Journal of Forensic and Investigative Accounting
Volume 17: Issue 1, January–June 2025

Decrypting the Investigation of Cryptocurrency Fraud: A Discussion of Challenges, Recommendations, and Future Research

Michael Killey
Stephanie Walton
Oscar Harvin

Introduction

Public faith in the fiat monetary system was significantly impaired due to numerous international financial catastrophes that resulted from the questionable actions of institutional leaders during the late 20th and early 21st centuries (Chafee, 2018; Florea and Nitu 2020). In 2009, cryptocurrency, a purely electronic medium of exchange, was introduced for global citizens who preferred a store of economic value that was less subject to government manipulation or oversight (Florea and Nitu, 2020; Hamil, 2020).[1] Since the alternative monetary form was introduced, cryptocurrency demand has continually surged (Kerr et al., 2023). Businesses, investors, and individuals conducting personal financial transactions are amongst those who employ the electronic medium of exchange for monetary transactions (ACFE, 2022). Many leading global corporations are accepting Bitcoin, the most demanded type of cryptocurrency, payments and the magnitude of cryptocurrency transactions has exceeded $15 trillion since 2021 (Jacquelyn, 2021; Kerr et al., 2023).

Cryptocurrency transactions are dependent on blockchain, a decentralized platform that utilizes distributed digital ledgers to permanently and reliably document transactions in a sequential, public manner (Reid and Harrigan, 2013; Joo et al., 2023).[2] The technology utilizes a cryptographic, open-sourced peer-to-peer network that provides any individual the opportunity to access the technological infrastructure and transmit information (Liedel, 2018). When utilizing blockchain, users do not operate under the authority or protection of authoritative of third parties (Arnsten, 2021). The anonymity of the transactions and the obscuring of the parties affiliated with the cryptocurrency exchanges provides significant value for those who seek to avoid transactional hassles and regulatory scrutiny for legitimate purposes (Pistoria et al., 2004; Florea and Nitu, 2020; ACFE, 2022).

However, cryptocurrencies also are utilized for illegal, illegitimate purposes (Liedel, 2018; Ankier, 2019; Florea and Nitu, 2020). The decentralized, anonymous nature of the network provides a fertile environment for the expansion of fraudulent behaviors, money laundering, tax evasion, and other illegal activities (Harvey, 2014; Ankier, 2019; ACFE, 2022). Further, as a result of the typical regulatory latencies that occur with nascent technology such as virtual assets, there are inconsistencies in reporting that allow for significant financial fraud (Kuegler, 2020). Indeed, there have been substantial increases in both the volume of fraudulent cryptocurrency transactions and the associated amounts of monetary losses (FBI, 2023).[3] Therefore, given the risks pertaining to virtual currencies, companies must adjust their governance systems in order to properly account for the new types of transactions and ensure compliance with legal standards (Vincent and Wilkins, 2020). Traditional control procedures and investigation techniques pertaining to fraud prevention, detection, and remediation need to be amended to account for digital assets and blockchain infrastructure.

---

[1] Example of cryptocurrencies include Bitcoin, Ethereum, Tether, BNB, USDC, XRP, Dogecoin, Cardano, and Toncoin, among others.

[2] Blockchain technology is the base technology underpinning cryptocurrencies. Blockchain technology occurs where "nodes collect new transactions into a block, hash them into a hash tree, and scan through nonce values to make the block's hash satisfy proof-of-work requirements. When they solve the proof-of-work, they broadcast the block to everyone, and the block is added to the block chain" (Nakamoto 2009). Then hash verification procedures, called mining, occur to add and link blocks within the chain. Once blocks are added then cannot be changed easily. Blockchain ledgers can be public or private and can be used for cryptocurrency, smart contract, or application development purposes.

[3] Cryptocurrency fraud also can be perpetuated through cryptocurrency trading platforms. For instance, Sam Bankman-Fried was sentenced to 25 years in prison on seven counts of fraud and conspiracy for stealing approximately $8 billion form the FTX cryptocurrency exchange he founded (Cohen and Godoy, 2024). Terraform Labs and Do Kwon, its founder, have reached a tentative civil fraud case settlement with the SEC for allegedly misleading cryptocurrency investors prior to the 2022 collapse of the stablecoin TerraUSD (Godoy, 2024). Kwon currently faces extradition from Montenegro to either the U.S. or South Korea pending court proceedings.

Accordingly, based on professional experience and the current literature, we develop guidance and suggestions that can be utilized by forensic professionals and other authoritative parties to create and implement strategies and tools for mitigating the fraudulent conduct associated with cryptocurrency transactions. The information and recommendations provided in the article also can be useful in reconsidering the current academic paradigms pertaining to fraud. First, we provide background information regarding cryptocurrency, blockchain technology, and relevant legal provisions. Second, we consider the current dominant theoretical framework pertaining to occupational fraud, the fraud triangle (Cressey, 1953) and argue our assertion that more advanced models may be needed when digital currency fraud is considered in a workplace setting. Our study then considers many of the common impediments and dilemmas associated with cryptocurrency fraud investigations. We extend this discussion by delineating recommendations for forensic professionals who are investigating and assisting with the prosecution of illicit cryptocurrency schemes. Finally, we provide suggestions for further academic research.

Literature Review

Cryptocurrency and Blockchain Technology Definitions

Cryptocurrencies are a digital medium of exchange that are used for investment and transactional purposes (Soni, 2021). Some cryptocurrencies can be exchanged into traditional fiat currency while other types are non-convertible and can only be utilized in specific domains (Cachanosky, 2022). While some cryptocurrencies have a singular administering authority, most varieties operate on an open-sourced, distributed, peer-to-peer network with no central oversight by a financial institution or other third-party intermediary (Liedel, 2018). The term open-sourced refers to the ease of accessing the technology and sharing the information. The public decentralized virtual ledger is protected and distributed across all the computers utilizing the technology. The ledger, known as blockchain, is not controlled by any particular entity and there is, therefore, less potential to institutional manipulation (Roper, 2021).

Blockchain refers to batched transactions linked in cryptographically connected blocks (Venkatesh, 2018). Each block contains transaction data and an encrypted mathematical cipher that encodes the data. Blocks are time-stamped, immutable, and added to the chain sequentially. Transactions are generally anonymous and conducted using wallets, storage software that engages with the blockchains in order to convey the virtual currencies between parties.[4] In order to conduct transactions, both public and private keys are utilized. The public key is the address that the cryptocurrency sender employs to transmit the asset while the private key is the address that the cryptocurrency receiver uses to accept the payment (Engle, 2015). Relative to traditional mediums of exchange, the value of virtual currencies is more closely aligned with their acceptance by individuals since the assets typically have little, if any, dependence on third-party institutions (Reynolds, 2017).

