2025

Modus operandi and blockchain analysis of romance scams: cryptocurrency-driven victimization

BOSTON UNIVERSITY

METROPOLITAN COLLEGE

Thesis

MODUS OPERANDI AND BLOCKCHAIN ANALYSIS OF ROMANCE SCAMS: CRYPTOCURRENCY-DRIVEN VICTIMIZATION

by

AMY HYUNJEONG LIM

B.A., University of Washington, 2015
M.S., Arizona State University, 2022

Submitted in partial fulfillment of the

requirements for the degree of

Master of Science

2025

Approved by

First Reader _____

Kyung-Shick Choi, Ph.D.
Professor of the Practice of Criminal Justice
Director, Center for Cybercrime Investigation and Cybersecurity

Second Reader _____

Shea W. Cronin, Ph.D.
Assistant Professor of Criminal Justice
Chair of Applied Social Sciences

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my thesis committee members. My thesis committee chair, Dr. Kyung-Shick Choi provided thoughtful and consistent mentorship throughout the research process. He helped me stay focused on the fundamental purpose of this study, to contribute to law enforcement investigations, and guided me in developing a professional mindset essential for both academic and practical success. My committee member, Dr. Shea W. Cronin, provided dedicated instruction in the fields of crime analysis and data visualization. His insightful career advice was instrumental in shaping my academic path. I sincerely thank both members of my thesis committee for their invaluable guidance and mentorship throughout my academic journey.

Finally, I would like to extend my heartfelt thanks to my family in South Korea and my beloved husband, Sangho for their unconditional love, encouragement, and support. Their constant presence has been a source of strength, uplifting me mentally, emotionally, and physically throughout this journey. Without their support, none of this would have been possible.

MODUS OPERANDI AND BLOCKCHAIN ANALYSIS OF ROMANCE SCAMS: CRYPTOCURRENCY-DRIVEN VICTIMIZATION

AMY HYUNJEONG LIM

ABSTRACT

Crime happens in relationships, including romantic ones. A significant portion of intimate crimes are financially motivated, frequently leveraging emotional manipulation as a core tactic. In the digital realm, romance scammers often initiate contact with individuals through dating applications, gradually build trust, and ultimately exploit emotional bonds to extort money under various pretenses. Increasingly, the proceeds of these scams are laundered through cryptocurrency, further complicating efforts to trace and disrupt illicit financial flows.

This study examines three key components of cryptocurrency-driven romance scams: (1) the modus operandi employed by scammers, (2) the financial deception strategies used to defraud victims, and (3) the patterns of cryptocurrency laundering techniques. Using self-reported data from Chainabuse.com from May 2022 to October 2024, 107 verified cases were analyzed through descriptive statistics, ordinary least squares (OLS) regression, and blockchain forensic mapping analysis. Findings reveal that Bitcoin and Ethereum are the most frequently used cryptocurrencies in romance scams and are significantly associated with monetary losses. In terms of modus operandi, Tinder emerged as the most common platform for initiating contact, with WhatsApp used for continued communication. Regarding financial deception, 54.2% of cases involved fraudulent investment schemes, while 43.0% featured fabricated emergency scenarios.

With respect to cryptocurrency laundering techniques, scammers frequently used mixers (78.5%), self-funding (45.8%), and swapping (43.0%) to obscure transaction trails. Notably, the use of mixers was positively associated with monetary losses at the individual level monetary losses, while the number of swaps was negatively correlated with losses at cluster level. Interestingly, the use of swap tools such as MetaMask was linked to greater financial losses in cluster level analysis. Preferred exchanges used for laundering were also identified, with platforms such as OKXs being associated with financial losses negatively. Furthermore, direct deposits to scammer wallets were negatively correlated with monetary losses at both individual and cluster levels.

This study contributes to the understanding of romance scams involving cryptocurrency by analyzing scammers' tactics, preferred cryptocurrencies, platforms, laundering techniques, and exchanges, as well as their relationship with monetary losses. It highlights the complexity of tracing illicit digital transactions and emphasizes the need for advanced investigative tools, risk-based investigative prioritization, and broader public awareness campaigns to strengthen prevention efforts, law enforcement responses, and victim protection.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

INTRODUCTION

In today's digital age, forming friendships and starting relationships through dating apps has become increasingly common. However, alongside these connections, crimes in the online environment are also on the rise, leading to a growing number of victims and an escalation in the severity of harm. Crimes, particularly those involving romantic relationships, are increasingly utilizing cryptocurrency as a method for receiving funds. The unregulated and anonymous nature of cryptocurrencies has contributed to a steady rise in these offenses. In 2023, 65,715 cases of romance scams were reported, and $1,179 million was lost to romance scams (Tableau Public, 2024; Fair, 2024). In addition, there has been a notable surge in romance scams in recent times, with data indicating a more than 75-fold increase in romance scam activity in 2023 compared to 2020 (Chainalysis, 2024). Additionally, romance scams were the fifth most common complaint out of 26 types of crimes involving cryptocurrency of complaints received in 2023 (FBI, 2023a), and were in the top third for complainants over the age of 60 according to the IC3 report (FBI, 2023b).

Romance scams is a contemporary form of fraud that has evolved alongside the Internet. The scammers employ romantic tactics to gain a person's trust, deceives victims into believing they are in relationships and ultimately exploit the victims financially (DOJ, 2024b). In the initial stage of their deception, scammers create an appealing fake profile to attract the victim (Whitty, 2015). Subsequently, they engage in grooming behaviors to build trust with the victim during the second stage (Whitty, 2015). In the third stage, scammers initiate requests for financial assistance (Whitty, 2015). Once

scammers accomplish their monetary gain in their last stage, they suddenly cut off all contact and communication with victims and disappear with no trace left behind (Whitty, 2015). Victims often struggle to recognize or report suspicious activity, as scammers typically do not overtly solicit funds. Instead, they employ subtle and covert tactics to foster an emotional connection with their targets, often presenting scenarios that evoke a sense of obligation to assist (Whitty, 2013). In the case of United States v. Marfo (2022), the perpetrator presented a range of scenarios to multiple victims to solicit financial contributions and consequently received at least $4.7 million (DOJ, 2022).

As the victimization becomes evident, victims often struggle to accept or cope with the reality of their situation (Buchanan & Whitty, 2014) and erosion of trust in romantic relationships contributes to significant psychological and emotional harm. Whitty and Buchanan (2016) identified that victims of romance scams experience a range of distressing emotions, including embarrassment, anger, stress, fear, and a sense of mental violation. In addition, victims often suffer significant psychological harm when they realize they have been involved in a crime, such as unknowingly participating in money laundering or aiding a scammer obtain a visa (Whitty, & Buchanan, 2016). In severe forms of cases, scammers have lured victims to travel to African or Asian countries, which are known to be a source of many scams and kidnapped them upon arrival for purpose of human trafficking or labor exploitation to commit new crimes (Buchanan & Whitty, 2014; United Nations, 2023). In extreme cases, victims are often coerced into committing criminal acts under the duress and direction of the scammers (Maras & Arsovska, 2023). Research indicates that victims exposed to these severe

crimes frequently experience symptoms of posttraumatic stress disorder (PTSD) (Whitty & Buchanan, 2016). Moreover, the psychological impact of these experiences has led some victims to develop suicidal thoughts (Whitty & Buchanan, 2016; Chuang, 2021).

In addition to the emotional and psychological damage inflicted on victims, a concerning aspect is that scammers often launder the proceeds from romance scams through cryptocurrency. Since the goal of scammers is to shield themselves from criminal prosecution, they employ mixer or tumbler techniques (Neumann & Sartor, 2016; Wronka, 2022) and tools like UniSwap or Sushiswap to enhance the anonymity of cryptocurrency transactions (Homeland Security, 2023). The case of United States v. Lam and Serrano (2024) exemplifies cryptocurrency money laundering, in which the perpetrators stole over 4,100 Bitcoins (worth more than $230 million) after engaging with the victim online and subsequently laundered the money using various techniques. In addition, Bellei et al. (2024) have identified a pattern in which cryptocurrency scammers do not transfer their entire balance to the destination address; instead, they "peel" off small amounts and send them to other addresses under their control, making even more challenging for law enforcement to trace illicit transactions.

The purpose of this study is to analyze trends in romance scams through the examination of cryptocurrency address reported in open-source data. Rather than focusing on victim demographic data, this study will examine modus operandi of romance scams by determining the contact method scammers initially utilized and examining what strategy the scammers developed the romantic relationship with victims to deceive trust and financially extorted. Furthermore, this study examines the

cryptocurrency addresses in reported cases of romance scams to identify the illicit money laundering techniques employed by scammers. Finally, the study recommends effective countermeasures to reduce victimization in romance scams and explore strategies to support law enforcement in identifying the patterns of illicit transactions, thereby enhancing investigative approaches to romance scam cases.

LITERATURE REVIEW

Modus Operandi of Romance Scams

Romance scammers capitalize on the fact that they can commit crimes through online communication without meeting in person. They utilize a variety of online dating platforms or major social media platforms to interconnected with victims such as Tinder, Bumble, Hinge, Badoo, Happn, Grindr, Tantan, and Plenty of Fish (Curry, 2024). According to a survey conducted by the Pew Research Center, 46% of Americans adults reported that they have ever used a dating app, Tinder (McClain & Gelles-Watnick, 2023). Among users aged 18–29, 79% reported that Tinder is their primary dating app and 44% of aged 30–49 indicated they have used Tinder the most (McClain & Gelles-Watnick, 2023). Additionally, among users with LGBTQ, Tinder is the most commonly used platform for finding partners in the U.S., as it allows to add sexual orientation (McClain & Gelles-Watnick, 2023; Baluch & DiGiacinto, 2024).

In addition, the second mostly used dating app in users aged 18 to 29 is Bumble (McClain & Gelles-Watnick, 2023). Unlike other dating apps, Bumble creates a female friendly environment by integrating features that give female complete control over their experience (Baluch & DiGiacinto, 2024). Allowing female to initiate contact with potential matches attracts more female users by reducing the number of inappropriate messages from men (Murphy, 2018). As the number of female users increases, the Bumble naturally attracts a corresponding increase in male users. Accordingly, Tinder is the most downloaded dating apps across the U.S. and followed by Bumble (Curry, 2024; Marrazzo, 2024). In addition to Tinder and Bumble, Asia-founded dating apps such as

Momo and TanTan are among the most popular in China (Low et al., 2022; Thomala, 2024; Wu & Trottier, 2022), while Badoo ranks highly in Europe (Marrazzo, 2024).

