information

MDPI

Article

Uncovering Cryptocurrency-Enabled Sextortion: A Blockchain Forensic Analysis of Transactions and Offender Laundering Tactics

Kyung-Shick Choi [1], Mohamed Chawki [2,*] and Subhajit Basu [3]

[1] Department of Applied Social Sciences, Boston University, Boston, MA 02215, USA; kuung@bu.edu
[2] Department of Law, Naif Arab University for Security Sciences, Riyadh 14812, Saudi Arabia
[3] School of Law, University of Leeds, Leeds LS2 9JT, UK; s.basu@leeds.ac.uk
* Correspondence: mshaker@nauss.edu.sa

Abstract

Sextortion has rapidly expanded into a global cyber-enabled crime that leverages anonymous digital communication and decentralized payment systems. This study examines the financial infrastructures underlying contemporary sextortion by conducting a two-phase analysis of 87 confirmed cases involving cryptocurrency payments. Using blockchain forensic tools and open-source intelligence, the research traces fund movements across perpetrator-controlled wallets, identifies laundering techniques such as mixers, peel-chain transfers, and exchange-based cash-outs, and links these behaviors to narrative patterns within victim reports. The results reveal a dual-tier ecosystem in which mass-produced, multilingual extortion scripts coexist with divergent laundering typologies that differentiate lower-value, high-volume scams from more organized and higher-yield operations. By integrating qualitative and quantitative evidence, this study provides a forensic framework for detecting illicit cryptocurrency activity, improving threat classification, and strengthening investigative and regulatory responses to sextortion and related crypto-enabled interpersonal crimes.

Keywords: sextortion; cryptocurrency; blockchain forensics; money laundering typologies; crypto mixing; financial cybercrime; transaction forensics; dark web laundering; digital extortion; crypto-facilitated abuse

1. Introduction

Sextortion, defined as coercing individuals through threats to disclose intimate images, videos, or personal information unless a demand is met, has emerged as one of the most rapidly expanding forms of cyber-enabled interpersonal crime [1]. Recent data from the National Center for Missing and Exploited Children reveal a dramatic escalation in reported financial sextortion, increasing from 10,731 cases in 2022 to 26,718 cases in 2023 [2]. Federal agencies, including the Federal Bureau of Investigation (FBI) and Homeland Security Investigations (HSI), documented more than thirteen thousand sextortion cases involving minors during the same period and linked several youth suicides to these escalating threats [3]. This surge reflects a broader transformation in the global cybercrime landscape in which interpersonal exploitation is increasingly automated, financially motivated, and technologically mediated.

Cryptocurrency now plays a central role in this evolution. Its pseudonymous architecture, combined with a growing ecosystem of privacy-enhancing tools, has made digital

Academic Editors: Paulina Rutecka and Pedro Pinto

Received: 11 January 2026
Revised: 25 February 2026
Accepted: 27 February 2026
Published: 1 March 2026

assets particularly attractive to extortion offenders seeking to obscure the movement of illicit proceeds. Blockchain analytics firms have reported a steady rise in crypto-based sextortion payments, including identifiable laundering signatures that differentiate low-skill mass-email offenders from more organized and technologically capable groups [4,5]. These laundering signatures, which include the use of mixers, peel chains, and multi-hop obfuscation paths, offer an emerging but underutilized source of insight into offender sophistication and financial decision-making.

Law enforcement investigations increasingly highlight sextortion as an organized rather than purely interpersonal crime problem. In November 2023, the indictment of Olamide Oladosu Shanu and affiliated West African actors illustrated the scale of contemporary sextortion networks. Using coordinated social engineering, scripted victim engagement strategies, and layered cryptocurrency cash-outs, the group generated approximately 2.5 million dollars in Bitcoin from victims across multiple countries [6]. This case demonstrated that sextortion could operate within structured criminal ecosystems that separate luring, threatening, and laundering functions across distributed actors, similar to patterns identified in transnational romance fraud and pig-butchering schemes.

Technological innovations have further expanded the threat surface. The increased availability of generative artificial intelligence has enabled offenders to fabricate sexually explicit deepfake imagery even when no real content exists, thereby dramatically enlarging the pool of potential victims and complicating the evidentiary landscape for both prosecution and prevention. In 2025, the United States enacted the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (the TAKE IT DOWN Act), establishing the first federal regulatory framework that criminalizes the non-consensual publication of intimate visual depictions, including digitally generated images of adults and minors, and requires covered platforms to remove such content quickly [7]. Although a significant policy milestone, the law does not fully address adult sextortion or financially motivated deepfake-based extortion, leaving substantial regulatory gaps.

The psychological consequences of sextortion can be devastating [8]. Victims frequently report escalating threats, repeated monetary demands, and severe emotional distress, and some cases have led to suicide. The death of seventeen-year-old Jordan DeMay in 2022, following repeated extortion threats from overseas offenders demanding additional Bitcoin payments, illustrates the acute psychological harms that can arise from this crime type [9].