Cryptocurrency Usage

Given inflationary concerns pertaining to traditional currency and the advance of electronic commerce, the demand for cryptocurrency is rapidly increasing (Sage Group, 2022). Many developing countries are even considering implementing cryptocurrencies and other digital mediums of exchange as a mechanism for lowering operational costs and enhancing efficiencies, increasing the potential damage from security threats (International Monetary Fund, 2019). Further, many businesses are utilizing cryptocurrencies for a wide range of economic transactions and investment objectives. In addition, numerous organizations accept cryptocurrency as payment for goods or services (Sage Group, 2022).

Unfortunately, while the anonymity and relative freedom from third-party interference is attractive to users (Pistoria et al., 2004), the anonymity and decentralization of the transactions also enables a plethora of destructive illegal activities, including fraud (Dyson et al, 2019; Florea and Nitu, 2020). For instance, parties engaged in illicit activities have inappropriately utilized Silk Road, a dark web site that allows parties to purchase illegal goods and services, to mask substantial criminal activities from authorities by conducting exchanges through cryptocurrency transactions (Stroukal and Nedvedova, 2016). Further, the lack of third-party institutional involvement increases the likelihood that misappropriated funds will be permanently lost or stolen. However, even though cryptocurrency investigations face numerous challenges, the transactions do provide law enforcement with a timestamped, permanent record that can often be accessed without the approval of a foreign agency (Balaban, 2017). Given the ubiquity of digital mediums of exchange, those involved in an audit engagement, including forensic professionals, must seriously the challenges of virtual currencies when assessing both inherent and business risks (Dupuis et al., 2023). Since cryptocurrency fraud detection is becoming increasingly relevant to

[4] Wallets can either be hot (connected to the internet either via software or web-based) or cold (not connected to the internet via physical devices) (State of Connecticut Department of Banking, 2024).

business transactions (Hossain, 2023), fraud examiners must be familiar with both cryptocurrency regulation and the proper investigation tools.

Cryptocurrency Regulation

Current governance pertaining to the accounting and usage of cryptocurrency, however, is constrained. The usage of virtual currency is not receiving the same oversight as activities involving traditional securities in terms of audits, disclosures, and other reporting or record keeping requirements (Prewett et al., 2019). Many nations are experiencing difficulties enacting and enforcing functional taxation and licensing standards for cryptocurrency transactions (Anush et al., 2020).

Digital assets are also often subject to incongruous or inconsistent classifications. For instance, SEC regulations indicate that cryptocurrency is subject to national securities laws when utilized as an investment but is identified as a medium of exchange beyond agency scope when used for transactional purposes (Kuegler, 2020; Barton et al., 2022). Therefore, the SEC's equity disclosure framework is generally not applicable to cryptocurrency holders, including banks and exchanges (Schonberger, 2022). Further, even though an SEC Staff Accounting Bulletin (SAB) asks that cryptocurrencies and the associated risks be labeled as assets or liabilities on the balance sheet, several institutional authorities argue that mere disclosure is adequate (Schonberger, 2022). Further, the Internal Revenue Service (IRS) treats virtual currencies as property even though the assets are frequently utilized for transactional pseudo-monetary purposes (Mudroncik, 2022).[5]

To impede the illegal usage of cryptocurrencies and enhance confidence in blockchain technology, the United States Department of Justice (DOJ) established the National Cryptocurrency Enforcement Team (a component of FinCEN) to investigate and prosecute criminal activity pertaining to cryptocurrency (DOJ, 2023). FinCEN determined that cryptocurrency administrators and exchanges are money-service businesses required to adhere to the Bank Secrecy Act (BSA) and submit suspicious activity reports (DOJ, 2023). Parties merely sending or receiving digital currencies, however, are not required to comply with these standards. Even though domestic entities and individuals engaged in cryptocurrency transactions with prohibited countries are subject to sanctions by the Office of Foreign Assets Control (OFAC), international standards addressing cryptocurrency regulation are generally nebulous, incongruous, and unenforceable (DOJ, 2020).

In response to technological trends and concerns, President Biden issued Executive Order 14067, "Ensuring Responsible Development of Digital Assets" (Exec. Order No. 14067, 2022) in order to protect business stakeholders and secure the global economy (Koutmos, 2023). The initiative was intended to target particular illicit financial risks, including cybercrime, ransomware, money laundering, terrorism, narcotics, human trafficking, and proliferation financing. Another focus of the order was ensuring the payment integrity of the payment innovations associated with the new technology. The initiative also aimed to promote national security and encourage economic investment.

The international regulatory framework is also relatively nascent. Cryptocurrency is currently legal in 119 countries but only 62 of those regions have established regulations. Amongst the countries with cryptocurrency governance systems, 22 (35.5 percent) are members of the European Union (1971), 36 (58 percent) are autonomous countries while four (6.5 percent) are British Overseas Territories (Amase, 2023). The lack of substantive regulation in countries that have legalized cryptocurrency introduces concerns pertaining to economic security and investor protection for global businesses. Most countries that have regulated cryptocurrencies have merely applied traditional regulatory frameworks to cryptocurrency transactions. The adaption approach commonly involves the application of established anti-money laundering, tax, and counter-financing of terrorism laws to cryptocurrency activities.

There have been variations in implementation and enforcement. Countries such as Germany, France, and Japan have successfully developed regulatory frameworks for digital assets. Meanwhile, other significant advanced economies, including Canada, Italy, the United Kingdom, and the United States, have experienced considerable challenges due to the numerous governmental authorities and regulatory bodies in these countries (Hicks and Adams, 2023). Even though countries have facilitated crypto innovation through legalization initiatives, there have been numerous attempts to lessen fraud concerns associated with digital assets. For instance, the Financial Conduct Authority, the U.K. regulator, recently prohibited activity by Binance, the largest global crypto exchange, and began regulating stablecoins due to fraud concerns.