Romance scammers prefer to initiate communication through dating apps as it offers benefits the same way legitimate users are offered. Since the primary aim of dating apps is to maximize users' chances of meeting others (Shapiro, 2023), the opportunity for romance scammers to connect with potential victims through these platforms is also substantial. Additionally, the widespread use of dating apps reduces the likelihood of scammers facing rejection from potential matches (Shapiro, 2023; Colussia et al., 2020), allowing scammers to interact with others more freely. Most importantly, dating apps allow scammers to remain pseudonymous. Since dating apps do not accurately verify whether an individual's actual appearance matches their profiles (Shapiro, 2023), scammers can use faked photo by selecting publicly available images and altering the facial features in those photos (Suarez-Tangil et al., 2020).

Once scammers successfully establish a connection with a target, they often request to move the conversation to other forms of communication (Whitty, 2013). Scammers primarily use instant messaging, such as WhatsApp, WeChat, Facebook, Telegram, and Instagram, to create swift and authentic connections and draw their victims closer (Global Coalition to Fight Financial Crime, 2024, Shapiro, 2023, Federal Trade Commission, 2023). Having conversations outside the dating service allows scammers to exert greater control over their victims without incurring costs and poses significant challenges for tracking (Craig, 2024). Furthermore, direct messaging applications are often exploited by criminals, leveraging the fact that end-to-end encryption ensures that

only the sender and recipient can access the data, preventing any third-party access (Bogos et al., 2023). In addition, criminals often converge on direct messaging platforms, such as Telegram, where a wide array of illicit data is exchanged. This includes fake identification, stolen banking credentials, and, notably, pre-KYC (Know Your Customer) verified cryptocurrency exchange accounts (Bolster, 2024). Data breaches that were initially leaked or sold ultimately find their way to Telegram, where they are either sold or distributed freely by scammers (Bolster, 2024). After transitioning to an instant communication tool, scammers invest considerable time in building trust with their victims, ultimately persuading them to send money. The amount of time it takes for a victim to send money to a scammer varies for each victim, but scammers typically invest 6 to 8 months in fostering an emotional attachment with their targets (Coluccia et al., 2020; Whitty, 2015). Personal information, such as phone numbers, is often shared in less than a week (Fansher & McCarns, 2019).

Scammers leveraging artificial intelligence (AI) have significantly enhanced their tactics. Through the use of deepfake technology, scammers can manipulate images, videos, and audio to create individuals they make realistic (Fletcher et al., 2024; Cross, 2022). Some scammers specifically target individuals who lost loved ones, searching obituaries to create fake profiles that resemble the deceased and utilize AI to generate appealing images and voices to attract potential victims (Craig, 2024). In addition, scammers exploit their victims by employing scenarios that evoke sympathy, such as medical bills, a sick child, multiple essential expenses, or debt to the government (Whitty, 2013; DOJ, 2024a).

Furthermore, scammers utilize automated bots to swiftly engage potential victims, encouraging victims to share personal contact and to click on links of photos or videos sent by the scammer unwittingly, making victim fall into phishing as well (Murphy, 2018; Fletcher et al., 2024). Additionally, scammers begin providing victims with cryptocurrency investment advice, guiding them on where to put their funds (Agarwal et al., 2023). They create fake websites and cryptocurrency wallets to show victims that invested funds are being effectively managed and generating substantial gains (Department of Treasury, 2024). By consistently flattering their victims and fostering a positive emotional environment, scammers build trust until the large amount of funds are invested (Agarwal et al., 2023). When victims invest significant amounts in cryptocurrency, scammers disappear with their money, leaving them exploited and defrauded.

Scammers are cognizant of AI development and the level where distinguishing between authentic and fabricated photos, videos, and audio has become difficult (Cross, 2022). By maintaining consistent communication both morning and night, scammers integrate into their victims' daily routines and foster a strong emotional attachment to the fraudulent profiles (Whitty, 2013). This level of engagement makes it increasingly difficult for victims to detect any suspicious behavior. Once full intimacy is established and the victim has sent money as instructed, scammers abruptly terminate the relationship by deleting all fictitious profiles, rendering the victim unable to make further contact.

Methods of Money Transfer in Romance Scams

The primary motive for scammers to establish rapport and cultivate close relationships with victims is to extort money. In doing so, scammers request funds from victims through various methods of money transfer (Cross, 2023). Commonly, scammers solicit victims to wire a series of payments through third-party wire transfer services such as Western Union (Sorell & Whitty, 2019). Using Western Union, senders (i.e., victims) can select how the recipient receives the funds—such as cash, mobile transfer, or direct deposit—and choose the payment method, including credit card, debit card, or bank account (Western Union, 2019). Given that senders have control over these options, they may not realize that they are being scammed.

Furthermore, scammers frequently suggest victims use gift cards, such as iTunes cards, as a payment method (Cross, 2023). According to the Federal Trade Commission (2023), gift cards were the most frequently reported payment method in 2022, with a median individual loss of $700, ranked third overall (cryptocurrency transactions ranked first, with a median loss of $10,079, and bank transfers ranked second, $10,000). Once the transfer is completed and the funds are sent to the recipients (i.e., scammers) within minutes, victims often realize they have been scammed only after receiving no response from their partner (Cross, 2023). Furthermore, scammers often use Cash App for money transfers as it is free on Bitcoin transactions, and the payments cannot be canceled or reversed once completed (Staples, 2024).

Pandemic has also impacted the method of money transfer in romance scams. As cyber-enabled romance scams surged following the pandemic (Chainalysis, 2024)–driven

by increased online activity and loneliness due to lockdown (Buil-Gil & Zeng, 2022), and heightened communication via phone, text, email, and social media (Global Coalition to Fight Financial Crime, 2024)–scammers' use of cryptocurrency for money transfers in romance scams has also increased. In this case, scammers frequently employed pretenses, the most common scenarios involving requests for donations to charities (49%) and funds for COVID-19 treatment or equipment (41.5%) (Teaster et al., 2023). In terms of payment methods used in 2022, cryptocurrency was the most common payment method used in romance scams, accounting for 34% of reported cases, followed by bank wire transfers (27%), gift cards (7%), payment app or service (3%) and others (28%) (Federal Trade Commission, 2023).

Understanding of Cryptocurrency in Romance Scams

Cryptocurrencies are digital currencies that exist only on the internet. Generally, users can buy or sell cryptocurrencies using their cell phones, computers, or cryptocurrency ATMs (Federal Trade Commission, 2022) and can be exchanged and tracked on public ledgers known as blockchains (Congressional Research Service, 2023). When a cryptocurrency transaction occurs, it generates a unique, immutable combination of letters and numbers and is being recorded on the blockchain, remaining publicly visible and traceable (Wronka, 2022). Detailed information such as the total number of transactions, amount sent or received, transaction date, sender, and recipient are stored in each cryptocurrency addresses (Wronka, 2022) and can be looked up on Internet.

Although cryptocurrency transactions are publicly viewable and recorded, the anonymity they provide is a significant reason why scammers favor them as payment

methods. In transactions, users send and receive cryptocurrency through private wallets, which store keys that secure ownership of transactions (Congressional Research Service, 2023). This enables cryptocurrency payments to occur without any personal information verification linked to the transaction. The use of cryptography further enhances security and protects user anonymity (Ingolf & Brett, 2021). To encrypt data, cryptography utilizes a public key; however, a private key is needed to decrypt the data and revert it to its original form (Congressional Research Service, 2023). Consequently, criminals employ various techniques to obscure transactions and make tracking these anonymous payments significantly more difficult (Vejačka, 2014), which is why criminals often prefer using cryptocurrencies as a payment method.

A key factor facilitating the use of cryptocurrency by scammers is the widespread adoption of financial technologies (FinTech). It provides easy access to bank accounts and payment cards with minimal Know Your Customer (KYC) requirements (Homeland Security, 2022). This ease of access enhances the convenience of cryptocurrency transactions as it also enables individuals to open multiple bank accounts without the proof of residence or income (Homeland Security, 2022). Consequently, this access simplifies the movement of funds, providing a mechanism for money laundering. In jurisdictions with weak or absent KYC regulations, this greater accessibility to financial services provides scammers with more opportunities to obtain and launder illegal funds, including cryptocurrency transactions (Homeland Security, 2022).

Deception in Cryptocurrency Transaction in Romance Scams

Cryptocurrency transactions in romance scams typically involve small amounts of funds, as it is relatively easier to be sent and moved across the world (Kramer et al., 2023). Due to the large transactions can be flagged as "unusual" under anti-money laundering regulations–rendering them subject to investigation by banks and Financial Intelligence Unit (FIU) (Kramer et al., 2023)–scammers employ specific methods, crypto mixer/tumbler techniques to prevent from cryptocurrency transaction being a publicly traceable on blockchain and to evade detection (Wronka, 2022). Using a crypto mixer/tumbler services means scammers pay for the service to create new wallet addresses. For instance, when users send a certain amount of cryptocurrencies to mixer, it collects, pools and pseudo-randomly shuffles the assets (Chainalysis, 2022a). After some time, users can withdraw their cryptocurrencies to newly created wallet addresses with small amount of service fee deducted (Chainalysis, 2022a). In simple terms, the use of these techniques complicates the traceability of cryptocurrency transactions by obscuring the connection between legitimate (origin addresses) and illegitimate addresses (newly created addresses) (Dupuis & Gleason, 2021).