Despite the urgency of the problem, empirical criminological research integrating narrative analysis with blockchain forensics remains limited. Existing studies primarily focus on descriptive victimization patterns, psychological impacts, or case-based law enforcement narratives. Very little work has systematically examined the financial infrastructure of sextortion at scale or explored how laundering patterns reflect underlying offender sophistication and shape the severity of victimization [10,11]. Moreover, although blockchain analysis has proven essential in studying ransomware, darknet markets, and large-scale investment fraud, comparable analytic frameworks have not been widely applied to sextortion.

The present study advances this emerging research agenda through a two-phase analytical design that combines thematic examination of victim narratives with blockchain-based forensic analysis of cryptocurrency transactions. Using eighty-seven validated sextortion cases collected from Chain abuse between January and December 2024, the study provides new empirical evidence on two critical dimensions of contemporary sextortion.

First, the thematic analysis demonstrates that sextortion narratives are overwhelmingly standardized, multilingual, and template-driven, with more than ninety percent of

cases relying on identical scripted threats that reference fabricated recordings and imminent exposure. Only a very small subset of cases involves interactive grooming or live manipulation, suggesting a global model of industrialized extortion that prioritizes speed, automation, and scale.

Second, the regression analysis reveals that distinct laundering ecosystems correspond to differing levels of monetary loss. Higher-loss cases are marked by peel-chain sequences and withdrawals through regulated exchanges, reflecting more organized and sophisticated laundering infrastructures. Lower-loss cases, in contrast, display the reliance on basic mixers and offshore exchanges that are characteristics of high-volume, low-skill operations.

By integrating narrative patterns with transactional evidence, this study provides a comprehensive forensic framework for identifying high-risk sextortion typologies. These insights offer critical implications for law enforcement triage, policy development, blockchain analytics, and public safety interventions. They also highlight the need for comparative research across other interpersonal crypto-enabled crime types, including romance scams, pig-butchering schemes, and hybrid sextortion models, to more fully understand offender modus operandi and enhance early detection strategies.

2. Related Work

Over the past decade, sextortion has evolved from relatively isolated cases of interpersonal coercion into a scalable, industrialized form of cyber-enabled blackmail. Offenders now routinely exploit mainstream and niche social media and dating platforms, including Instagram, Snapchat, Wizz, Tinder, Bumble, and region-specific services such as Momo and TanTan, to create or hijack deceptive profiles, cultivate rapport, and solicit explicit content from victims [12–15]. The absence of robust identity verification on many of these platforms allows offenders to recycle stock images or deploy AI-generated personas that are difficult for users to distinguish from genuine profiles [16]. Recent advances in generative AI have further expanded this toolkit by enabling the fabrication of highly realistic synthetic intimate images and "face swaps", which can be used both to groom victims and to create convincing threats even when no authentic material exists [17,18].

Once initial contact is established through social media or dating services, communications frequently migrate to encrypted messaging applications such as WhatsApp, Telegram, Facebook Messenger, and Instagram Direct. These channels provide end-to-end encryption, low barriers to account creation, and access to underground markets for compromised or pre-verified accounts [19]. Through extended interaction, offenders construct emotionally charged narratives, simulate intimacy or crisis, and strategically escalate requests for sexual content or money [20]. Empirical studies consistently show that scammers rely on psychological leverage, including threats, shame, and false claims of technical compromise, to accelerate compliance and discourage disclosure to trusted others [12–14,21].

An equally important branch of the sextortion ecosystem, however, does not involve any prior relationship or grooming. Recent data from the FBI Internet Crime Complaint Center indicate that a substantial proportion of contemporary sextortion complaints originate from unsolicited email campaigns rather than from social media or dating-app interactions [22]. Large-scale measurement studies confirm the prominence of spam-based sextortion. Paquet-Clouston et al. [23] analyzed hundreds of millions of inbound emails and identified persistent sextortion spam that leveraged leaked password databases, recycled "I hacked your webcam" scripts, and cryptocurrency payment demands to induce rapid payment. Follow-up analyses by Microsoft Threat Intelligence [24] and Hernández-Castro and Boiten [11] show that these email campaigns are highly automated, multilingual, and globally distributed, often relying on botnets and automated translation tools to deliver nearly identical blackmail messages in many languages. In these cases, there is no attempt

to build trust; offenders bypass grooming entirely and instead rely on the shock value of apparent technical compromise and the fear of reputation damage.

Across both groomed and spam-initiated sextortion, offenders ultimately weaponize real or fabricated intimate material through escalating threats of disclosure to family members, employers, or social networks. This dynamic creates cycles of psychological coercion and repeated financial extortion where initial payment often leads to further demands [12,25]. The coexistence of personalized, relationship-based sextortion and mass email blackmail underscores the operational diversity of offender strategies and highlights the need for analytical frameworks that can distinguish between highly standardized extortion scripts and more targeted, socially engineered schemes.

Bitcoin is the dominant currency in sextortion due to its accessibility, pseudonymity, and global liquidity [26]. Threat-intelligence reports and official complaint data converge on this point: many sextortion payment instructions specify a Bitcoin address, even when multiple cryptocurrencies are available, because victims are more likely to recognize and comply with Bitcoin requests [22,25]. According to the Federal Trade Commission [27], cryptocurrency accounted for more than one third of all reported sextortion payments in 2022, surpassing traditional bank transfers and gift cards, and median reported losses exceeded ten thousand dollars.