Nevertheless, despite reform efforts, the FBI and international agencies reported a significant increase in both the number of cryptocurrency fraud victims and the amount of the associated financial losses in recent years (DOJ, 2023). While many of the illicit activities involving digital currencies are investment or consumer schemes (Hetler, 2023), there are also

[5] That is, the sale of cryptocurrency would be treated as the sale of a capital asset.

numerous occupational based cryptocurrency frauds (ACFE, 2022). Since occupational fraud is considered the most costly and frequent form of global financial crime (ACFE, 2024), a proper modeling of occupational-based digital currency fraud would be helpful. The most common of these employment-based schemes were activities associated with bribery or kickback payments made in cryptocurrency (48 percent), conversion of misappropriated assets to cryptocurrency (43 percent), and cryptocurrency being utilized to launder other funds (35 percent).

Frameworks For Cryptocurrency Fraud

The Fraud Triangle

Since 1997, the fraud triangle has been the primary paradigm that practitioners, regulators, and academics have utilized to study, investigate, prevent, and detect occupation-based fraud (Schuchter and Levi, 2015; Boyle et al., 2018). The model is championed by the Association of Certified Fraud Examiners (ACFE) and serves as the basis for several fraud related regulatory pronouncements of the Public Company Accounting Oversight Board (PCAOB) and the International Accounting Standards Board (IASB) (IFAC, 2010; Buchholz, 2012). The paradigm also is ubiquitous in both professional practice and the academic literature (Morales et al., 2014). The framework utilized by Wells (2014), based upon research conducted by Cressey (1953), explicates that individuals are more likely to commit fraud when the potential fraudster encounters the triad of perceived financial pressures, discerned opportunities, and accepted rationalizations. The premise of the model is that all three factors must be sufficiently present for fraud to occur.

However, the fraud triangle does not properly account for certain factors that are likely to impact the incidence of fraudulent activity pertaining to cryptocurrencies. First, the model emphasizes justifications and external considerations but does not properly emphasize knowledge and skill-based influences that are highly relevant when examining cryptocurrency fraud. Similarly, the triangle paradigm focuses on the risk of attempted fraud but does not highlight the successful occurrence of the illicit activity (Buchholz, 2012). The link between effort and completion may be more tenuous due to the complexities related to digital currencies and blockchain technology. Moreover, Cressey (1953), when creating his model, envisioned the average fraudster as a middle-aged person who was not a career criminal or regularly engaged in criminal behavior. However, individuals may be pathological fraudsters who regularly engage in fraudulent conduct and do not require a financial pressure or rationalization to engage act (Schuchter and Levi, 2015). Given the unique multiplex challenges associated with executing cryptocurrency-related fraud, such as managing and disguising the virtual financial flows, individuals or networks engaged in the conduct may not reflect a typical fraudster. In addition, the fraud triangle does not account for certain personality factors that may present more frequently in those engaged in illicit digital currency schemes. Therefore, alternative models for understanding fraud may be more useful in forensic investigations pertaining to cryptocurrency.

The Fraud Diamond

Wolfe and Hermanson (2004) formulate a fraud diamond model that also considers whether an individual has the requisite technical capability and personal traits to commit fraud. The capability aspect assesses whether the person has the competence and skills to exploit opportunities to engage in fraud (Dorminey et al., 2010; Mushin et al., 2018). Capability includes a deep knowledge of the subject of the fraud as well as expertise in the associated accounting and auditing matters (Wolfe and Hermanson, 2004). The fraud diamond is more effective when detecting fraud and provides an entity with a more conservative fraud risk assessment when technical competence is imperative for successful execution of the illicit act (Boyle et al., 2015). However, since many individuals do not properly understand basic aspects of cryptocurrency and its underlying blockchain technology (Crypto Literacy, 2024), the inclusion of the competency aspect may not be imperative. Thus, the fraud diamond is likely not suitable for cryptocurrency fraud settings.

The Fraud Pentagon

Crowe's fraud pentagon theory supplements the earlier models by contributing a fifth variable, arrogance, to the design (Mushin et al., 2018). The arrogance aspect references an individual belief of superiority and a sentiment that the rules do not apply to oneself. A belief that one is better than others because of one's abilities is often a key aspect of arrogance (Cowan et al., 2019). Similarly, the MICE model (Buchholz, 2012), conceptualizes fraud in terms of money, ideology, coercion, and ego. Egoism, a core aspect of the MICE model, also addresses a belief that one is superior due to abilities or some other factors. Given the superior technological expertise required in order to manage, manipulate, and conceal maneuvers pertaining to digital currency and blockchain, the capability and arrogance components may be highly relevant for fraud investigations pertaining to digital technology.

The A-B-C Formula

Moreover, the A-B-C formula (Dorminey et al., 2012), another mechanism for classifying and assessing fraud, conceptualizes fraudulent behavior as a manifestation of a bad apple, a bad bushel, and a bad crop. According to the model, the individual is the bad apple, the bad bushel is reflective of societal and circumstantial forces that enable fraud, and the bad crop encompasses the relatively static ethical culture that exists within the individual's social groupings. While the opportunity element of the fraud triangle mainly addresses an organization's internal controls, the A-B-C formula also considers additional external forces (Dorminey et al., 2012). Currently, there are unique circumstantial and societal dynamics that are increasing the likelihood of fraudulent transactions involving cryptocurrency. One important consideration is that there is no central institution responsible for overseeing the legitimacy of virtual currency transactions given the decentralized nature of the system (Pandya et. al, 2022). Further, the Securities and Exchange Commission (SEC) indicates that virtual currency is subject to federal securities laws when utilized as an investment but not when treated as a medium of exchange (Chaffee, 2018). Since organizations could manipulate the usage classification, regulatory scrutiny can be avoided. Similarly, there is also significant inconsistency and confusion regarding which governing bodies (such as the SEC, FBI, state law enforcement agencies, etc.) have the authority to investigate and prosecute cyber fraud (Naqvi, 2018). Therefore, the A-B-C formula, which does consider a broader array of external environmental forces, may also be more helpful when attempting to model the likelihood of cryptocurrency fraud and other cyber-crimes. *[See Table 1, pg. 140]*

Cryptocurrency Fraud Challenges

While having an appropriate model for assessing the likelihood of fraud is important, fraud examiners also face other numerous challenges when investigating and prosecuting both internal and external cryptocurrency fraud. Unlike other types of criminal activity, digital currency fraud is difficult to prosecute due to the lack of physical evidence and recovery of losses is problematic due to the irreversible nature of the transactions (Brill and Keene, 2014). The lack of reporting channels for individuals with information on digital currency fraud is also a hindrance to law enforcement and forensic professionals (Alton, 2018).