In addition to crypto mixers/tumblers, scammers also utilize Tornado Cash, which operates similarly to crypto mixers but is more user-controlled and decentralized (Chainalysis, 2022b). "Tornado Cash is a smart contract-based crypto asset mixer that uses zkSNARKs to create a decentralized privacy enhancing protocol" (Nadler and Schär, 2023). Tornado Cash generates a secret hash every time a user deposits funds and uses Merkle tree to store those hashes (Nadler and Schär, 2023). Additionally,

cryptographic between deposits and withdraws are disconnected in Tornado Cash, and users withdraw from the smart contract funding pool, making difficult to track the origin source (Nadler and Schär, 2023). When users withdraw the funds, the zero-knowledge cryptography (i.e., zkSNARKs) generates a proof of ownership of deposited funds without having to reveal the details of users (Chainalysis, 2022b; Nadler and Schär, 2023). Thus, by using Tornado Cash, scammers can conceal both their transaction history and the origin of their funds and ownership, rendering them untraceable.

Additionally, scammers employ the peel chain technique to route cryptocurrency across multiple destinations. Scammers break down large transactions into complex smaller patterns, converting funds across various cryptocurrencies (Homeland Security, 2023; Bellei et al., 2024). To simply put it, scammers transfer a specified amount to a designated wallet address while redirecting the remaining balance to an alternative address under their control, thereby obfuscating the transaction trail and complicating the ability to trace the flow of funds (Bellei et al., 2024; Turner et al., 2020). In other words, by repeatedly sending money to new addresses, scammers split the transaction history, further making more difficult to trace the source of funds. In the case of United States v. Ilya “Dutch” Lichtenstein and Heather Morgan (2022), the perpetrators employed the peel chain technique to do money laundering, where a large amount of cryptocurrencies held at single address is sent through a series of transaction in smaller amounts to a new address.

Furthermore, scammers often employ a technique known as cryptocurrency swapping, whereby one type of cryptocurrency is exchanged for another, such as

converting Bitcoin into Ethereum (Paredes, 2024). A common method of swapping is through decentralized exchanges (DEXs), which allow users to trade directly without intermediaries or custodians of funds (Paredes, 2024). By utilizing these techniques, scammers can effectively disrupt the audit trail, making it more challenging for investigators to trace the source and movement of illicit funds.

Ongoing Problems with Using Cryptocurrency in Romance Scams

Cryptocurrency accounts lack government backing. If the company storing cryptocurrency goes bankrupt or suffers a cyberattack, the government will not step in and secure it, a lack of government protection in cryptocurrency (Federal Trade Commission, 2022). In addition, cryptocurrencies operate in a largely unregulated environment, functioning without central intermediaries, such as banks (Congressional Research Service, 2023). This decentralized nature allows cryptocurrency users to swiftly and securely send and receive any amount of money at any time and from any location worldwide (Vejačka, 2014). Due to their ability to facilitate large transactions that can be quickly distributed across multiple destinations, scammers often rely on cryptocurrencies for money transfers. However, comprehensive regulatory frameworks are lacking globally, for example, the U.S. Treasury has no jurisdiction over exchanges that are not registered within the United States (Homeland Security, 2022).

Furthermore, there is also an absence of regulatory oversight for the technologies used in cryptocurrency transactions. Consequently, individuals with the technical skills can engage in cryptocurrency trading without formal restrictions. For example, on August 8, 2022, Tornado Cash was sanctioned by Office of Foreign Assets Control (OFAC)

(Chainalysis, 2022b; 2024). However, due to the decentralized nature of its operation, meaning the transfer of control and decision-making shift from a centralized entity (individual, organization or group) to the network (lack of government), it could not be effectively shut down, resulting in a gradual increase in inflows (Chainalysis, 2024). Using these money laundering techniques, such as depositing an asset and withdrawing it in multiple addresses, severed the connection between deposit and withdrawal addresses, scammers thereby enhancing confidentiality (Immunebytes, 2023). Furthermore, crypto mixers are legal in most jurisdiction in United States with a license registered (Chainalysis, 2022a; Wronka, 2022). However, some intelligent scammers exploit these tactics to launder cryptocurrency obtained through romance scams. The structure of these transactions is akin to that of a tornado, with a single point of entry that expands significantly as the operation progresses. Therefore, to illustrate the typical structure of romance scams that involve the use of cryptocurrency, the actual reported cryptocurrency addresses in romance scams will be analyzed in this paper.

METHODOLOGY

Data Collection

Between May 23, 2022, and October 31, 2024, a total of 783 reports from chainabuse.com were initially collected to identify trends in online romance scams, focusing on cryptocurrency involvement. These reports, self-reported by individuals, included detailed accounts of their experiences along with associated cryptocurrency wallet addresses. Reports were excluded if they lacked detailed scam information, were in non-English languages, or did not include cryptocurrency wallet addresses. Cases involving ‘sugar daddy’ or ‘sugar mommy’ where older and wealthier individuals exchange money for companionship with younger individuals, often involving sexual relationship, were also excluded due to the lack of cryptocurrency wallet addresses involved.

To ensure data accuracy, several open-source intelligence (OSINT) tools were employed for verification. These included bitcoinwhoswho.com for fraudulent address identification, sanctionssearch.ofac.treas.gov for sanctions checks, okx.com for cryptocurrency address validity, and blockchain.com and blockchair.com for transaction details. After cross-referencing data, 165 cases of online romance scams were identified. An additional screening was conducted to exclude cases with unverified or inconsistent financial details, such as discrepancies between reported losses and transaction histories. For example, cases where the victim's reported loss was $11,395, but the total amount received in the transaction history of cryptocurrency was $6,605.05, were excluded due to insufficient data credibility. Therefore, total 107 data were collected and analyzed.

General Characteristics

Types of Cryptocurrencies

Table 1 shows overall sample characteristics and their measurements in the current study. The Skewness and Kurtosis of number of reported cryptocurrencies was found to be 3.49 and 14.688 for Bitcoin, 2.08 and 5. 32 for Ethereum, and 3.14 and 10.30 for Tron (Acceptable skewness standard is ± 3 and Kurtosis is ± 7 (Kline, 2011)). Consequently, these data were recoded into new variables, where values of 0 remained 0, values of 1 remained 1, system-missing values were retained as system-missing, and values in the range of 2 through 12 were recoded to 2. This recoding was necessary because some victims reported multiple cryptocurrency addresses within a single case. Among the cryptocurrencies, Bitcoin was the most reported cryptocurrency, representing 61.7% (*n*=66) of the total sample, followed by Ethereum at 34.6% (*n*=37), and Tron at 15.0% (*n*=16).

Modus Operandi in Romance Scams

The types of dating app platforms used by scammers to initiate contact in romance scams were measured. Tinder was the most frequently used dating app 8.4% (*n*=9) of the cases, followed by Hinge 7.5% (*n*=8). Other dating apps were also used, including Bumble, Plenty of Fish, Boo, and Happen, each representing 1.9% (*n*=2) of the cases. Coffee Meets Bagel and Match were less commonly used, each representing 0.9% (*n*=1). In addition, 4.7% (*n*=5) of the cases involved other, unspecified dating apps, 42.1% (*n*=45) of the cases had unknown information, and 28% (*n*=30) of the scammers used social media platforms to contact victims.

The types of messaging applications used by scammers to maintain communication with victims were also assessed. The transition to messaging platforms was coded as follows: if the scammer transitioned to a direct messenger, it was marked as "Yes=1," and if the scammer did not use a messaging app or no information was provided, it was marked as "No=0." About 26.2% (*n*=28) victims were directed to messaging platforms for further communication. Among these platforms, WhatsApp was the most frequently used, representing, 57.1% (*n*=16) of the cases. Other messaging apps included Line and Instagram, each representing 7.1% (n=2) of the cases. Telegram was used in 17.9% (n=5) of the cases, while other platforms such as Google Chat or Skype were utilized in 10.7% (n=3) of the cases. Scammers established relationships with victims through online platforms and subsequent messenger applications for further communication.

Table 1. Descriptive Statistics (N=107)

Variables	Measures	Mean	S.D.	*N* (%)
Types of Cryptocurrencies				
Number of Bitcoin		0.79	0.71	66 (61.7 %)
Number of Ethereum		0.42	0.63	37 (34.6%)
Number of Tron		0.20	0.50	16 (15.0%)
Modus Operandi in Romance Scams				
Types of Dating App				
Tinder				9 (8.4%)
Hinge				8 (7.5%)
Bumble				2 (1.9%)
Plenty of Fish				2 (1.9%)
Coffee Meets Bagel				1 (0.9%)
Boo				2 (1.9%)

Match				1 (0.9%)
Happen				2 (1.9%)
Other Dating App				5 (4.7%)
Unknown				45 (42.1%)
Social media				30 (28.0%)
Transition to Messengers				
Yes				28 (26.2%)
Types of Messengers				
WhatsApp				16 (57.1%)
Line				2 (7.1%)
Instagram				2 (7.1%)
Telegram				5 (17.9%)
Others [Google Chat or Skype]				3 (10.7%)
Financial Deception Strategies				
Types of Deception				
Investment				58 (54.2%)
Emergency				46 (43.0%)
Unknown				3 (2.8%)
Direct Deposit				
Yes				50 (46.7%)
Method of Money Deposit				
Fake Investment Website				58 (54.2%)
Direct Deposit Crypto Wallet				43 (40.2%)
Direct Deposit Cash App				10 (9.3%)
Individual level Monetary Loss (DV1)	Ordinal (1– 4)	2.48	1.12	
Range 1 thru 1525 = 1				24 (25.3%)
Range 1526 thru 7400 = 2				24 (25.3%)
Range 7401 thru 41167 = 3				24 (25.3%)
Above 41167 = 4				23 (24.2%)
Cluster level Monetary Loss (DV2)	Ordinal (1– 4)	2.52	1.18	
Range 1 thru 9683 = 1				25 (24.3%)
Range 9684 thru 77839 = 2				26 (25.2%)
Range 77840 thru 270984 = 3				25 (24.3%)
Above 270984= 4				27 (26.2%)
Identification of ML Activities				
BitcoinWhosWho.com Scam Alert				
No				89 (83.2%)
Yes				18 (16.8%)

Breadcrumbs Flags/Risks Alert			
CDA (hack, scam)	0.21	0.41	23 (21.5%)
ATII (human trafficking)	0.08	0.28	9 (8.4%)
Use of ML Techniques			
Swap	0.43	0.50	46 (43.0%)
Mixer or Tornado Cash	0.79	0.41	84 (78.5%)
Peel Chain	0.08	0.28	9 (8.4%)
Self-Fund	0.46	0.50	49 (45.8%)
Type of Swaps			
Tokenlon			16 (15.0%)
MetaMask			13 (12.1%)
UniSwap			12 (11.2%)
Outgoing Exchanges			
Kucoin	0.14	0.35	14 (14.4%)
OKX	0.27	0.45	26 (26.8%)

Financial Deception Strategies

The types of deception were assessed and coded as follows: if a reported cases involved a fake domain address, it was coded as “Investment=1,” if a reported case involved an emergency scenario, it was coded as “Emergency=2,” and “Unknown=3.” The most common deception type utilized by scammer was investment, representing 54.2% (*n*=58) of the cases. This Investment deception typically involved fake promises of high returns on investments via fraudulent websites or link. The second most frequent type was emergency with 43.0% (*n*=46) of cases. In this deception, scammer fabricated urgent financial needs to elicit money from victims. A smaller portion of the cases, 2.8% (*n*=3) involved unknown types of deception, where the deception used by scammer was unclear. The use of direct deposit was also measured, with coding “Yes=1” if used and “No=0” if not. Direct deposit was identified in 46.7% (*n*=50) of cases.