To obscure the origin and destination of extorted funds, offenders employ a range of laundering techniques. Mixers and tumblers commingle deposits from many users and return randomized withdrawals, while decentralized protocols such as Tornado Cash use advanced cryptographic methods to further anonymize flows [28,29]. Peel-chain transfers repeatedly disperse value across long sequences of disposable wallets, fragmenting large holdings into small increments that are harder to track. Decentralized and centralized exchanges enable rapid cross-asset swapping and cross-chain movement, weakening the forensic signal available to investigators [30]. These techniques collectively complicate attribution and frequently move funds into or out of exchanges that operate outside the jurisdiction of the investigating authority.

Despite these challenges, forensic research on blockchain analytics has demonstrated that cryptocurrency transactions are not inherently untraceable. Graph-based clustering heuristics, transaction-pattern analysis, and subgraph representation learning can identify characteristic laundering structures, including mixer entry and peel-chain signatures, even within noisy or partially obfuscated networks [31]. Commercial blockchain-analysis platforms and academic models have shown promise in detecting coordinated illicit flows in ransomware, darknet-market, and investment-fraud contexts [4,31]. However, most of this work has focused on high-value enterprise crimes, and there remains a notable gap with respect to sextortion, which often involves comparatively small individual payments but very high aggregate volumes. Sextortion transfers are frequently structured as small-value payments that fall below standard anti-money-laundering thresholds, which makes them less likely to trigger automated alerts despite generating substantial profits when aggregated across large victim pools [32].

The convergence of unsolicited email outreach, coercive threat scripts, synthetic media, encrypted communication, and decentralized financial infrastructures has transformed sextortion into a highly resilient and adaptive global crime problem. Offenders can combine low-skill mass-distribution campaigns with widely available crypto-laundering tools to operate with limited risk of immediate disruption. This evolution highlights the need for research that integrates narrative analysis with blockchain-based financial investigation to illuminate the operational structures and laundering typologies that distinguish low-value, high-volume campaigns from more organized, higher-yield schemes.

The present study addresses this gap by systematically mapping cryptocurrency flows in confirmed sextortion cases and integrating these financial traces with qualitative patterns derived from victim narratives. By identifying characteristic laundering typologies, such as peel-chain activity and exchange-specific exit routes, and linking them to victim monetary loss, the study provides an analytical framework to support early detection and investigative triage.

3. Methods

3.1. Data Collection and Case Verification

Between 1 January 2024 and 28 December 2024, user-submitted reports related to online sextortion scams were collected from Chainabuse.com, a public reporting platform that allows individuals, organizations, and investigators to submit information about suspected cryptocurrency-related fraud. Reports typically include narrative descriptions of incidents and, when available, cryptocurrency wallet addresses provided by perpetrators for ransom payments.

To align with the study's focus on financially consequential sextortion, cases were excluded if victims did not report monetary loss or if submissions lacked sufficient usable information (e.g., missing wallet addresses or unclear incident descriptions). Because reporting on the platform is voluntary and user-driven, the dataset may be influenced by self-selection, potentially overrepresenting victims who are aware of the platform, motivated to report, or able to identify cryptocurrency payment details. In addition, some high-profile cases under active law-enforcement investigation were restricted or greyed out on the platform and therefore were not retrievable for analysis. Although the platform is considered a reliable source for cryptocurrency-related abuse reporting, it also includes complaints filed after sextortion attempts that did not result in payment; accordingly, the final dataset reflects filtered cases meeting the study criteria and does not represent the full population of sextortion incidents.

Each remaining case underwent a multi-stage open-source intelligence (OSINT) verification process. Wallet addresses were first validated using BitcoinWhosWho.com for fraud-risk identification, the OFAC Sanctions List for sanctions screening, OKX's address verification tool for structural validation, and blockchain explorers such as Blockchain.com and Blockchair.com to retrieve detailed incoming and outgoing transaction histories. To support reproducible behavioral analysis, Breadcrumbs.io was used to examine transaction-flow patterns and identify indicators of money-laundering activity. Within Breadcrumbs, coin mixer exposure was identified through transaction paths interacting with known mixing services or wallets labeled as mixers, as well as characteristic patterns such as pooled inputs, rapid redistribution, and obfuscated fund paths. Peel-chain behavior (chain stripping) was identified through repeated sequential transactions in which funds were split into smaller amounts and forwarded across multiple newly generated addresses, typically retaining one portion while transferring the remainder onward to form a linear chain. Indicators included high-frequency sequential transfers, consistent incremental segmentation, and rapid multi-hop propagation across fresh addresses.

Together, these tools enabled confirmation of deposits, exchange interactions, swaps, mixer exposure, and peel-chain activity while providing transparent visualization of transaction flows to support analytic consistency and reproducibility. After verification, the dataset was further refined to include only reports confirmed as genuine sextortion incidents involving observable cryptocurrency transactions. Cases in which reported monetary losses did not correspond with verifiable blockchain activity, or showed substantial inconsistencies between self-reported losses and transaction histories, were excluded to preserve analytical reliability.

The final dataset comprised 87 fully validated sextortion cases included in the qualitative content analysis. Of these, 76 cases contained usable and independently verified USD loss values and were therefore retained for quantitative modeling. Regression analyses employed listwise deletion, excluding cases with missing or unverifiable monetary loss data; consequently, only cases with complete transaction histories, verifiable losses, and traceable laundering indicators were included in the final quantitative analysis.