Another issue is that most forensic professionals, including most CFE's, are unfamiliar with the nascent, emergent technology and inexperienced in the virtual tracing of transactions (Courtois et al., 2021). CPA firms have failed to develop the competencies to audit digital assets (Vincent and Wilkins, 2020). Virtual currencies can not be easily classified into any of the cash or cash equivalent categorizations of the FASB and current auditing standards do not address the medium of exchange (Ferris et al., 2024).

Even though federal law enforcement agencies have significantly improved their cryptocurrency fraud investigation competencies, many state and local law enforcement officials do not have the training, knowledge, or resources required to conduct these forensic investigations (Hughes, 2017). Further, most non-federal jurisdictions do not have divisions or experts that specialize in cryptocurrency fraud and national agencies will typically not seriously consider pursuing an investigation unless there are at least several million dollars in estimated losses (Rizzo, 2022).

In addition, given the unique, heightened concerns that individuals have regarding cybersecurity, many organizations may not report these frauds due to concerns that various stakeholders may be more likely to sever business relationships (Knight and Nurse, 2020). Investigators may also experience challenges obtaining access to complete transaction information and recognizing the virtual procedures that occur for each cryptocurrency algorithm (Arsi et al., 2022). There are also few legal or regulatory safeguards regarding the security of cryptocurrency assets (Low and Teo, 2018). For instance, cold wallet holders who lose physical access to their wallet lose access to the underlying assets while hot wallet holders who lose to their seed phrase often lose permanent access to their cryptocurrency accounts (State of Connecticut Department of Banking, 2024).

In addition, since there is no central authority responsible for regulating cryptocurrency, determining the proper jurisdictional authority for prosecutions can be extremely challenging (Naqvi, 2018). Moreover, cryptocurrency schemes function as large international organizations and the laws pertaining to pilfered property and asset seizures vary significantly from region to region. There are collaboration and communication challenges between authorities in different jurisdictions (Dyson et al., 2019). Many officials are unaware of the investigatory actions of functionaries in separate jurisdictions or there is confusion regarding the territorial boundaries of cases.

There is also uncertainty whether evidence involved in cryptocurrency investigations would be considered inadmissible hearsay in a court of law. Blockchain records utilized for business purposes would likely satisfy the consideration requirements if a record custodian or other expert witness could certify the validity of the documentation (Concord Law School, 2019). However, as only four states (Arizona, Vermont, Ohio, Delaware) have codified the courtroom admissibility of hearsay evidence, significant concern still exists regarding the future success of digital fraud investigations and prosecutions. Further, in many nations, cryptocurrencies are nebulously classified and weakly regulated (Gikay, 2018). There are also highly complex Fourth Amendment search and seizure issues that have not yet been consistently addressed by the courts, further jeopardizing the viability of fraud cases (Harper, 2019).

There are also numerous potential obstacles when tracing digital currency transactions in order to detect and investigate potential criminal activity (Wegberg et al., 2018). Many cryptocurrencies incorporate numerous anonymization layers in order to conceal the sender, receiver, and transaction data (Agarwal et al., 2023). Further, the decentralized peer-to-peer blockchain networks permit users to convey crypto-backed assets or cryptocurrency without incorporating Know Your Client (KYC) checks that allow the exchanges to verify and identify an individual's identity. Fraudsters who utilize digital currencies can also employ VPNs (Virtual Private Networks) to conceal their identities, producing fictitious addresses to obscure the source of a transaction (Corbet, 2021). Mixers, non-compliant exchanges, multi-signature services, and numerous wallets are also often used by those who desire to evade detection (Reynolds, 2017). Broadly, fraud may also be perpetuated by a cryptocurrency trading platform, adding complexity to investigations and asset recovery processes.

Another significant impediment when investigating cryptocurrency frauds is that fraudsters can engage mules to launder money through various exchanges (e.g., United States Attorney's Office Eastern District of Texas, 2022). Even though the fraudsters cannot falsify or hide information since blockchain transactions are immutable or permanent, those engaged in criminal activity can easily conceal links between themselves and an assuming, innocent money mule. The speed with which cryptocurrency transactions occur can also be problematic (Bhalla, 2024). The planning phase of an investigation can be hindered since identifying and tracing fraudulent transactions in a timely manner is even more onerous when crimes pertaining to digital currencies are being explored.

Further, despite the nascency of cryptocurrency technology, the losses associated with digital asset-based frauds can be staggering and irreparable. For instance, in 2024, a Kansas bank executive pleaded guilty to embezzling $47.1 million from Heartland Tri-State Bank in order to invest in digital assets, an action which resulted in the bankruptcy of the financial institution and catastrophic losses for investors (United States Attorney's Office District of Kansas, 2024). The bank officer, Shan Hanes, was the target of a pig-butchering scheme, which primarily rely on social engineering tools and initiated a series of wire transfers to a cryptocurrency wallet. The assets were transferred to numerous cryptocurrency accounts administered by anonymous third parties (Grant, 2024). Hanes also misappropriated resources from his church and a local investment club as part of the scheme. Many victims were unable to recoup the monumental losses in their life savings and retirement funds. For example, a fellow colleague of Hanes and a bank shareholder lost seventy percent of his retirement funds due to the embezzlement(Castillo, 2024). Unfortunately, due to the sophisticated blockchain technology, complex transaction trails, and other related factors pertaining to the digital assets, the misappropriated funds were unable to be reclaimed by fraud professionals.

Similarly, Sharon Doughty's mother, a Canadian resident, lost $250,000 within two years due to an investment scheme and recovery scam, where perpetrators provide false claims of asset recovery (Knope, 2023). The misappropriated wealth originated from credit cards, lines of credit, and employment-related funds. The perpetrators were able to use blockchain technology to obtain control over her financial accounts. Even though the victim was eventually able to regain control of her accounts, the misappropriated funds were unable to be recouped due to the anonymity of blockchain technology and cryptocurrency transactions.

Recommendations For Cryptocurrency Fraud Investigations

While there are numerous challenges associated with the investigation of cryptocurrency frauds, investigators can employ several proactive measures in order to mitigate these obstacles. Since many stakeholders have indicated that a large portion of forensic investigators do not have the necessary knowledge or expertise to conduct cryptocurrency investigations, governments and professional organizations should prioritize investments in specialized training and advanced software tools needed to conduct these digital investigations. Trainings should encompass blockchain access, tracing virtual transactions, and understanding of the data presented in transaction statements. Instruction in blockchain analysis tools such as Cipher Trace, Chain Analysis and Elliptic could be especially helpful (descriptions included in Table 2). Local and state

governments should be provided the necessary funds to invest in the resources required for proper cryptocurrency fraud investigations. If the funds cannot be obtained from local and state tax revenues, the federal government could provide grants to state and local governments for such purpose. *[See Table 2, pg. 140]*

Academic institutions should also ensure that those training to be fraud examiners by studying in fields such as accounting or criminal justice receive the proper educational background to investigate criminal activities involving digital currencies. Courses in topics related to auditing, fraud examination, or cybersecurity should include a focus on teaching about virtual currencies and the related fraud investigation methods.