Scammers utilized several different methods to collect money from victims. The most frequent method was through a fake investment website, with 54.2% (n=58) of the cases. Scammer often set up fraudulent websites that appeared legitimate in order to deceive victims into transferring money. Another common method was through direct deposit into a crypto wallet, which was used in 40.2% (n=43) of the cases. Finally, a smaller portion of cases, 9.3% (n=10) involved direct deposit through Cash App, a popular mobile payment service, which scammer used to facilitate the transfer of funds. In a few cases, both types of direct deposits, including deposits to crypto wallets and Cash App, were used and a total of 53 direct deposit cases were found. The methods of exploitation and manipulation employed to deceive victims included both fake investment websites and direct deposit to cryptocurrency wallets as means for transferring funds.

Dependent variables

The dependent variables consist of two measures: (1) The monetary loss reported by individual cases (*individual level of monetary loss*) and (2) the total sum received in the reported cryptocurrency wallet addresses (*cluster level of total monetary loss*). In individual cases, the reported loss amounts are based on self-reported data from each victim, while cluster cases account for additional victims who were not individually counted but have sent funds to the same wallet, leading to a larger number of victims being associated with the reported address. The reported amounts were in cryptocurrency initially, however, to ensure consistency, all values were converted into U.S. dollars based on the exchange rate corresponding to the reported date. Due to the presence of extreme

outliers, each variable was recoded as explained below.

The Skewness and Kurtosis of *individual level of monetary loss* (dependent variable 1) was found to be 6.71 and 53.13 (Acceptable skewness standard is ± 3 and Kurtosis is ± 7 (Kline, 2011)), meaning there was a huge outlier exists in dollar amount lost. Consequently, these data were recoded into new variables by 25%, 50%, and 75% of the data, where values in the range of 1 through 1,525 were recoded to 1, values in the range of 1,526 through 7,400 to 2, values in the range of 7,401 through 41,167 to 3, values in above 41,167 to 4, and system-missing values were retained as system-missing. The mean of individual level of monetary loss was 2.48 (standard deviation (SD)=1.12).

The *cluster level of total monetary loss* (dependent variable 2) in each reported cryptocurrency addresses was measured to determine the total combined financial losses. In cases where multiple cryptocurrency addresses were reported by one victim, the monetary received from all addresses in each case were combined to provide a comprehensive total received. The Skewness and Kurtosis of cluster level of total received were found to exceed the standards values. Therefore, the data were recoded into new variables based on quartiles. Values from the 1 to 9683 were recoded as 1, values between 9684 through 77,839 were recoded to 2, values in the range of 77,840 to 270,984 were recoded as 3, and values above 270,984 were recoded as 4.

While the *individual level of monetary loss* (dependent variable 1) reflects data reported by an individual victim, the *cluster level of total monetary loss* (dependent variable 2) represents the larger scale of victimization. In other words, cluster level of total monetary amount received allows for a more accurate assessment of the scale of the

scam, as it provides a broader view of how the amount of financial damage fluctuates across multiple victims. The mean of cluster level of monetary loss was 2.52 (standard deviation (SD)=1.18).

Identification of Money Laundering (ML) Activities

The identification of money laundering activities was identified by using bitcoinwhoswho.com scam alert. If the alert was found "none," it was coded as 0, if the alert was found "This address has been reported as fraudulent," it was coded as 1. In most cases, 83.2% (*n*=89), no scam alert was found, while 16.8% (*n*=18) of the cases were found alert. Flags and risk alerts on Breadcrumbs, a blockchain analytics platform for investigating and tracking crypto transactions (Breadcrumbs, n.d.), were assessed. If the Risks/Flags were indicated with reported cryptocurrency wallet, it was marked as "Yes=1," and if the Risks/Flags were not indicated, it was marked as "No=0." The most notable was the CDA (hack, scam) flag, present in 21.5% (*n*=23) of the cases, while ATII (human trafficking) flags appeared in 8.4% (*n*=9) of the cases. The sanction status of each case was verified and coded as follows: if a reported case has been sanctioned by OFAC, it was marked as "Yes=1," and if not, it was coded as "No=0." None of the reported romance scams utilized in this study has been sanctioned by OFAC.

The use of money laundering techniques was identified according to the following variables: Swap, Mixers or Tornado Cash, Peel Chain, and Self-Fund. If any of these techniques were found in Breadcrumbs investigation tool, it was coded as "Yes=1," and "No=0" if none of these techniques were identified. The most common technique involved was the use of Mixers or Tornado Cash, found in 78.5% (*n*=84) of the cases,

meaning that scammers frequently employed these methods to obscure the origin of funds. Other money laundering techniques identified included Self-Fund, utilized in 45.8% (n=49) of cases, and Swap, which appeared in 43.0% (n=46) of cases. A smaller proportion of cases, 8.4% (n=9) involved the use of the Peel Chain technique. The type of swapping tools, the data was gathered and coded as follows: if any type of Swapping was detected in reported cases using the Breadcrumbs investigation tool, it was marked as "Yes=1," and "No=0" if there were none. Tokenlon was the most frequently utilized type of swap, representing 15.0% (n=16) of the cases, followed by MetaMask 12.1% (n=13), and UniSwap 11.2% (n=12).

Lastly, outgoing exchanges were assessed. The Breadcrumbs investigation tool allowed for the expansion of the outgoing path to trace three or more hops and identified the exchanges to which the funds were directed. A total fifty-seven exchanges were identified and coded as "Yes=1," if exchanges were identified in reported case and "No=0" if not. Among them, OKX exchange was the most frequently utilized by scammers, appearing in 26.8% (n=26) of the cases, followed by Kucoin exchange, which appeared in 14.4% (n=14) of cases. These exchange platforms played a significant role in the money laundering activities, as they were used multiple times, while other exchanges were utilized less times.

RESULTS

Regression analysis for monetary losses

The ordinary least squares (OLS) regression analysis was performed to analyze the relationship between dependent and independent variables. Dependent variables: *Individual level* and *cluster level of monetary losses.* Individual level refers to the amount of money lost as reported by individuals, while the cluster level represents the total received amount associated with the reported cryptocurrency addresses. Independent variables: *Bitcoin and Ethereum* (Types of Cryptocurrencies), *Direct deposit* (Financial Deception Strategies), *Use of money laundering (ML) techniques*, *Mixer or Tornado Cash*, *Number of Swaps*, *MetaMask*, *UniSwap*, *Kucoin*, and *OKX* (Identification of ML Activities).

As presented in Table 2, both Bitcoin and Ethereum were significantly associated with an increase in individual monetary loss ($b=.967$, $p<.001$ for Bitcoin; $b=.915$, $p<.001$ for Ethereum). Similarly, cluster level of monetary loss was also visible in usage of Bitcoin and Ethereum ($b=.675$, $p<.001$ for Bitcoin; $b=1.019$, $p<.001$ for Ethereum). In other words, scammers often target these two popular cryptocurrencies to maximize their gains. Bitcoin and Ethereum are the most widely used and valuable cryptocurrencies. Their high market capitalization and liquidity make them attractive to scammers, as they facilitate rapid conversion, while maintaining anonymity and lacking legal protections (Interpol, 2021; Federal Trade Commission, 2022).

Direct deposits to crypto wallets were also significantly associated with monetary losses. However, the relationship was negative for both individual monetary loss

(*b=-.469, p=.035*) and cluster monetary loss (*b=-.631, p=.011*). This finding suggests that when victims used direct deposits, they transferred smaller amounts of money. In other words, scammers tend to request relatively lower sums for direct deposits, not only to avoid raising suspicion from the victims but also to minimize the complexity of laundering the funds. In the context of money laundering, scammers often collaborate with specialized money laundering service providers, who typically manage the laundering processes rather than the scammers themselves (Chainalysis, 2023). Because such conversions involve additional technical steps, scammers may perceive them as more complex and requiring extra effort. As a result, they may be likely to limit the transaction to reduce the risk of detection.

Interestingly, use of money laundering techniques did not show a significant relationship with individual (*p=.165*) and cluster level of monetary losses (*p=.243*). This finding suggests that employing money laundering techniques does not necessarily lead to substantial monetary losses. Since scammers tend to conduct more transactions of smaller amounts (Foley et al., 2019) and given the availability of laundering tools on dark web services (Möser et al., 2013), no clear pattern emerges between monetary losses and the use of money laundering techniques.

When examining specific money laundering techniques, such as Mixer or Tornado Cash, the findings indicate a significant association with individual level of monetary loss (*b=.584, p=.029*). However, no significant effect was observed on cluster level of monetary loss (*b=-.129, p=.648*). These results suggest that the data analyzed in this study, the likelihood of financial loss at the individual level increases when scammers

employ Mixers or Tornado Cash. Mixers are often used in high-value romance scams to obscure the origin of funds (Chainalysis, 2023). In this study, high-value cases reported by individuals were more commonly associated with investment tactics. Given that large sums of money are frequently laundered through Mixers, individual monetary losses showed a significant relationship with the use of Mixers or Tornado Cash. On the other hand, monetary losses at the cluster level remained statistically insignificant. While the exact amounts of deposited funds remain unknown, when small sums are transferred from multiple victims, scammers can effectively evade detection without relying on Mixers or other money laundering techniques (Möser et al., 2013).

