CSA. (2022a, August 15). *Canadian securities regulators expect commitments from crypto trading platforms pursuing registration*. Canadian Securities Administrators. https://www.securities-administrators.ca/news/canadian-securities-regulators-expect-commitments-from-crypto-trading-platforms-pursuing-registration/

CSA. (2022, December 12). *CSA provides update to crypto trading platforms operating in Canada*. Canadian Securities Administrators. https://www.securities-administrators.ca/news/csa-provides-update-to-crypto-trading-platforms-operating-in-canada/

Deane, S., & Fines, O. (2023, January 4). *Cryptoassets Beyond the Hype - An Investment Management Perspective on the Development of Digital Finance*. Cryptoassets:

DOJ. (2020, December 7). *South Korean national and hundreds of others charged worldwide in the takedown of the largest darknet child pornography website, which was funded by Bitcoin*. The United States Department of Justice. https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

Edelberg, W., Cohen, G. J., Seefer, C., & Feldberg, G. (2011, February 25). The Financial Crisis Inquiry Report - Gov Info. https://www. https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pd

Euromoney. (n.d.). *How does a transaction get into the blockchain?*. Blockchain Explained: How does a transaction get into the blockchain? | Euromoney Learning. https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain

FBI. (2017, July 20). *Alphabay takedown*. FBI. https://www.fbi.gov/news/stories/alphabay-takedown

Frankenfield, J. (2023a, January 16). *Altcoin explained: Pros and Cons, types, and future*. Investopedia. https://www.investopedia.com/terms/a/altcoin.asp

Frankenfield, J. (2023, February 10). *What are smart contracts on the blockchain and how they work*. Investopedia. https://www.investopedia.com/terms/s/smart-contracts.asp

Gogel, D., Taylor, T. B., Cloots, A. S., Forster, B., Gustave, J. L., Schär, F., & Sokolin , L. (2021). *DeFi beyond the hype - Wharton Initiative on Financial Policy and Regulation*. University of Pennsylvania. https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf?ref=tokendaily

Global cryptocurrency market charts. CoinMarketCap. (n.d.). https://coinmarketcap.com/charts/

Greenberg, A. (2023). *Tracers in the dark: The global hunt for the Crime Lords of Cryptocurrency*. Knopf Us.

He, X., He, K., Lin, S., Yang, J., & Mao, H. (2022, May 31). *Bitcoin address clustering method based on multiple heuristic conditions*. Institution of Research And

Technology. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12014

Khatri, Y., & Copeland, T. (2022, February 23). *A look at Chainalysis' claim to track bitcoin through mixing service coinjoin*. The Block. https://www.theblock.co/post/135148/a-look-at-chainalysis-claim-to-track-bitcoin-through-mixing-service-coinjoin

Kohler, C. (2022, March 13). *Can your bitcoin be seized by governments?*. The Bitcoin Manual. https://thebitcoinmanual.com/articles/can-bitcoin-seized/

Leng, S. (2020, December 1). *Chinese cryptocurrency platform ringleaders jailed in US$2.25 billion scam*. South China Morning Post. https://www.scmp.com/economy/china-economy/article/3112115/chinese-cryptocurrency-scam-ringleaders-jailed-us225-billion

Mastando, M. (2023, March 15). *Why do blockchains need oracles?*. Forbes. https://www.forbes.com/sites/digital-assets/article/why-do-blockchains-need-oracles/#:~:text=Oracles%20are%20lines%20of%20code,%2C%20and%20off%2Dchain%20data.