Authoritative professional organizations, such as the AFCE, should also ensure that their members are encouraged to obtain the knowledge needed to complete cryptocurrency fraud investigations. For instance, the CFE exam should include assessments that adequately cover cryptocurrency fraud investigations. Moreover, educators may need to develop professional certifications that specifically address the investigation of frauds pertaining to digital currencies. Further, as many third-party software programs do not provide evidence that would be admissible or helpful in a court case (Butler, 2018), increased collaboration between specialized cryptocurrency investigation software providers and legal authorities would be beneficial in ensuring that software tools (such as Chain Analysis) provide evidence that satisfies courtroom standards.

In addition, legal reclassifications of cryptocurrencies would also be helpful to law enforcement investigations. Since the Federal Commodities Futures Trading Act of the United States defines virtual currencies as commodities (Gikay, 2018), anti-money laundering laws can be evaded through utilization of cryptocurrencies. Digital currencies, however, can still be actively traded to and from more traditional monetary forms. Therefore, in order to aid cyber investigations and reduce online criminal activity, legal authorities should either designate digital assets as currencies rather than commodities or clarify cryptocurrency legal standing. Similarly, several companies are intentionally aiding criminal activity via the dark web by facilitating cryptocurrency use between different parties. Reclassification regulation would require the complicit organizations to be accountable for customer verification, activity report filing, record maintenance, and law enforcement information requests (Brill and Keene, 2014). Enforcement of such provisions would likely deter illicit cryptocurrency frauds, aid prosecution efforts, and promote the recovery of monetary losses.

Increased collaboration and communication between stakeholders and various authoritative organizations would also be helpful during investigations. The regulatory bodies involved should create a central authority for managing cases and sharing resources in order to accelerate the initiation and completion of investigations. The appointment of a primary agency or a regional board for investigating the virtual currency frauds could also reduce difficulties associated with overlapping jurisdictional boundaries and territorial disputes. In order to further assist victims, current laws and regulations should be amended so that law and enforcement agencies have a broader investigatory and prosecutorial reach. Moreover, academic and professional organizations should frequently communicate with fraud investigators in order to ensure that knowledge and skills of current importance to practitioners are being taught in the classroom. Collaboration between various parties would promote economies of scale and lower the overall costs of cryptocurrency investigations, ensuring more available resources for other investigation improvements.

Since third-party software programs may not be providing evidence that would be permissible in a court case (Butler, 2018), increased partnerships between the specialized cryptocurrency investigation software providers, other private organizations, and legal authorities would be helpful in ensuring that the relevant software tools (such as Chain Analysis) provide evidence that satisfies courtroom standards. Similarly, more states should consider codifying the admissibility of blockchain ledger records as courtroom evidence. Further, regulatory reforms ensuring that cryptocurrency exchanges and platforms are subject to more stringent requirements pertaining to KYC and other types of information reporting would be useful. Given the nebulous, relatively uncharted legal issues examined in many cases, legal advisors and experts should also play a larger role in most investigations.

Future Cryptocurrency Fraud Research

Although prior academic literature has begun to examine cryptocurrency fraud (Tworney and Mann 2020; Trozze et al., 2022), there are still many avenues for future research that should be explored. There is a dearth of cryptocurrency data, associated protocols, and methods that criminals utilize to mask their identity when utilizing digital currencies (Alton, 2018). Researchers of cryptocurrencies and cyber-crimes should adjust their emphasis towards identifying suspicious users, analyzing user similarities, and discovering malicious behavior (Tundis et al., 2019).

Employing a qualitative method can provide a rich background of information from impacted stakeholders. Examples of qualitative methods include focus groups composed of fraud professionals and ranked narratives where the descriptions are ranked based upon the likelihood of the event sequence. Phenomenological approaches where the fraud examiner carefully considers the mindset of various stakeholders (victims, potential perpetrators, third parties) to determine how illicit conduct can or did occur can also be assistive. Grounded theory, which aims to describe the origins of events, can also be beneficial in developing fraud prediction models. Quantitative models that incorporate AI and Machine Learning, such as Decision Tree, Random Forest, Ada Boost, and Support Vector Machine (SVM) can be utilized to detect problematic or outlying information that could then be more carefully assessed by human experts. For example, a model created by Decision Tree could be utilized to identify the most likely sequence of events prior to a fraud examiner personally investigating the scenarios identified the software.

Specifically, the literature should examine which types of cryptocurrencies are more susceptible to certain types of frauds, including money laundering, ransomware, embezzlement, proliferation financing, and cybercrime. Many cryptocurrencies lack transparency and more likely to be subject to pump-and-dump schemes and other criminal manipulations (e.g., Robbins, 2022). Similarly, cryptocurrencies can obscure more transaction information (sender, receiver, transaction amount) and increase the difficulty of tracing the transaction flows. Studies focusing on the prevalence of different types of cryptocurrency frauds, such as ransomware, money laundering, and cybercrime, can provide much needed insight into the growing use and potential misuse of cryptocurrency.

The optimal progression of cryptocurrency fraud investigations should also be examined. For instance, given the speed with which cryptocurrency fraud and other cybercrimes occur, the evidence gathering phase of an investigation may need to be accelerated and occur earlier than in other fraud examinations. Therefore, studies considering the success of forensic cases relative to the protocols utilized would also be beneficial. Various cryptocurrency fraud investigation software programs should also be examined in order to assess the strengths and weaknesses of the various tools. Instruments will have varying potential for providing expert witness services, risk assessment, compliance support, transaction analysis, asset recovery, and other blockchain forensics characteristics. Specifically, the research could explore how machine learning methods could be implemented to distinguish between fraudulent and non-fraudulent actors. Given the importance of artificial intelligence, the literature should also compare and contrast the ability of AI technology tools (such as ChatGPT) to predict and detect financial crimes.