In contrast, the frequency of swap technique usage (number of swaps) demonstrated a significant associated with monetary loss at cluster level ($p=.042$). Notably, the relationship was negative ($b=-.351$), suggesting that a higher frequency of swaps may contribute to a slight reduction in total monetary losses. This finding suggests that scammers employ swapping tools to convert one cryptocurrency into another while simultaneously fragmenting large transactions into smaller amounts. By doing so, scammers enhance transaction obfuscation, complicating traceability and diminishing the likelihood of detection by law enforcement (Pandey, 2024). The frequency of swap technique usage was also negatively associated with individual monetary losses ($b=-.005$), but this relationship was statistically insignificant ($p=.974$).

Table 2. OLS Regression of Individual and Cluster Level of Monetary Losses

	Individual level monetary loss			Cluster level monetary loss		
	b	S.E.	*p*	*b*	S.E.	*p*
IV1. Bitcoin	.967	.170	<.001***	.675	.194	<.001***
IV2. Ethereum	.915	.193	<.001***	1.019	.223	<.001***
IV3. Direct Deposit	-.469	.218	.035*	-.631	.244	.011*
IV4. Use of ML Tech.	-.942	.672	.165	.892	.758	.243
IV5. Mixer or Tornado	.584	.263	.029*	-.129	.282	.648
IV6. # of Swap	-.005	.150	.974	-.351	.170	.042*
IV7. MetaMask	-.512	.430	.237	1.015	.489	.041*
IV8. UniSwap	.706	.549	.202	1.030	.611	.096
IV9. Kucoin	.396	.275	.153	.592	.298	.050*
IV10. OKX	-.546	.218	.014*	-.585	.246	.020*

*$p < .05$; **$p < .01$; ***$p < .001$.

The type of swapping tool utilized was found to be related with monetary loss. Specifically, the use of MetaMask had a positive relationship in cluster level of monetary loss (*b=1.015, p=.041*), but did not significantly affect individual level of monetary loss (*b*=-.512, *p*=.237). This finding suggests that while the use of MetaMask in individual cases does not significantly influence financial losses, its application as a swapping tool by scammers contributes to greater at cluster level of monetary losses. MetaMask is widely used platform that enables users to interact with decentralized applications. Through MetaMask users securely connect digital wallets to various decentralized applications without compromising while also facilitating cryptocurrency swaps across blockchain (MetaMask, 2025; Tangem, 2025).

Interestingly, on the other swapping tools, such as Tokenlon, was found to be insignificantly associated with monetary losses. Similarly, the use of UniSwap did not demonstrate a significant relationship with financial losses. Tokenlon and UniSwap enable swaps, allowing all transactions to be executed via smart contracts without the need for intermediary or trusted third party (Agarwal et al., 2023; Maras & Ives, 2024). However, the frequency of a tool's usage does not necessarily correspond to its involvement in high-value crimes, as many criminals adopt widely accessible tools primarily for convenience (Foley et al., 2019; Möser et al., 2013).

Certain cryptocurrency exchanges demonstrated a relationship with monetary loss. While Kucoin was not significantly associated with individual monetary loss, it demonstrated a weak but positive relationship with cluster level of monetary loss (*b=.592, p=.050*). This finding suggests that cases involving the use of the Kucoin exchange were linked to increased financial losses. Kucoin's relatively lenient KYC requirements, which do not mandate full ID verification but only require an email at sign up, have made it an attractive platform for scammers (Homeland Security, 2022). In contrast, OKX exchange was negatively associated with both individual level (*b=-.546, p=.014*) and cluster level (*b=-.585, p=.020*) of monetary losses. Scammers often employ a strategy of splitting funds into smaller amounts and utilizing OKX exchange for micro-withdrawals of cryptocurrency to enhance anonymity and reduce traceability (OKX Learn, 2023). The correlations and covariance between the variables are presented in Appendix A.

Romance Scams Mapping

Modus operandi of romance scams

Figure 1 illustrates the structured progression of a romance scams involving cryptocurrency, detailing the steps-by-steps employed by scammers to deceive victims and obscure illicit financial transactions. The process began with scammers initiating contact through dating applications, such as Tinder, which was identified as the most frequently utilized platform in this study. Communication then transitioned from the dating app to a private, encrypted messaging platform, such as WhatsApp, allowing scammers to establish trust and rapport with their victims. Once trust is cultivated, scammers fabricated financial hardships or presented high-return investment opportunities to persuade victims to transfer cryptocurrency. In investment-related scenarios, scammers directed victims to fraudulent investment platforms or deceptive links, whereas in emergency-related scenarios, scammers asked money for medical bills and provided direct cryptocurrency wallet addresses for fund transfers. Victims, believing they were either assisting a trusted individuals or securing a lucrative financial return, proceeded with the cryptocurrency transfer. Upon receipt of funds, the scammers employed various money laundering techniques including swaps, mixers, peel chains and self-fund to conceal the origin and movement of funds. The laundered cryptocurrency was then ultimately withdrawn through exchanges with weak regulatory oversight. As the scam reaches its final stage, the scammers sever all lines of communication with victims. In most case in this study, victims reported that their messages went unanswered, social media profiles were deleted, and any previously used phone numbers or email addresses

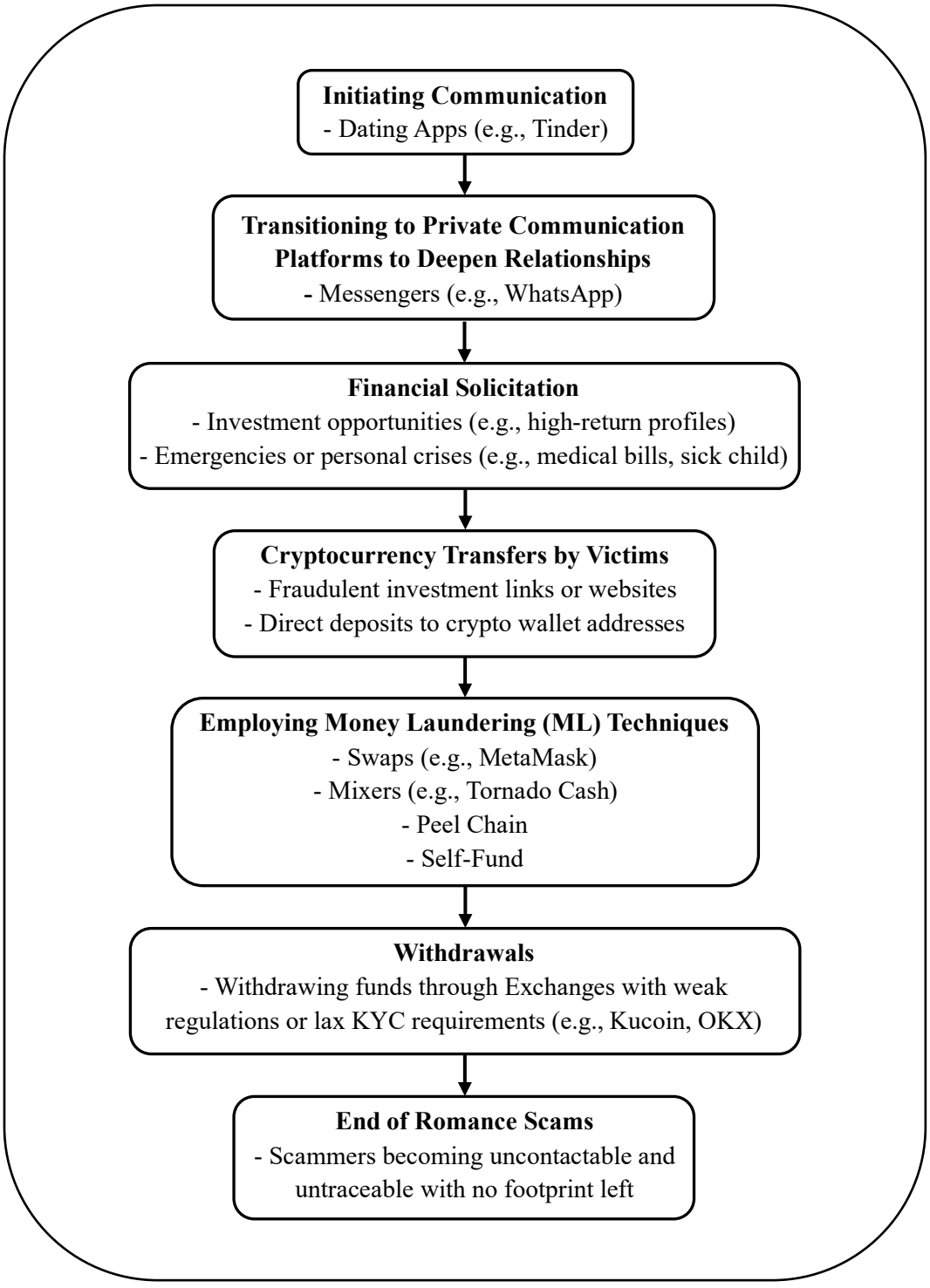
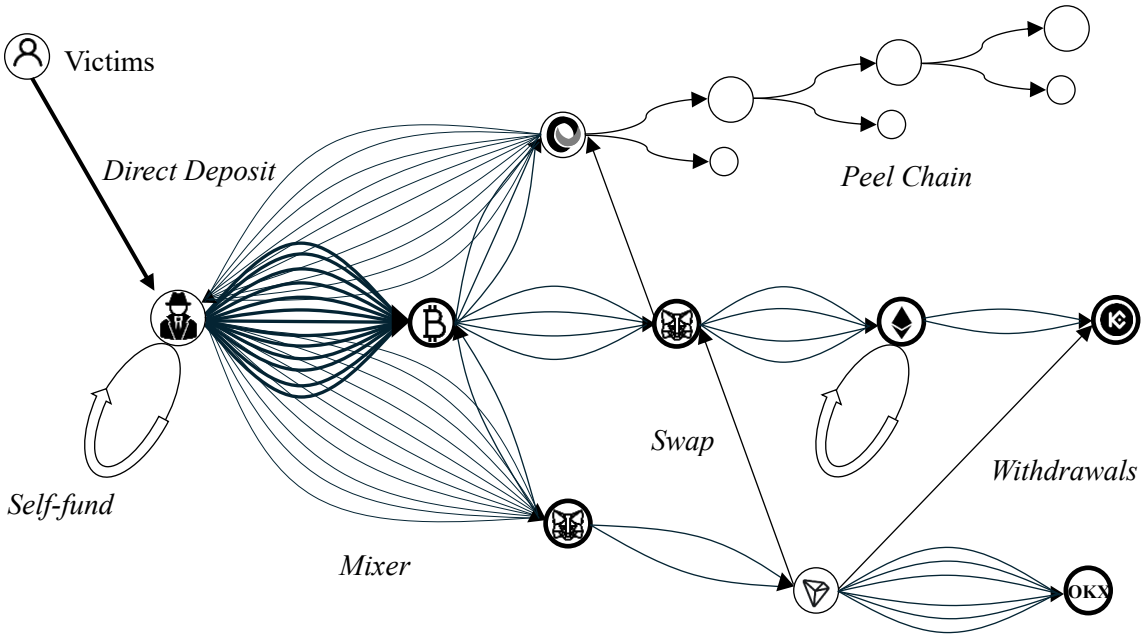