3.2. Analytical Framework

Two analytic phases were conducted to examine the structure and financial dynamics of sextortion cases in the dataset.

Phase 1 consisted of a qualitative thematic analysis of victims' narrative descriptions to identify recurring patterns in scam scripts, threat strategies, and forms of psychological coercion. An initial coding framework was developed through iterative review of a subset of reports, combining inductive identification of emerging themes with refinement based on prior research on online fraud and sextortion. The coding scheme was then applied systematically across the dataset, with multiple reviewers independently coding the narratives and resolving discrepancies through discussion to ensure consistency and reliability. This process enabled the distinction between mass-produced, multilingual extortion scripts and more targeted or technically elaborate sextortion attempts.

Phase 2 consisted of a quantitative assessment in which a multiple linear regression model was estimated to test whether specific laundering techniques and exchange pathways predicted the amount of monetary loss sustained by victims. Identification of money laundering (ML) activity was derived from blockchain investigation methods applied to victims' cryptocurrency wallet addresses, using transaction traces to categorize behaviors such as mixer use, peel-chain activity, swap transactions, self-funding behaviors, and inflows or outflows routed through major exchanges. All quantitative analyses were conducted using SPSS Version 29.0, and diagnostic testing confirmed that regression assumptions were met, including the absence of multicollinearity, normally distributed residuals, and acceptable homoscedasticity.

4. Results

4.1. Phase 1: Thematic Patterns in Sextortion Narratives

Qualitative analysis of the 87 validated reports identified five primary sextortion script types and one cross-cutting narrative element (victim counterinterpretations). As shown in Table 1, Mass-Produced Sextortion Scripts were the predominant category (92%, $n = 80$). These messages followed a highly uniform format in which offenders claimed to possess explicit recordings and threatened exposure unless payment was paid in Bitcoin. Although minor language or formatting differences were present, the scripts consistently relied on fabricated claims, most notably the "dual-screen recording" assertion, and emphasized reputational harm to induce urgency. Messages appeared in multiple languages (e.g., Japanese, Spanish, Dutch, German, Romanian, French), reflecting the automated, globally scaled nature of these campaigns.

Less frequent categories reflected more personalized or technically framed intimidation strategies. Malware and access claims were observed in 4.6% of cases ($n = 4$), where offenders alleged Remote Access Trojans (RATs), webcam compromise, or full system control to enhance perceived credibility. Device and contact list access threats accounted for 1.1% of cases ($n = 1$) relying on claims of accessing personal files, contacts, or social media accounts to intensify coercion. Three additional categories each occurred in 1.1% of cases ($n = 1$): targeted interactive sextortion, involving real-time video interactions often initiated through dating platforms; and elaborated narrative-based extortion mes-

sages, characterized by extended and technically styled explanations paired with specific ransom demands.

Table 1. Thematic classification of sextortion event descriptions (N = 87).

Theme	Definition	Representative Excerpts	*n*	%
1. Mass-Produced Sextortion Scripts	Highly standardized messages claiming possession of sexual recordings and demanding Bitcoin payment; includes all multilingual variants.	"I recorded you and will send the video to all your contacts unless you pay."	80	92.0%
2. Malware and Access Claims	Offenders assert installation of trojans, RATs, webcam access, or total device control; typically used to increase credibility.	"I installed a trojan on your device and recorded you."	4	4.6%
3. Device and Contact List Access Threats	Messages threaten to expose explicit content using alleged access to contacts, files, or social media credentials.	"I have your entire contact list and will share your videos."	1	1.1%
4. Targeted Interactive Sextortion	Offenders elicit sexual content during real-time video calls and later use the recordings for extortion.	"We video chatted, and then she threatened to expose the recording."	1	1.1%
5. Elaborated Narrative-Based Extortion Messages	Extended narratives with technical-sounding explanations or specific ransom amounts intended to enhance plausibility.	"My malware updated itself every 4 h; send $1620 in Bitcoin."	1	1.1%
6. Victim Counterinterpretations	Statements in which victims express skepticism or awareness that the extortion attempt was fraudulent.	"This is clearly a scam; I don't even own a webcam."	Not counted as standalone cases	—

This distribution indicates that contemporary sextortion is driven primarily by standardized, automated communication templates rather than individualized social-engineering approaches. Personalized or technically elaborate strategies including malware claims, contact-list threats, interactive video-based sextortion, and extended narrative messaging were rare, suggesting that most offenders prioritize scalable messaging designed to maximize reach and efficiency. Nevertheless, the small number of interactive or narrative-intensive incidents indicates that a subset of offenders employ more personalized tactics that may reflect higher operational sophistication or alternative recruitment channels.

Victim counterinterpretations, although not counted as a standalone category, appeared across multiple narratives and revealed variation in victim awareness and digital literacy. These statements suggest that recognition of fraudulent tactics may shape threat appraisal and potentially influence compliance behavior and financial outcomes.