Research thoroughly assessing the legal environment and regulatory agencies responsible for regulating cryptocurrency usage should be conducted. Gaps in current regulatory frameworks and suggestions for enhancing the global governance system of cryptocurrency need to be identified. The success of cryptocurrency fraud prosecutions in states that have codified the admissibility of blockchain evidence relative to those that have not should also be explored. The results would be useful in assessing the value of future jurisdictional codification efforts. Research examining variations in the judicial treatment of digital evidence and the impact on case prosecutions across different jurisdictions would also be helpful. Further, the literature should consider how the risk assessment portion of an internal control audit should be adjusted for cryptocurrency related risks.

Studies determining how fraud investigation tools and methods could be further updated in order to ensure that the proper evidence is obtained for court proceedings addressing blockchain technology would also be helpful. Research assessing the curriculum adopted in accounting and criminal science coursework relative to the skills and expertise that cryptocurrency fraud examination requires would also be valuable in identifying deficits and opportunities for improvements in current academic instruction.

Conclusion

While both cryptocurrencies and illicit conduct pertaining to their usage have become ubiquitous (Kerr et al., 2023), fraud examiners and other forensic specialists still encounter numerous obstacles when investigating frauds pertaining to virtual currencies. Indeed, cryptocurrencies function through decentralized and anonymous algorithms that permit anonymity and a rapid increase in the consumer supply (Franks, 2020). Gaps in jurisdictional oversight, a lack of investigator expertise, and informational silos are among the challenges facing those investigating cryptocurrency frauds (Florea and Nitu, 2020; Arsi et al., 2022). However, initiatives such as increased collaboration between stakeholders, amendments to the current regulations, and increased training would be helpful in mitigating these concerns. Research that addresses these investigatory limitations should also be conducted and could benefit from using a qualitative methodology.

Further, the dominant paradigm for investigating employment-based fraud (Wells, 2014), the fraud triangle (Cressey, 1953), may not be the optimal framework for considering crimes pertaining to digital currencies and other cyber-crimes. Moreover, we demonstrate how other fraud investigation models, such as the fraud diamond/pentagon, are superior for examining frauds pertaining to digital assets and cryptocurrencies. A clarion call for greater stakeholder investments in resources for cryptocurrency fraud examinations was also issued. Given the magnitude of cryptocurrency fraud and the associated investigatory challenges (Naqvi, 2018), significant advances in the forensic investigation of digital currencies are imperative.

References

Agarwal, S., Atondo-Siu, G., Ordekian, M., Hutchings, A., Mariconti, E. and Vasek, M. (2023, May). Short paper: DeFi deception—uncovering the prevalence of rugpulls in cryptocurrency projects. In *International Conference on Financial Cryptography and Data Security* (pp. 363–372). Cham: Springer Nature Switzerland.

Alton, L. (2018). 8 opportunities and limitations for AI making cryptocurrency predictions. https://venturebeat.com/2018/01/24/8-opportunities-and-limitations-for-ai-makingcryptocurrency-predictions

Amase, W. (2023) Countries where cryptocurrency is legal vs illegal. CoinGecko. https://www.coingecko.com/research/publications/crypto-legal-countries

Ankier, A. (2019). Debugging IRS Notice 2014–21: Creating a viable cryptocurrency taxation plan. *Brook. L. Rev.*, 85, 883–912.

Anush, B., Inna, G., Tatyana, S., Aleksey, D., and Tetyana, B. (2020). Comparative and informative characteristics of legal regulation of the Blockchain and cryptocurrency: State and prospects. *TEST Engineering& Management*, 20(3), 1541–1550.

Arntsen, C.B. (2020). Who stole my bitcoin?! A Look into the problems associated with state custodial taking of unclaimed cryptocurrencies. *Iowa L. Rev.*, 106, 1923–1959.

Arsi, S., Guesmi, K. and Bouri, E. (2022). Herding behavior and liquidity in the cryptocurrency market. *Asia-Pacific Journal of Operational Research*, 39 (4), 2140021.

Association of Certified Fraud Examiners. (2022). *Occupational Fraud 2022: A Report to the Nations*. https://legacy.acfe.com/report-to-thenations/2022/?ga=2.269223923.380905738.1658940794-1467913131.1623681431

Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A Report to the Nations.* https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Balaban, D. (2017). How law enforcement can investigate bitcoin related crimes and why that's good. https://cointelegraph.com/news/how-law-enforcement-can-investigate-bitcoin-relatedcrimes-and-why-thats-good

Barton. R. E., Mcnamara, C. J., and Ward, M.C. (2022, March 21). Are cryptocurrencies securities? The SEC is answering questions. *Reuters*. https://www.reuters.com/legal/transactional/arecryptocurrencies-securities-sec-is-answering-question-2022-03-21/

Basile, A., Handy, S., and Fret, F. N. (2015). A retrospective look at the Sarbanes-Oxley Act of 2002: Has it accomplished its original purpose? *Journal of Applied Business*.

Bhalla, A. (2024). Top cryptocurrencies with their high transaction speeds [updated]. *Blockchain Council*. https://www.blockchain-council.org/cryptocurrency/top-cryptocurrencies-with-their-high-transaction-speeds/

Boyle, D. M., DeZoort, F. T., and Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, 34(6), 578–596.

Boyle, D. M., Boyle, J. F., and Mahoney, D. P. (2018). Behavioral assessment and modification in fraud mitigation efforts. *Management Accounting Quarterly*, 20, 1–11.

Brill, A. and Keene, L. (2014). Cryptocurrencies: The next generation of terrorist financing? *Defence Against Terrorism Review*, 6(1), 7–30.

Buchholz, A. K. (2012). SAS 99: Deconstructing the fraud triangle and some classroom suggestions. *Journal of Leadership, Accountability and Ethics*, 9(2), 109–118.

Butler, E. (2018). Cryptocurrencies: Threats and investigative opportunities for law enforcement. https://dspace.cuni.cz/bitstream/handle/20.500.11956/101806/120311105.pdf?sequence

Cachanosky, N. (2022). Can cryptocurrencies become a commonly accepted means of exchange? In *The Economics of Blockchain and Cryptocurrency* (pp. 13–28). Edward Elgar Publishing.

Castillo, E. (2024). Former CEO of Kansas bank embezzled $47 million in crypto scheme. He's going to prison. *The Witchita Eagle*. https://finance.yahoo.com/news/former-ceo-kansas-bank-embezzled-233616015.html

Chaffee, E. C. (2018). The heavy burden of thin regulation: Lessons learned from the SEC's regulation of cryptocurrencies. *Mercer L. Rev.*, 70, 615.