Figure 1. The modus operandi of romance scams involving cryptocurrency

became inactive. This sudden disappearance is also a deliberate tactic to avoid detection and prevent the victim from pursuing further contact or legal action (Whitty, 2015; Cross 2023).

Blockchain forensic mapping of money laundering

Each reported case was tracked down using Breadcrumbs investigation tool with the law enforcement plan. Various money laundering techniques were identified, including Swap, Mixer or Tornado Cash, Peel Chain, and Self-Fund. Figure 2 shows a



The figure represents a simplified version of blockchain cryptocurrency mapping in romance scams with various money laundering techniques. The thickness of the line represents the elements that were found to be significant in this study (e.g., Bitcoin, Ethereum, MetaMask, OKX, and Mixer). The component within the figure is categorized as follows:

	Reported crypto address		Bitcoin (Crypto)		Ethereum (Crypto)
	MetaMask (Swap)		Tron (Crypto)		Kucoin (Exchange)
OKX	OKX (Exchange)		Larger Cryptocurrency		Smaller Cryptocurrency
	Tokenlon (Swap)				

Figure 2. The pattern of money laundering techniques in romance scams

simplified representation of the structural pattern associated with each technique.

Swap Technique: The Swap technique involved the conversion of one cryptocurrency into another. In this study, cryptocurrency was converted through swap techniques and mostly utilized tools were Tokenlon and MetaMask. Although Tokenlon was found to be not significantly associated with monetary losses, the number of swapping activities was found to be significantly associated negatively. *Mixer technique*: The Mixer technique displayed a "Bell shaped" pattern, where cryptocurrency was fragmented into smaller amounts and distributed across multiple times. In most cases, a fixed sum was repeatedly transferred, generating ten or more transactions and reinforcing Bell shaped characteristic (Chainalysis, 2023). Furthermore, funds were repeatedly split and rerouted to multiple wallets in this study. *Peel Chain*: The Peel Chain technique involved a recurring pattern of two-part transactions, where a larger sum was transferred alongside a smaller amount. When tracing the larger transactions, they exhibited a continuous, repetitive pattern, resembling a wave-like structure and the funds were gradually dispersed. Although Peel Chain was found to be insignificant in this study, the pattern of cryptocurrency “peels” has been observed in various criminal cases and is widely utilized as money laundering techniques (Bellei et al., 2024). *Self-Fund*: The Self-Fund technique involved a loop or circular transaction, where funds were sent out and then partially or fully returned to the same wallet. Although it was found to be not significant, it was the second most utilized technique in this study, with a total of 49 cases (45.8%).

DISCUSSION AND LAW ENFORCEMENT ROMANCE CRYPTO SCAMS INVESTIGATION GUIDELINES

The study is focused on cryptocurrency, specifically exploring the patterns of its use and the modus operandi in romance scams. In romance scams, scammers often utilize dating apps or social networking sites to begin communication with potential victims. The next step scammers take is transitioning to a private messaging platform for further interaction. The reason scammers transited to a private communication platform is not only to make it more difficult for law enforcement agencies to track communications but also to get more personal information from the victims (Lafayette Federal Credit Union, 2023) and to isolate the target (Anderer, 2023). In addition, the emergence of messaging applications that do not require users to link their accounts to real phone numbers or to provide personal information has facilitated various forms of cybercrime (Owen-Jackson, 2024). Scammers use private messengers to pressure victims into making decisions relatively quickly. Once scammers have built a relationship with victims, they begin requesting money through fake pretenses. The findings of this study revealed that the tactics scammers use more to extort money was investment tactic. After the relationship has deepened and victims are no longer suspicious, scammers present a fake investment opportunity, directing them the links to fake websites or platforms. Initially, scammers persuade victims to make a small investment, demonstrating fabricated profits to build credibility and encourage further contribution (Agarwal et al., 2023). This method allows scammers to extract substantial sums of money with minimal effort. The fake websites scammers created often taken down shortly after the funds are received, making it easier for scammers to cover their tracks. This ability to disappear, and the large sum gains are

key reasons scammers favor investment scenarios using messengers in romance scams involving cryptocurrency.

The use of cryptocurrency as the preferred method for receiving money in criminal activities has become increasingly mainstream (Chainalysis, 2025). Its speed, ease of transfer, and ability to obscure transaction trails have contributed to its widespread adoption among scammers. This study showed that the monetary loss increased significantly when the Bitcoin or Ethereum were involved. In other words, scammers generated substantial profits by extorting these types of cryptocurrencies from victims. Bitcoin often exhibited lower volatility, making it a relatively safter investment option (Anuar & Hussain, 2024). As a result, users may perceive Bitcoin as a more stable asset, potentially influencing their willingness to use it in financial transactions. Interestingly, this study revealed that the direct deposit has significant association with monetary losses, however, the relationship was negative. This negative correlation suggests that as the use of direct deposits increased, overall monetary losses decreased. Specifically, victims who directly deposited fund into cryptocurrency addresses provided by scammers, typically observed in emergency-related scenarios, incurred lower financial losses compared to those who transferred funds through fraudulent investment websites. These findings indicate that scammers favored investment scenario, as these facilitated larger financial transactions and yielded higher profits.

In terms of money laundering techniques, the findings suggest that while the overall use of money laundering techniques is not directly associated with monetary losses, the specific types of money laundering techniques employed do have an impact.

Among the four types, mixers, swaps, peel chain and self-fund, the use of mixers was linked to an increase in monetary losses in the individual case of this study. In contrast, a greater use of swapping tools was associated with lower financial losses in the cluster case, suggesting that scammers may swap multiple times with smaller amount of funds. By utilizing swapping, scammers can conduct multiple swaps across various platforms, including decentralized and centralized exchanges, creating a convoluted transactions trails that complicates investigative efforts (Pandey, 2024). In other words, the scammers use more frequently swaps to lower the total monetary losses appeared to be to hinder trails. Among the type of swaps, MetaMask was used for tending to involve significant amounts of money, the study found, indicating that scammers profit from its use the most. In summary, cases involving swapping tools may result in small (and large) losses and it could be linked to severe incidents. Therefore, prioritizing cases based on risk level rather than the reported amount would be beneficial in investigations. Even when losses seem minimal, they may contribute substantially to larger patterns, thus it is important not to overlook smaller amounts during the investigation.

This study also identified a withdrawal exchange frequently utilized by scammers, which exhibited a significant correlation with increased monetary losses, Kucoin. Kucoin implemented measures to prevent customers from identifying themselves as U.S.-based, thereby circumventing Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations (DOJ, 2025a). Kucoin offered an alternative way for identity verification process such as larger daily withdrawals (Botwinick, 2024). As a result, Kucoin functioned as a conduit for laundering proceeds derived from suspicious and criminal

activities. In addition, OKX, another exchanges, was found to be scammer's favored exchanges due to a weak or no KYC process (DOJ, 2025b). The relationship found to be negative with monetary losses, suggesting scammers withdrawals relatively smaller amount of money repetitively. OKX has served as preferred withdrawals platform due to its features that facilitate the use of mixer techniques, enhancing transaction privacy and anonymity (OKX Learn, 2023). Recently, on January and February of 2025, Kucoin and OKX exchanges pleaded guilty violating anti-money laundering laws and sentenced to pay hundreds of millions of dollars (DOJ, 2025a; DOJ, 2025b).

POLICY AND RECOMMENDATIONS

One of the biggest challenges is the growing use of cryptocurrency in illegal activities. Because digital currencies are anonymous and decentralized, they make it much easier for criminals to hide their actions. To stay ahead of these evolving threats, developing stronger, more comprehensive strategies is crucial.

Strengthening Law Enforcement Training on Cryptocurrency and Romance Scams: Given the rising prevalence of romance scams, which increasingly involve cryptocurrency transactions, it is essential that law enforcement agencies receive enhanced, specialized training to effectively detect, investigate and respond to crimes. Training should focus on the identification of digital fraud patterns, understanding the intricacies of blockchain technology, and developing the skills necessary to trace illicit cryptocurrency transactions. In addition, equipping law enforcement personnel with the knowledge to recognize red flags in online interactions would be helpful in addressing the global nature of crime in virtual space.

Developing Advanced Investigative Techniques: As cryptocurrency transactions are increasingly used for money laundering, it is crucial for law enforcement agencies to adopt advanced investigative techniques tailored to tracing digital currencies. Tools that can quickly detect suspicious transactions and track funds across multiple wallets and exchanges will greatly enhance their efforts. Additionally, specialized forensic tools and expertise will help law enforcement track and analyze blockchain data, identify illicit withdrawals, and uncover hidden networks of criminal activity.