Overall, Phase 1 results indicate that contemporary sextortion campaigns are highly formulaic and multilingual, relying predominantly on urgency, fear, and reputational threat rather than verifiable technical compromise. The consistency of these patterns suggests the presence of a mature, globally coordinated ecosystem in which Bitcoin serves as the primary mechanism for monetization.

4.2. Phase 2: Descriptive Statistics of Monetary Loss and Laundering Indicators

Table 2 summarizes monetary loss, cryptocurrency use, and blockchain-derived laundering indicators across the 87 verified cases. Of these, 76 cases (87.4%) contained usable and independently verified USD loss values. Among cases with valid loss data, the mean loss was USD 1086.03 (SD = USD 372.44), with payments ranging from USD 500 to USD 2000. The grouped median was USD 1144.50, indicating a relatively constrained payment band.

Table 2. Descriptive statistics for monetary loss and ML activity (N = 87).

Variables	Measures	Mean	S.D.	N (%)/Range
Monetary Loss				
USD Lost	Continuous	1086.03	372.44	76 valid (87.4%)
Range	—	—	—	500–2000
Median	—	1144.50	—	—
Crypto Type				
Bitcoin	Percentage	1.00	0	87 (100%)
Identification of ML Activities				
BitcoinWhosWho Scam Alert	Dichotomous	0.78	0.42	68 Yes (78.2%) No (21.8%)
Mixer	Dichotomous	0.91	0.29	79 Yes (90.8%) No (9.2%)
Peel Chain	Dichotomous	0.21	0.41	18 Yes (20.7%) No (79.3%)
Bybit Incoming	Dichotomous	0.06	0.23	5 Yes (5.7%) No (94.3%)
Kraken Outgoing	Dichotomous	0.23	0.42	20 Yes (23.0%) No (77.0%)
MEXC Outgoing	Dichotomous	0.20	0.40	17 Yes (19.5%) No (80.5%)

Bitcoin was used in 100% of cases, indicating exclusive reliance on this cryptocurrency for extortion payments. Laundering-related behaviors were highly prevalent. A total of 78.2% of wallet addresses were flagged as fraudulent on BitcoinWhosWho, and mixer exposure appeared in 90.8% of cases, indicating widespread reliance on readily available anonymization tools and the repeated reuse of known scam infrastructure within high-volume campaigns.

More structured financial routing behaviors appeared less frequently but remain analytically important. Peel chain activity occurred in 20.7% of cases, while exchange-linked transfers included Kraken outgoing flows in 23%, MEXC outgoing flows in 19.5%, and Bybit incoming flows in 5.7%.

4.3. Regression Analysis Predicting Monetary Loss

Table 3 presents the regression findings. A multiple linear regression was conducted to examine whether specific blockchain-based laundering behaviors predicted the amount of monetary loss reported by victims. The model included six binary indicators: (1) BitcoinWhosWho scam alert, (2) Mixer use, (3) Peel-chain activity, (4) Bybit incoming transfers, (5) Kraken outgoing transfers, and (6) MEXC outgoing transfers. Preliminary analyses confirmed that the dependent variable, USD monetary loss, demonstrated acceptable normality (skew = 0.217; kurtosis = −0.839), and visual inspection of histograms and residual plots showed no violations of linear regression assumptions. In addition, multicollinearity was not detected (VIFs = 1.04–1.10).

Table 3. Regression predicting victims' monetary loss (USD).

Predictors	B	SE	β	*p*
BitcoinWhosWho	−163.45	88.48	−0.18	0.069
Mixer	−382.69	159.33	−0.23	0.019 *
Peel Chain	278.20	83.82	0.31	0.001 **
Bybit Incoming	277.07	145.03	0.19	0.060
Kraken Outgoing	247.40	85.59	0.28	0.005 **
MEXC Outgoing	−222.46	84.07	−0.25	0.010 *
R^2	0.41			
Adjusted R^2	0.36			

* $p < 0.05$; ** $p < 0.01$.

The overall model was statistically significant, $F(6, 69) = 8.05$, $p < 0.001$, and explained 41.2% of the variance in monetary loss ($R^2 = 0.412$, Adjusted $R^2 = 0.360$). The Durbin–Watson statistic was 1.97, indicating no autocorrelation. Examination of VIF values (1.04–1.10) showed no evidence of multicollinearity. The standard error of the estimate was $297.84, indicating good model precision considering the observed loss range ($500–$2000).

Peel chain activity emerged as a positive and statistically significant predictor of increased loss, B = 278.20, $p = 0.001$. Outgoing cash out through Kraken was also a significant positive predictor, B = 247.40, $p = 0.005$. These findings indicate that structured sequential wallet dispersion and regulated exchange routing are associated with substantially higher financial victimization, suggesting more organized laundering pipelines and greater offender capacity.

In contrast, Mixer involvement was a significant negative predictor, B = −382.69, $p = 0.019$, as was MEXC outgoing transfers, B = −222.46, $p = 0.010$. These pathways were associated with lower reported losses, consistent with automated, high-volume sextortion operations that prioritize speed and anonymization over extracting higher individual payments. The comparatively lower losses linked to MEXC may reflect its frequent use in rapid, opportunistic routing or cash out stages within lower-tier scam infrastructures, whereas Kraken routing may indicate offenders capable of navigating stricter compliance environments and therefore positioned to extract larger payments.