Merle, R. (2018, September 10). *A guide to the financial crisis - 10 years later*. The Washington Post. https://www.washingtonpost.com/business/economy/a-guide-to-the-financial-crisis--10-years-later/2018/09/10/114b76ba-af10-11e8-a20b-5f4f84429666_story.html

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, December). *A fistful of bitcoins: Characterizing payments among men with no names*. University of California San Diego. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Merle, R. (2018, September 10). *A guide to the financial crisis - 10 years later*. The Washington Post. https://www.washingtonpost.com/business/economy/a-guide-to-the-financial-crisis--10-years-later/2018/09/10/114b76ba-af10-11e8-a20b-5f4f84429666_story.html

Nakamoto, S. (2008, October 31). *A peer-to-peer electronic cash system*. Bitcoin. Retrieved April 29, 2023, from https://bitcoin.org/en/bitcoin-paper

Nelson, D. (2023, May 9). *Inside chainalysis' multimillion-dollar relationship with the US Government*. CoinDesk . https://www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government/

Okta (2023, February 14). *The plustoken cryptocurrency scheme: Architecture and exposure*. Okta. https://www.okta.com/identity-101/plus-token/

Pisa, M. (2018). *Initial Coin Offering (ICO) mania and its implications for technology-led Social Enterprise*. Center For Global Development | Ideas to Action. Retrieved April 30, 2023, from https://www.cgdev.org/blog/initial-coin-offering-ico-mania-and-its-implications-technology-led-social-enterprise

Protocol, T. B. (2019, May 14). *The evolution of the Decentralized Exchange: A brief history*. Medium. https://theblocknetchannel.medium.com/the-evolution-of-the-decentralized-exchange-a-brief-history-888ee0ce1803

Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Vagneur, K., & Zhang, B. Z. (2019, December 18). *Distributed Ledger Technology Systems: A conceptual framework*. SSRN. https://deliverypdf.ssrn.com/delivery.php?ID=274113064065074065091066116066087107105033003077055038110067092100120114005106015071001030031003012032002100109028026115030026039038064079079117011092005113102027077036087049117015065093126011091096122068022088123005098088124102120121029089105090093078&EXT=pdf&INDEX=TRUE

Reiff, N. (2023, May 25). *Decentralized Autonomous Organization (DAO): Definition, purpose, and example*. Investopedia. https://www.investopedia.com/tech/what-dao/

Rosenberg, E. (2023, February 28). *What are cross-chain bridges?*. Investopedia. https://www.investopedia.com/what-are-cross-chain-bridges-6750848

SCHÄR, F. (2022, September). *Defi's promise and pitfalls - IMF*. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/Fandd/Article/2022/September/Schar.ashx

Shin, L. (2022, February 23). *Exclusive: Austrian programmer and ex crypto CEO likely stole $11 billion of ether*. Forbes. https://www.forbes.com/sites/laurashin/2022/02/22/exclusive-austrian-programmer-and-ex-crypto-ceo-likely-stole-11-billion-of-ether/?sh=7e5f457f7f58

SEC. (2022, December 14). *Press release - SEC Charges Eight Social Media Influencers in $100 Million Stock Manipulation Scheme Promoted on Discord and Twitter*. SEC Emblem. https://www.sec.gov/news/press-release/2022-221

Stein, L., & Sorell, R. (2022, November 11). *Retail investment limits under the Canadian Crypto Asset Trading Platform (CTP) regulatory regime*. McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/techlex/retail-investment-limits-under-canadian-crypto-asset-trading-platform-ctp-regulatory-regime

Team, C. (2022, May 20). *Why you can't trace funds through services using blockchain analysis (and why you don't need to anyway)*. Chainalysis. https://blog.chainalysis.com/reports/blockchain-analysis-trace-through-service-exchange/

Team, C. (2022a, May 20). *Chainalysis in action: DOJ announces shutdown of largest child pornography website*. Chainalysis. https://blog.chainalysis.com/reports/chainalysis-doj-welcome-to-video-shutdown/

Team, C. (2022b, August 10). *Cross-chain bridge hacks emerge as top security risk*. Chainalysis. https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/

Team, C. (2023, February 16). *Crypto pump and dump schemes make up 24% of new tokens*. Chainalysis. https://blog.chainalysis.com/reports/2022-crypto-pump-and-dump-schemes/