Establishing an Awareness and Prevention Program for Public: Due to the nature of romance scams and the way dating apps operate, traditional detection methods, such as spam filtering, are often inadequate (Suarez-Tangil et al., 2020). Therefore, educating the public about the risks and warning signs of scams is essential. For instance, public awareness campaigns targeting vulnerable populations can significantly reduce the number of victims. Specifically, providing individuals with practical tips on how to recognize fake online profiles, understanding the role of cryptocurrency in these scams and avoiding fraudulent relationships can help mitigate the risks associated with cryptocurrency-involved scams. Despite consistent educational efforts, some individuals may still fall victim to romance scams due to socio-demographic factors, such as cultural backgrounds and a lack of awareness about cyber threats (Back & Guerette, 2021). Therefore, the establishment of a culture and environment of cybersecurity awareness may be crucial for the enhancement of strategies aimed at the prevention of romance scams. Regular updates on the latest romance scams information and cybersecurity issues would also help create a cybersecurity awareness culture.

Enhancing Ongoing Education and Capacity building for Prosecutors and Judges: To effectively prosecute these crimes, legal professionals should be equipped with the technical knowledge necessary to understand the complexities of cryptocurrency transactions and digital forensics. Therefore, developing specialized legal resources and guidelines to assist the judiciary in navigating cryptocurrency-related cases may be helpful. Additionally, fostering collaborations between legal experts, blockchain

specialists, and law enforcement could provide ongoing support to the legal community in addressing these complex cryptocurrency-related cases.

Building a Robust Cryptocurrency Regulation in the Second Trump Administration: The recent U.S. presidential election results have had a notable impact on the value of cryptocurrency, particularly Bitcoin, which experienced a sharp increase in price following the election of President Donald Trump (Sherman, 2024). While President Trump's commitment to fostering cryptocurrency growth presents exciting opportunities for the industry (McGinnis et al., 2024), the rapid rise in value without proper regulation could create a breeding ground for criminal activity. Therefore, it is crucial for the U.S. to take a proactive approach to regulating this emerging sector. A well balanced and structured regulatory framework that encourages innovation while ensuring accountability will help keep the cryptocurrency market stable, transparent, and conducive to long term crime free growth.

Adopting of a Unified Global Jurisdiction: As countries have varying legal frameworks and jurisdictions for addressing crimes, this disparity extends to virtual spaces as well. Different jurisdictions may apply to different countries and their online activities. For instance, browser extensions like MetaMask, operating in certain regions, may not be subject to subpoenas due to jurisdictional differences between countries. Therefore, the implementation of a unified global jurisdiction for cybersecurity is essential to effectively address cross-border cybercrimes and ensure accountability under a common legal framework.

LIMITATIONS

There are several limitations related to the data used in this study that should be acknowledged. First, the data is based on self-reported accounts from individuals who believe they have fallen victim to romance scams. These individuals may not have the necessary expertise to distinguish between romance scams and other types of online fraud, such as pig butchering scams, which can be difficult to identify, particularly in online relationships. Another key limitation is that the data relies on victims' recollections of events. The narratives and cryptocurrency addresses provided by the victims were collected as reported. There was no ability for researcher to contact victims and verify data reported independently. Additionally, the timing of victims' realization and reporting may vary. Some victims may have recognized and reported the romance scam immediately, while others may have done so long after the incident occurred. Despite these limitations, the data offers valuable insights into the patterns of cryptocurrency usage in online romance scams.

Appendix A Correlations and Covariance Between Variables

	DV1	DV2	IV1	IV2	IV3	IV4	IV5	IV6	IV7	IV8	IV9	IV10
DV1	1											
	1.252											
DV2	.585**	1										
	.702	1.272										
IV1	.318**	.048	1									
	.252	.039	.510									
IV2	.230*	.361**	-.510**	1								
	.167	.259	-.230	.397								
IV3	-.054	-.220*	.441**	-.329**	1							
	-.030	-.124	.158	-.104	.251							
IV4	.024	.183	.079	.054	.086	1						
	.005	.040	.011	.006	.008	.036						
IV5	.123	-.061	.002	-.048	.216*	.377**	1					
	.055	-.029	.001	-.013	.045	.030	.170					
IV6	.083	.152	-.442**	.617**	-.368**	.098	-.030	1				
	.128	.223	-.422	.520	-.247	.025	-.016	1.791				
IV7	-.146	.187	-.411**	.435**	-.291**	.073	-.084	.566**	1			
	-.056	.070	-.096	.090	-.048	.005	-.011	.249	.108			
IV8	.168	.127	-.351**	.423**	-.333**	.070	.042	.779**	.230*	1		
	.060	.046	-.079	.084	-.053	.004	.005	.331	.024	.101		
IV9	.054	.044	.186	-.219*	.180	.060	.045	-.173	-.131	-.131	1	
	.022	.018	.046	-.048	.032	.003	.006	-.077	-.014	-.014	.125	
IV10	-.246*	-.125	-.147	.058	-.273**	.088	-.070	.064	.047	.047	.149	1
	-.125	-.061	-.046	.016	-.061	.006	-.012	.036	.006	.006	.023	.198

The upper value in each cell is the Pearson correlation coefficient, while the lower value is covariance.
** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).

Variable identifier chart

DV1	Individual monetary loss	IV3	Direct deposit	IV7	MetaMask
DV2	cluster monetary loss	IV4	Use of ML tech.	IV8	UniSwap
IV1	Bitcoin	IV5	Mixer or Tornado cash	IV9	Kucoin
IV2	Ethereum	IV6	Number of swaps	IV10	OKX

REFERENCES

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management, 34*(2), e2255. doi:10.1002/nem.2255

Anderer, J. (2023, February 10). *Valentine's Day deception: Here's how scammers use dating apps to target victims*. StudyFinds. https://studyfinds.org/scammers-dating-apps-victims/

Anuar, M., & Hussain, S. I. (2024). Behaviour of extreme volatility in cryptocurrency: Bitcoin VS Ethereum. *AIP Conference Proceedings. 2905*(1). https://doi.org/10.1063/5.0172079

Back, S., & Guerette, R. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *Journal of Contemporary Criminal Justice, 37*(3), 427–451. doi:10.1177/10439862211001628

Baluch, A. (Writer), & DiGiacinto, J. (Editor). (2024, October 8). *Best Dating Apps of 2024, According to Research.* Forbes Health. https://www.forbes.com/health/dating/best-dating-apps/

Bellei, C., Xu, M., Phillips, R., Robinson, T., Weber, M., Kaler, T., … Chen, J. (2024). The Shape of Money Laundering: Subgraph Representation Learning on the Blockchain with the Elliptic2 Dataset. https://arxiv.org/pdf/2404.19109

Bogos, C-E., Mocanu, R., & Simion, E. (2023). A security analysis comparison between Signal, WhatsApp and Telegram. *ResearchGate.* https://www.researchgate.net/publication/367350335_A_security_analysis_comparison_between_Signal_WhatsApp_and_Telegram

Bolster. (2024, May 30). *Why Do Scammers Want You to Use Telegram?* https://bolster.ai/blog/why-do-scammers-want-you-to-use-telegram

Botwinick, N. (2024, April 4). *Kucoin and founders charged with operating illegally as money transmitter and futures commission merchant*. Ballard Spahr. https://www.moneylaunderingnews.com/2024/04/kucoin-and-founders-charged-with-operating-illegally-as-money-transmitter-and-futures-commission-merchant/

Breadcrumbs. (n.d.). *Making Blockchain Analytics Accessible to Everyone*. https://www.breadcrumbs.app/about

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law, 20*(3), 261–283. doi:10.1080/1068316X.2013.772180

Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime, 29*(2), 460–475. doi:10.1108/JFC-02-2021-0042

Chainalysis. (2022a, August 23). *Crypto Mixers and AML Compliance.* https://www.chainalysis.com/blog/crypto-mixers/

Chainalysis. (2022b, August 30). *Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions.* https://www.chainalysis.com/blog/tornado-cash-sanctions-challenges/#how-it-works

Chainalysis. (2023, February). *The 2023 Crypto Crime Report*. https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf

Chainalysis. (2024, February). *The 2024 Crypto Crime Report*. https://www.pensamientopenal.com.ar/system/files/Documento_Editado1686.pdf

Chainalysis. (2025, January 15). *2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized.* https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

Chuang, J-Y. (2021). Romance Scams: Romantic Imagery and Transcranial Direct Current Stimulation. *Frontiers in Psychiatry, 12*. doi: 10.3389/fpsyt.2021.738874

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. *Clinical Practice & Epidemiology in Mental Health, 16,* 24–35. doi: 10.2174/1745017902016010024

Congressional Research Service. (2023, May 23). *Introduction to Cryptocurrency*. https://sgp.fas.org/crs/misc/IF12405.pdf

Craig, W. (2024, July 18). *Love at first sight? AI making it even harder to detect romance scams.* The Canadian Press; Toronto. https://www.proquest.com/docview/3082836479

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety, 24,* 30–41. https://doi.org/10.1057/s41300-021-00134-w

Cross, C. (2023). "I knew it was a scam": Understanding the triggers for recognizing romance fraud. *Criminology & Public Policy, 22,* 613–637. doi:10.1111/1745-9133.12645

Curry, D. (2024, September 30). *Dating App Revenue and Usage Statistics (2024).* Business of Apps. https://www.businessofapps.com/data/dating-app-market/

Department of Treasury. (2024). *2024 National Money Laundering Risk Assessment.* https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf

DOJ. (2022, April 13). *Four Individuals Charged with Conspiring to Launder Money Obtained from Romance Scams.* https://www.justice.gov/usao-nj/pr/four-individuals-charged-conspiring-launder-money-obtained-romance-scams

DOJ. (2024a, February 14). *Romance Scammers Accused of Taking More Than Love from Victims, Approximately $8M*. https://www.justice.gov/usao-ut/pr/romance-scammers-accused-taking-more-love-victims-approximately-8m

DOJ. (2024b, September 11). *Florida Woman Pleads Guilty to Laundering Millions of Dollars As Part Of Romance Scams*. https://www.justice.gov/opa/pr/florida-woman-pleads-guilty-laundering-millions-dollars-part-romance-scams