Two variables showed directional but not conventionally significant effects. BitcoinWhosWho scam alerts were negatively associated with loss, B = −163.45, $p = 0.069$, while Bybit incoming transfers were positively associated with loss, B = 277.07, $p = 0.060$. Although these effects did not reach conventional significance thresholds, their directions are substantively informative. Scam-alerted wallets appear more common in lower-value, repetitive campaigns, whereas Bybit inflows may reflect intermediary roles in certain higher-tier laundering chains.

Residual diagnostics indicated normally distributed errors and stable model fit. The standardized residuals ranged from −2.44 to 2.16, remaining within acceptable bounds, and the standard error of the estimate remained $297.84.

Overall, the regression findings demonstrate that laundering behaviors function not only as concealment strategies but also as observable indicators of offender sophistication and expected financial harm. Structured routing patterns such as peel chain dispersion and regulated exchange cash out activity are linked to higher-severity victimization, whereas anonymization-heavy pathways are more closely associated with high-volume, lower-value sextortion activity.

4.4. Visualizing Monetary Loss Across Laundering Indicators

Figure 1 presents boxplots illustrating the distribution of victim monetary losses across the primary laundering indicators identified in the blockchain analysis. The figure enables

visual comparison of medians, interquartile ranges, and dispersion patterns, thereby complementing the descriptive statistics and regression findings. Notches in each box represent approximate 95% confidence intervals around the median, allowing visual comparison of central tendencies across groups.

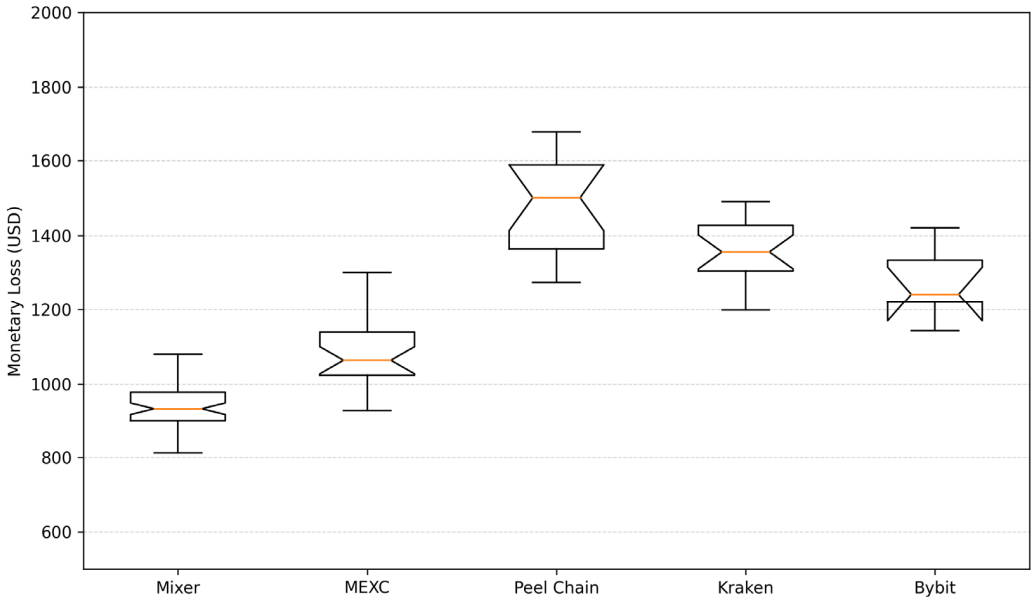

Figure 1. Boxplots of loss by Money-Laundering (ML) indicators.

Overall, losses range from USD 500 to USD 2000, with a mean of USD 1086.03 and a median of USD 1144.50. Within this bounded range, the boxplots reveal clear stratification in victim losses depending on the laundering pathway used after payment.

Peel chain cases occupy the highest position in the distribution. The median appears around the upper portion of the loss range, with most values concentrated between USD 1400 and USD 1600 and upper whiskers extending toward the highest observed payments. The relatively compact interquartile range indicates consistently high payments rather than isolated extremes. This visual pattern aligns with the regression results identifying peel chain activity as a significant positive predictor of loss (B = 278.20, $p = 0.001$), suggesting that sequential wallet dispersion is typically associated with structured laundering pipelines capable of extracting larger payments.

Kraken outgoing transfers also correspond to elevated losses. The median is slightly below peel chain but still well above the overall midpoint, with most observations clustered between USD 1300 and USD 1500 and upper values approaching USD 1600. The moderate spread indicates consistently higher losses across cases. This visual pattern reinforces the regression finding that Kraken routing significantly predicts higher victim loss (B = 247.40, $p = 0.005$), suggesting that routing funds through a regulated, high-liquidity exchange may reflect offenders with stronger operational infrastructure or greater ability to process higher-value transactions.

Bybit incoming flows appear within the higher-loss group but with somewhat greater variability. The median sits above the dataset midpoint, approximately around the USD 1300 range, while the interquartile span extends broadly from about USD 1200 to USD 1400, with whiskers reaching toward higher values. This wider dispersion suggests a mixture of moderate and higher payment levels. The visual pattern is consistent with the smaller number of Bybit cases and with the regression coefficient showing a positive but not statistically significant association with loss (B = 277.07, $p = 0.060$). This distribution

may indicate that Bybit sometimes functions as an intermediary step within more complex laundering chains, though additional data would be required to confirm this interpretation.