Cohen, L., and Godoy, J. (2024). Bankman-Fried sentenced to 25 years for multi-billion dollar FTX fraud. *Reuters*. https://www.reuters.com/technology/sam-bankman-fried-be-sentenced-multi-billion-dollar-ftx-fraud-2024-03-28/

Concord Law School. (2019). The admissibility of blockchain as digital evidence. https://www.concordlawschool.edu/blog/news/admissibility-blockchain-digitalevidence

Corbet, S. (2021). Understanding elevated operational and reputational risks through the corporate usage of cryptocurrency. *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies*, 2, 159.

Courtois, N. T., Gradon, K. T. and Schmeh, K. (2021). Crypto currency regulation and law enforcement perspectives. *arXiv preprint arXiv:2109.01047*.

Cowan, N., Adams, E.J., Bhangal, S., Corcoran, M., Decker, R., Dockter, C.E., Eubank, A.T., Gann, C.L., Greene, N.R., Helle, A.C. and Lee, N. (2019). Foundations of arrogance: A broad survey and framework for research. *Review of General Psychology*, 23(4), 425–443.

Cressey, D. R. (1953). Other people's money; A study of the social psychology of embezzlement.

Crypto Literacy. (2024). Data insights. https://cryptoliteracy.org/insights/

Dorminey, J. W., Fleming, A. S., Kranacher, M. J. and Riley Jr, R. A. (2010). Beyond the fraud triangle. *The CPA Journal*, 80(7), 17.

Dorminey, J., Fleming, A. S., Kranacher, M. J. and Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579.

Dupuis, D., Smith, D., Gleason, K., and Kannan, Y. (2023). Bitcoin and beyond: Crypto asset considerations for auditors/forensic accountants. *Journal of Forensic and Investigative Accounting*, *15*(3).

Dyson, S., Buchanan, W. J. and Bell, L. (2019). The challenges of investigating cryptocurrencies and blockchain related crime. *arXiv preprint arXiv:1907.12221*.

Engle, E. (2015). Is bitcoin rat poison: Cryptocurrency, crime, and counterfeiting (CCC). *J. High Tech. L.*, 16, 340.

Federal Bureau of Investigations. (2023). *Federal Bureau of Investigation Internet Crime Report 2022*. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Ferris, S., McGown, J., Ravenscraft, J., and Smith, S. S. (2024). Fraud and unethical behavior in cryptoassets: Strategies and recommendations for improved forensic accounting. *Journal of Forensic and Investigative Accounting*, *16*(1).

Florea, I. O. and Nitu, M. (2020). Money laundering through cryptocurrencies. *Romanian Economic Journal 22*(76), 66–71.

Franks, P. C. (2020). Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal*, 30(3), 287–299.

Gikay, A. (2018). Regulating decentralized cryptocurrencies under payment services law: Lessons from European Union law. *Journal of Law, Technology & the Internet*, 9(1), 1–35.

Godoy, J. (2024). Terraform Labs, Do Kwon agree to settle SEC civil fraud case. *Reuters*. https://www.reuters.com/legal/terraform-labs-do-kwon-agree-settle-sec-fraud-case-2024-05-30/

Grant, W. (2024). Kansas pig butchering scam proves even financial professionals can be manipulated. PaymentsJournal. https://www.paymentsjournal.com/kansas-pig-butchering-scam-proves-even-financial-professionals-can-be-manipulated/

Hamil, B. (2020). EU cryptocurrency regulation: Creating a haven for businesses or for criminals? *Georgia Journal of International & Comparative Law*, 48(3), 833–849.

Harper, J. (2019). Administering the fourth amendment in the digital age. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-theDigital-Age

Harvey, T. (2014). Cryptocurrencies opening fraud gates. *Fraud Magazine.*

Hetler, A. (2023). Ten common cryptocurrency scams in 2023. *TechTarget*. https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams

Hicks, C., and Adams, M. (2023). Cryptocurrency regulations around the world. Forbes Advisor. https://www.forbes.com/advisor/investing/cryptocurrency/cryptocurrency-regulations-around-the-world/

Hossain, M. Z. (2023). Emerging trends in forensic accounting: Data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention. *Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention (May 16, 2023)*.

Hughes, S. D. (2017). Cryptocurrency regulations and enforcement in the US. *W. St. UL Rev.*, 45, 1.

International Federation of Accountants (IFAC). (2010). International standard on auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements. ISA 240 155–197. https://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa240.pdf

International Monetary Fund. (2019). IMF policy paper fintech: The experience so far. *International Monetary Fund,* (1), 19/255, 3–73.

Jacquelyn (2021, May 12). Who accepts bitcoin and ether cryptocurrencies? Currency exchange international. https://www.ceifx.com/news/who-accepts-bitcoin-and-ether-cryptocurrencies

Joo, M., Kim, S. H., Ghose, A. and Wilbur, K. C. (2023). designing distributed ledger technologies, like blockchain, for advertising markets. *International Journal of Research in Marketing*, 40(1), 12–21.

Kerr, D. S., Loveland, K. A., Smith, K. T. and Smith, L. M. (2023). Cryptocurrency risks, fraud cases, and financial performance. *Risks*, 11(3), 51.

Knight, R. and Nurse, J. R. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99, 102036.

Knope, J. (2023). Got scammed? Why it's 'really, really difficult' for victims of crypto scams to get their money back. *CBC*. https://www.cbc.ca/news/canada/toronto/crypto-scam-victim-money-back-1.7049577

Kuegler, A. J. (2020). Cryptocurrency and the SEC: How a piecemeal approach to regulating new technology selectively stifles innovation. *Conn. L. Rev.*, 52, 989.

Liedel, D. A. (2018). The taxation of bitcoin: How the IRS views cryptocurrencies. *Drake L. Rev.*, *66*, 107.

Low, K. F. and Teo, E. (2018). Legal risks of owning cryptocurrencies. In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1* (pp. 225–247). Academic Press.

Morales, J., Gendron, Y. and Guénin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39(3), 170–194.

Mudroncik, M. (2022, July 29). Virtual Currency [PowerPoint slides]. IRS Communications & Liaison: Stakeholder Liaison.

Muhsin, K., and Nurkhin, A. (2018). What determinants of academic fraud behavior? From fraud triangle to fraud pentagon perspective. *KnE Social Sciences*, 2018, 154–167.