DOJ. (2025a, January 27). *Kucoin pleads guilty to unlicensed money transmission charge and agrees to pay penalties totaling nearly $300 million*. https://www.justice.gov/usao-sdny/pr/kucoin-pleads-guilty-unlicensed-money-transmission-charge-and-agrees-pay-penalties

DOJ. (2025b, February 24). *OKX pleads guilty to violating U.S. anti-money laundering laws and agrees to pay penalties totaling more than $500 million*. https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and-agrees-pay-penalties

Dupuis, D., & Gleason, K. (2021). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime, 28*(1), 60–74. doi: 10.1108/JFC-06-2020-0113

Fair, L. (2024, February 13). *"Love Stinks" – when a scammer is involved*. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2024/02/love-stinks-when-scammer-involved

Fansher, A. K., & McCarns, K. (2019). Risky Online Dating Behaviors and Their Potential for Victimization. *Crime Victims' Institute.* doi: 10.13140/RG.2.2.24083.84007

FBI. (2023a). *Cryptocurrency Fraud Report 2023.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3CryptocurrencyReport.pdf

FBI. (2023b). *Elder Fraud Report 2023*. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

Federal Trade Commission. (2022, May). *What To Know About Cryptocurrency and Scams.* https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

Federal Trade Commission. (2023, February). *Romance scammers' favorite lies exposed*. https://www.ftc.gov/system/files/ftc_gov/pdf/romance-spotlight-2023.pdf

Fletcher, R., Tzani, C., & Loannou, M. (2024). The dark side of Artificial Intelligence – Risks arising in dating applications. *Assessment & Development Matters, 16*(1), https//doi.org/10.53841/bpsadm.2024.16.1.17

Foley, S., Karlsen, J. R., & Putnins, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853. https://www.jstor.org/stable/48568941

Global Coalition to Fight Financial Crime. (2024). *Financial Scams Report – An Assessment of Scams in East Asia – in Australia, Hong Kong & Singapore.* https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd-3.pdf

Homeland Security. (2022). Combating Illicit Activity Utilizing Financial Techniques and Cryptocurrencies. https://www.dhs.gov/sites/default/files/2022-09/Combatting%20Illicit%20Activity%20.pdf

Homeland Security. (2023). Combating Illicit Activity Utilizing Financial Techniques and Cryptocurrencies Phase II: A Focus on the Evolution of Digital Assets by Threat Actors and Organized Criminal Groups. https://www.dhs.gov/sites/default/files/2023-09/08.%20Combatting%20Illicit%20Activity%20Phase%202_508_0.pdf

Immunebytes. (2023, January 4). *What is Tornado Cash? Why Is It Popular with Hackers?* https://www.immunebytes.com/blog/what-is-tornado-cash-why-is-it-popular-with-hackers/#Decentralizednbsp

Ingolf, G. A. P., & Brett, S. (2021). Cryptocurrency. *Internet Policy Review, 10*(2). https://doi.org/10.14763/2021.2.1561

Interpol. (2021, December 9). Cryptocurrency crime: preventing the misuse of virtual assets by organized crime for money laundering. https://www.interpol.int/en/News-and-Events/News/2021/Cryptocurrency-crime-preventing-the-misuse-of-virtual-assets-by-organized-crime-for-money-laundering

Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3rd ed.). Guilford Press.

Kramer, J-A., Blokland, A. A. J., Kleemans, E. R., & Soudijn, M. R. J. (2023). Money laundering as a service: Investigating business-like behavior in money laundering networks in the Netherlands. *Trends in Organized Crime.* https://doi.org/10.1007/s12117-022-09475-w

Lafayette Federal Credit Union. (2023, March 2). *Tell-Tale Signs You're Falling for a Romance Scam*. https://www.lfcu.org/news/protecting-your-identity/tell-tale-signs-youre-falling-for-a-romance-scam/

Low, S. M. P., Bolong, J., Waheed, M., & Wirza, J. (2022). Online Dating in Asia: A Systematic Literature Review. *International Journal of Academic Research in Business and Social Sciences*, *12*(14), 177– 195. http://dx.doi.org/10.6007/IJARBSS/v12-i14/15822

Maras, M-H., & Arsovska, J. (2023). Understanding the Intersection Between Technology and Kidnapping: A Typology of Virtual Kidnapping. *International Criminology, 3*, 162–176. doi:10.1007/s43576-023-00091-4

Maras, M-H., & Ives, E. R. (2024). Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States. *Journal of Economic Criminology, 5*. https://doi.org/10.1016/j.jeconc.2024.100066

Marrazzo, L. (2024, February 15). *Most Popular Dating Apps per Country.* Apptweak. https://www.apptweak.com/en/aso-blog/check-out-the-most-popular-dating-apps-by-country

McClain, C., & Gelles-Watnick, R. (2023, February 2). *From Looking for Love to Swiping the Field: Online Dating in the U.S.* Pew Research Center. https://www.pewresearch.org/internet/2023/02/02/from-looking-for-love-to-swiping-the-field-online-dating-in-the-u-s/

McGinnis, J., Lichtenstein, J., & Reinstein, J. (2024, November 19). *A Second Trump Administration: Implications for Asset Managers.* Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2024/11/19/a-second-trump-administration-implications-for-asset-managers/

MetaMask. (2025, January 21). *How to swap crypto*. https://metamask.io/news/how-to-swap-crypto

Möser, M., Böhme, R., & Breuker, D. (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *2013 APWG eCrime Researchers Summit,* 1–14. https://doi.org/10.1109/eCRS.2013.6805780

Murphy, A. (2018). Dating Dangerously: Risks Lurking within Mobile Dating Apps. *Catholic University Journal of Law and Technology, 26*(1). https://scholarship.law.edu/jlt/vol26/iss1/7

Nadler, M., & Schär, F. (2023). Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers. *Review – Federal Reserve Bank of St. Louis, 105*(2), 122–136. https://doi.org/10.20955/r.105.122-136

Neumann, M., & Sartor, N. (2016). A Semantic Network Analysis of Laundering Drug Money. https://www.researchgate.net/publication/299997567

OKX Learn. (2023, May 22). *Coin mixer: What is it and how does it work?* OKX. https://www.okx.com/en-eu/learn/what-is-coin-mixer?

Owen-Jackson, C. (2024, November 6). *What Telegram's recent policy shift means for cyber crime*. Security Intelligence. https://securityintelligence.com/articles/what-telegrams-recent-policy-shift-means-for-cyber-crime/

Pandey, P. (2024, June 13). *Coin Swapping: Money Laundering Tactics on Crypto Exchanges*. Merkle Science. https://www.merklescience.com/blog/coin-swapping-money-laundering-tactics-on-crypto-exchanges

Paredes, N. (2024, August 8). *What is a Crypto Swap and How Does It Work?* CoinFlip. https://coinflip.tech/blog/what-is-a-crypto-swap

Shapiro, L. R. (2023). Online Romance Scammers. In *Cyberpredators and Their Prey* (1st ed., pp. 17–41). CRC Press. https://doi.org/10.4324/9781003092292-2

Sherman, R. (2024, November 22). Donald Trump could create first 'crypto czar.' *Fox 40.* https://fox40.com/news/national-and-world-news/donald-trump-could-create-first-crypto-czar/

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal, 32.* 342–361. doi:10.1057/s41284-019-00166-w

Staples, A. (2024, January 12). *What is Cash App and how does it work?* CNBC. https://www.cnbc.com/select/what-is-cash-app/

Suarez-Tangil, G., Edwards M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2020). Automatically Dismantling Online Dating Fraud. (2020). *IEEE Transactions on Information Forensic and Security, 15*, 1128–1137. doi:10.1109/tifs.2019.2930479

Tableau Public. (2024, July 24). Fraud Reports by Federal Trade Commission. Retrieved on September 13, 2024. https://public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6

Tangem. (2025, February 4). *What is MetaMask*. https://tangem.com/en/glossary/metamask/

Teaster, P. B., Roberto, K. A., Savla, J., Du, C., Du, Z., Atkinson, E., … Lichtenberg, P. A. (2023). Financial Fraud of Older Adults During the Early Months of the COVID-19 Pandemic. *The Gerontologist, 63*(6), 984–992.

Thomala, L. L. (2024, April 23). *Monthly active users of the largest mobile online casual dating apps in China as of Feb 2024.* Statista. https://www.statista.com/statistics/1131443/china-most-popular-mobile-dating-apps/

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science, 2*. doi: 10.3389/fcomp.2020.600596

United Nations. (2023). Online scam operations and trafficking into forced criminality in southeast Asia: recommendations for a human rights response. https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

United States v. Marfo, 2022R00271 (D. New Jersey. 2022). https://www.justice.gov/usao-nj/press-release/file/1494321/dl

United States v. Lam and Serrano (D. Columbia, 2024). https://www.justice.gov/usao-dc/media/1369661/dl

United States. v. Ilya "Dutch" Lichtenstein and Heather Morgan. (D.D.C. Feb. 7, 2022). No. 1:22-mj-00022-RMM, Document 1-1. https://www.justice.gov/opa/press-release/file/1470211/dl

Vejačka, M. (2014). Basic Aspects of Cryptocurrencies. *Journal of Economy, Business and Financing, 2*(2). https://www.researchgate.net/publication/292586903_Basic_Aspects_of_Cryptocurrencies

Western Union. (2019, May 2). *How do I send money with Western Union?* https://wucare.westernunion.com/s/article/How-do-I-send-money-online?language=en_US

Whitty, M. T. (2013). The scammers persuasive techniques model. *The British Journal of Criminology, 53*(4), 665–684. doi:10.1093/bjc/azt009. https://www.jstor.org/stable/23640056

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443–455. doi:10.1057/sj.2012.57

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: the psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice, 16*(2), 176–194.

Wronka, C. (2022). Money laundering through cryptocurrencies – analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25*(1), 79–94. doi: 10.1108/JMLC-02-2021-0017

Wu, S., & Trottier, D. (2022) Dating apps: a literature review. *Annals of the International Communication Association, 46*(2), 91–115, doi:10.1080/23808985.2022.2069046

VITA