In contrast, mixer-related cases cluster clearly toward the lower end of the loss distribution. The median indicates below USD 1000, with most values concentrated roughly between USD 900 and USD 1000, with whiskers extending toward lower payments. The relatively narrow interquartile range indicates consistent lower payment amounts across cases. Given the high prevalence of mixer exposure, this pattern suggests widespread use of anonymization tools in automated, high-volume sextortion campaigns that rely on standardized payment demands rather than individualized extraction. This interpretation is supported by the regression result identifying mixer involvement as a significant negative predictor of loss (B = −382.69, $p = 0.019$).

MEXC outgoing transfers also show comparatively lower losses, though generally slightly higher than mixer cases and with somewhat broader dispersion. The median indicates around the USD 1050 range, with the interquartile span extending from USD 950 to USD 1150 and upper values reaching toward USD 1250. This distribution places MEXC between the lowest-loss mixer cases and the higher-loss exchange pathways. The regression confirms a significant negative association with loss (B = −222.46, $p = 0.010$), suggesting that MEXC may be used more frequently in rapid routing or opportunistic cash-out stages within lower-tier scam infrastructures rather than in highly organized laundering pipelines.

Taken together, Figure 1 demonstrates a clear visual bifurcation between higher-loss and lower-loss laundering patterns. Peel chain dispersion and Kraken routing consistently align with the higher-loss segment, while mixer exposure and MEXC routing cluster within the lower-loss range. Bybit occupies an intermediate but generally higher-loss position with greater variability. This visual stratification closely mirrors the statistical relationships observed in the regression model, which explains 41.2% of the variance in victim losses. The convergence of visual, descriptive, and inferential evidence strengthens the interpretation that laundering pathways function not only as concealment mechanisms but also as observable indicators of offender organization and expected financial harm.

The findings across qualitative and quantitative analyses reveal a consistent pattern in contemporary cryptocurrency sextortion. Narrative evidence shows that the offense is dominated by highly standardized, multilingual scripts designed for scalable distribution, while blockchain analysis indicates similarly structured financial workflows characterized by widespread anonymization practices and selective use of more organized routing pathways. Victim payments fall within a relatively constrained range, and statistical modeling demonstrates that specific laundering indicators are systematically associated with differences in financial loss. The convergence of thematic, descriptive, regression, and visual results indicates that both communication strategies and post-payment transaction patterns correspond to distinct operational approaches within cryptocurrency sextortion activity.

5. Discussion

This study examined sextortion victimization through a dual-phase approach combining qualitative analysis of extortion narratives with quantitative modeling of blockchain-based laundering behaviors. Together, these findings illuminate how psychological coercion, scripted communication, and financial obfuscation jointly shape the severity of financial harm.

The thematic analysis showed that most sextortion attempts employed highly standardized, mass-produced scripts. Offenders disseminated multilingual threats asserting possession of explicit recordings and the intention to share them with the victim's contacts unless payment was made in Bitcoin. These messages appeared in languages including Japanese, Spanish, Dutch, German, Romanian, and French, suggesting the presence of

automated translation tools and bulk distribution infrastructure. Although some scripts referenced malware, trojan installation, or webcam compromise, these claims were primarily psychological tactics rather than evidence of genuine technical intrusion. Only a very small number of cases deviated from this pattern, including instances involving interactive video calls in which perpetrators captured sexual content during real-time communication. Such cases illustrate a more individualized social-engineering modus operandi but were exceedingly rare. Overall, narrative patterns point to the industrialization of sextortion, where scale and automation, rather than personalization, dominate offender strategy.

Importantly, victim counterinterpretations observed in several narratives revealed variation in victim awareness and digital literacy. Expressions of skepticism, recognition of common scam tactics, or dismissal of technical threats suggest that some victims can identify fraudulent messaging patterns before compliance. Although these responses were not treated as a standalone thematic category, they provide insight into defensive cognition and highlight the potential protective role of public awareness and digital literacy in reducing victimization risk.

Despite the narrative uniformity identified in Phase 1, the results from Phase 2 show substantial variation in the financial impact experienced by victims based on the laundering pathways employed by offenders. This indicates that financial behaviors offer important insight into offender capability and organizational structure beyond what can be inferred from narrative content alone.

Higher monetary losses were significantly associated with peel chain activity and Kraken outgoing transactions. Peel chain sequences, characterized by systematic micro-transfers across numerous wallets, are well established in organized laundering associated with ransomware, coordinated fraud, and darknet marketplaces [33]. Their strong association with higher losses suggests that offenders using complex laundering pipelines may be part of more organized or well-resourced criminal groups [1].

Kraken, a regulated and high-liquidity exchange, also appeared frequently in higher-loss cases. This pattern implies the involvement of offenders capable of navigating identity verification systems or exploiting preexisting or fraudulent accounts, further indicating higher organizational capacity [1].