Team, E. (2021, August 15). *The keys to crypto kingdom: Wallet address, public and private keys explained*. Blocktrade. https://blocktrade.com/wallet-addresses-public-and-private-keys-explained/

Trozze, A., Kamps, J., Akartuna, E. A., J. Hetzel, F., Kleinberg, B., Davies, T., & D. Johnson, S. (2022). *Cryptocurrencies and future financial crime*. Crime Science Journal. Retrieved May 1, 2023, from https://crimesciencejournal.biomedcentral.com/counter/pdf/10.1186/s40163-021-00163-8.pdf

Tuwiner, J. (2023, May 22). *9 major companies who accept bitcoin [spend crypto 2023]*. 9 Major Companies Who Accept Bitcoin [Spend Crypto 2023]. https://buybitcoinworldwide.com/who-accepts-bitcoin/

W. Steve Albrecht. (2014). *Iconic Fraud Triangle endures*. Fraud Magazine. https://www.fraud-magazine.com/article.aspx?id=4294983342

Wolfe, D. T., & Hermanson, D. R. (2004). *The fraud diamond: Considering the four elements of fraud*. Kennesaw State University . https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=2546&context=facpubs

Appendix

DeFi Building Blocks:

Blockchains:

DeFi services have primarily operated on the Ethereum blockchain due to its abilities and mass adoption, with transactions being settled on distributed ledgers (Blockchain). Nonetheless, as a result of rapid development, DeFi activity is also expanding across other public blockchains.

Digital Assets:

Bitcoin, among other cryptocurrencies, was the pioneer in the ecosystem of blockchain-based digital assets. As the technology evolved, tokens were introduced as a means of representing value or interest, which can be easily exchanged within the network, similar to the mechanism of stocks on traditional exchanges. While these two digital assets are some of the more familiar ones, various other assets were developed for purposes beyond just payments, further expanding the sphere of DeFi technology.

Wallets:

Based on software, wallets allow participants to administer their digital assets. There are two types of wallets: non-custodial and custodial. Non-custodial wallets provide users with full control of their assets through their private keys, whereas custodial wallets have service providers manage the private keys on behalf of the users.

Smart Contracts:

Smart contracts allow users to execute deals and commands through written code of if/then statements[126]. By being based on blockchain software code, smart contracts are secure and do not require the existence of a third party to oversee execution. Functions are automatically executed when agreed conditions or terms are fulfilled.[127]

Decentralized Applications (DApps):

Smart contracts are utilized to create software applications that are usually combined with user-friendly interfaces (UI) with the use of standard web technology.

Governance Systems:

Software-based tools typically used to implement changes on smart contracts that have been approved by stakeholders through voting, particularly in the context of tokens which grant voting rights.

Decentralized Autonomous Organizations (DAOs):

Decentralized entities operate on rules ascribed and enforced on smart contracts. Stakeholders, referred to as Tokenholders, hold decision-making voting power.[128]

Stablecoins:

[126] Ibid., 31.
[127] Ibid., 22.
[128] Reiff, N. (2023, May 25). *Decentralized Autonomous Organization (DAO): Definition, purpose, and example*. Investopedia. https://www.investopedia.com/tech/what-dao/

Cryptocurrencies that have their values tied to a fiat currency, a combination of fiat currencies, or other stable-value assets. An example of a Stablecoins is Tether (USDT) which is pegged to the US dollar. They are characterized as being more stable due to their connection with fiat.

Oracles:

Described as data feeds which enable DeFi services, such as smart contracts, to incorporate information from sources outside of the blockchain, for example, information on fiat currency prices. They operate like a bridge which connects off-chain information to on-chain blocks.[129]

[129] Mastando, M. (2023, March 15). *Why do blockchains need oracles?*. Forbes. https://www.forbes.com/sites/digital-assets/article/why-do-blockchains-need-oracles/#:~:text=Oracles%20are%20lines%20of%20code,%2C%20and%20off%2Dchain%20data.