Nakamoto, S. (2009). Bitcoin/src/primatives/block.h. https://github.com/bitcoin/bitcoin/blob/master/src/primitives/block.h

Naqvi, S. (2018). Challenges of cryptocurrencies forensics: A case study of investigating, evidencing and prosecuting organised cyber criminals. Proceedings of the *13th International Conference on Availability, Reliability, and Security*, 1–5. https://doi.org/10.1145/3230833.3233290

Pandya, S. B., Sanghvi, H. A., Patel, R. H. and Pandya, A. S. (2022, May). GPU and FPGA based deployment of blockchain for cryptocurrency–A systematic review. In *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)* (pp. 18–25). IEEE.

Prewett, K., Dorsey, R. W. and Kumar, G. (2019). a primer on taxation of investment in cryptocurrencies. *Journal of Taxation of Investments*, 36(4).

Pistoia, M., Nagaratnam, N., Koved, L., and Nadalin, A. (2004). The theory of cryptography. In *Enterprise Java Security: Building Secure J2EE Applications* (1st ed.). Addison-Wesley Professional. https://www.informit.com/articles/article.aspx?p=170808#

Reid, F. and Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197–223). Springer New York.

Reynolds, P. (2017). Tracking digital footprints: Anonymity within the bitcoin system. *Journal of Money Laundering Control*, 20(2), 172–189.

Rizzo, J. (2022). Are you a victim of crypto crime? Good luck getting help. *Wired*. https://www.wired.com/story/cryptocurrency-cybercrime-law-enforcement/

Robbins, C. (2022). How to spot crypto pump-and-dump schemes. *CoinDesk*. https://www.coindesk.com/learn/how-to-spot-crypto-pump-and-dump-schemes/

Roper, C. (2021). What is cryptocurrency? Financial Forensics. http://quickreadbuzz.com/2021/07/21/forensics-cathy-roper-what-is-cryptocurrency

Schonberger, J. (2022). SEC Chair: Investors need to know 'somebody is not lying to them.' *Yahoo!finance*. https://finance.yahoo.com/news/sec-gensler-securities-crypto-july2022-171955069.html?guccounter=1

Schuchter, A., and Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, 39, 176–187.

Soni, S. (2021). Crypto market cap doubles to eye-popping $2.3 trillion in 3 months as mainstream adoption gets nearer. *Financial Express*. https://www.financialexpress.com/market/crypto-market-cap-doubles-to-eye-popping-2-3-trillion-in-3-months-as-mainstream-adoption-gets-nearer/2245246/

State of Connecticut Department of Banking. (2024). Digital wallets. https://portal.ct.gov/dob/consumer/consumer-education/cryptocurrency-digital-wallets

Stroukal, D. and Nedvdova, B. (2016). Bitcoin and other cryptocurrency as an instrument of crime in cyberspace. *4th Business and Management Conference: International Institute of Social and Economic Sciences*, Istanbul.

The Sage Group, PLC. (2022). The Redefined CFO. The Sage Group, PLC. https://online.sageintacct.com/20220801EMAILTheRedefinedCFOeBookGBINTACCT.Email1_Thank_You_rebrand.html?aliId=eyJpIjoia3BaVjZFTzRcL1dkTE9pTVAiLCJ0IjoiSndMUXM5aE1rNytGVFp6T1IweUhOQT09In0%253D

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T. and Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11, 1–35.

Tundis, A. and Mühlhäuser, M. (2019). The role of information and communication technology (ICT) in modern criminal organizations. In *Organized Crime and Terrorist Networks* (pp. 60–77). Routledge.

Twomey, D. and Mann, A. (2020). Fraud and manipulation within cryptocurrency markets. *Corruption and fraud in financial markets: malpractice, misconduct and manipulation*, *624*.

United States Attorney's Office Eastern District of Texas. (2022). Eastern District of Texas Announces Multi-Year Investigation in Transnational Cryptocurrency Money Laundering Networks. Press Release. https://www.justice.gov/usao-edtx/pr/eastern-district-texas-announces-multi-year-investigation-transnational-cryptocurrency

United States Attorney's Office District of Kansas. (2024). Fmr. executive pleads guilty after losing bank's $47.1 million in crypto scheme. Press Release. https://www.justice.gov/usao-ks/pr/fmr-executive-pleads-guilty-after-losing-banks-471-million-crypto-scheme

United States Department of Justice. (2020). Report of the attorney general's cyber digital task force: Cryptocurrency enforcement framework. United States Department of Justice.

United States Department of Justice. (2023). Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes. Press Release 23–362. Office of Public Affairs.

United States Federal Register. (2022). Executive Order 14067. Ensuring responsible development of digital assets. https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets

Venkatesh, C. R. (2018). Four things that made blockchain the most disruptive tech in decades. Inc42. https://inc42.com/resources/4-things-that-made-blockchain-the-mostdisruptive-tech-in-decades

Vincent, N. E., and Wilkins, A. M. (2020). Challenges when auditing cryptocurrencies. *Current Issues in Auditing*, 14(1), A46.

Wegberg, R., Oerlemans, J. J. and van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435.

Wells, J. T. (2014). *Principles of fraud examination*. John Wiley & Sons.

Wolfe, D. T. and Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud.

Table 1: Fraud Investigation Models

Fraud Investigation Model	Components
The Fraud Triangle	Rationalization, Opportunity, Pressure
The Fraud Diamond	Rationalization, Opportunity, Pressure, Competence
The Fraud Pentagon	Rationalization, Opportunity, Pressure, Competence, Arrogance
The A-B-C Formula	Bad Apple (Individual), Bad Bushel (Circumstances), Bad Crop (Ethical Culture)

Table 2: Cryptocurrency Investigation Tools and Services

Cryptocurrency Investigation Tools/Services	Description
Chainalysis	• Mapping transaction patterns • Visualizing fund transmissions between crypto wallets • Connecting individual identities to crypto wallets through address clustering and data analysis • Communicating crime typologies and suspicious activity alerts
CipherTrace	• Analyzing blockchain transactions to identify criminal activity • Tracking cybercrimes and ransomware associated with cryptocurrency products • Delivering forensics training and investigator certification • Uncovering complex money trails
Elliptic	• Flagging transactions associated with criminal services • Providing in-depth forensics reports for legal proceedings • Investigating transaction histories
Nansen	• Identifying online schemes like spoofing, ramping, and wash trading • Screening transactions for money laundering risks • Tracking wallets and behavior to identify fraud risks • Monitoring transactions across various blockchains
TRM Labs	• Monitoring wallet activities and blockchain transactions in real-time • Delivering automated visualizing and reporting for investigation purposes • Supplying software API integrations for broader monitoring coverage