Lower monetary losses were instead associated with mixer usage and MEXC outgoing transfers. These behaviors are typical of high-volume, low-sophistication sextortion activity in which offenders prioritize speed and anonymity. Addresses flagged on BitcoinWhosWho were likewise associated with lower losses, indicating that wallets previously identified as scam-related are more commonly reused in repetitive, low-value extortion campaigns rather than in high-yield, targeted operations. This pattern is consistent with prior research showing that large-scale fraud operations often rely on readily disposable infrastructure rather than prolonged account longevity [1,33].

Bybit incoming transactions showed a positive but marginal association with monetary loss, raising the possibility that this exchange serves as an intermediary transfer point within some mid- to high-value laundering infrastructures. This relationship requires further study with larger samples.

Taken together, the qualitative and quantitative findings illustrate that sextortion operations exist within a dual-tier ecosystem. Most offenders rely on identical threat scripts, yet their laundering behaviors reveal substantial differences in criminal sophistication. Lower-loss cases align with high-volume, minimalistic laundering consistent with mass scam operations. Higher-loss cases, although less frequent, involve controlled multi-step laundering chains and regulated exchange cash-outs, patterns more consistent with coordinated or transnational crime groups. This divergence underscores the value of combining narrative analysis with blockchain forensic techniques to identify high-risk offenders.

The findings have several implications for cybercrime prevention and investigative strategy. First, laundering typologies can serve as actionable intelligence signals. Peel chain activity and regulated exchange outflows should be flagged as priority indicators of higher-value and more organized criminal operations [1,33]. Second, the dominance of mass-produced sextortion scripts highlights the need for improved global spam filtering systems, enhanced email authentication protocols, and large-scale public awareness initiatives [11,22,34,35]. Third, blockchain analytics improves investigative triage by enabling analysts to differentiate between high-frequency mass scams and targeted high-yield operations, allowing more efficient allocation of law enforcement resources [36,37]. Finally, coordinated responses across cryptocurrency exchanges are essential. Platforms such as Kraken, Bybit, and MEXC each play distinct roles within laundering pipelines, and stronger Know Your Customer (KYC) and Anti-Money Laundering (AML) controls, including enhanced transaction monitoring and real-time information sharing, could significantly disrupt offender operations and reduce the scalability of sextortion-related financial flows [1].

This study has several limitations. The sample size (N = 87) is modest, and some subcategories are very small. For example, targeted interactive sextortion appeared only once (n = 1, 1.1%), which likely reflects underreporting rather than true prevalence. Such limited representation constrains the depth of interpretation for certain patterns; accordingly, the findings should be viewed as exploratory rather than population-level conclusions. In addition, because the data derive from voluntary reports on a public cryptocurrency abuse platform, the sample may reflect reporting bias and may not capture all sextortion incidents, particularly those that go unreported or do not involve cryptocurrency payments.

Despite these limitations, the study's two-phase design demonstrates the value of integrating qualitative narrative evidence with blockchain transactional analysis to classify offender sophistication and assess financial harm. This framework links victim accounts with measurable financial flows, offering practical value for investigative triage and threat assessment.

Future research should extend this framework using larger, multi-platform datasets to enhance comparative validity. In particular, systematic comparison between sextortion, romance scams, and pig-butchering schemes would build directly on prior findings from research on cryptocurrency-enabled romance scams, which identified structured narrative stages of trust manipulation and distinct laundering pathways [38].

Preliminary contrasts suggest meaningful differences in modus operandi. Sextortion typically involves compressed timelines, immediate coercion following explicit digital interaction, and urgent ransom framing. In contrast, romance scams and pig-butchering schemes involve prolonged trust-building cycles, gradual emotional dependency, and payment requests framed as investment opportunities rather than explicit threats. From a blockchain perspective, sextortion payments often involve single-incident ransom transfers followed by peel-chain or mixer exposure, whereas romance scams and pig-butchering schemes more frequently demonstrate staged fund consolidation, cross-chain swaps, wallet clustering, and exchange cash-out patterns, consistent with prior blockchain analyses of romance scam victimization.

Comparative analysis of narrative strategies, trust-building cycles, payment urgency framing, and laundering architectures may help identify crime-specific behavioral signatures and early-warning indicators. Expanding to multi-chain blockchain analytics and integrating offender-centric intelligence would further strengthen predictive modeling and investigative applications across cryptocurrency-driven victimization models.

6. Conclusions

This study demonstrates that sextortion is not a monolithic or uniformly low-skill cybercrime but an ecosystem comprising both highly standardized extortion scripts and diverse, structurally differentiated laundering pipelines. While the vast majority of offenders employ nearly identical, multilingual threat templates, the blockchain analysis reveals substantial heterogeneity in offender sophistication. Low-loss cases align with high-volume, minimally organized operations that rely on basic mixers, offshore exchanges, and previously flagged scam wallets. In contrast, higher-loss cases are characterized by peel-chain sequences, regulated exchange cash-outs, and intermediary flows such as those observed through Kraken and Bybit, indicating more coordinated and technically capable actors.

By integrating thematic analysis of extortion narratives with blockchain-based forensic tracing, this study provides the first empirical framework that links narrative patterns to specific laundering typologies in sextortion. These findings underscore the value of financial behavioral indicators such as mixer-entry signatures, peel-chain velocities, and exchange specific pathways for distinguishing opportunistic offenders from more organized criminal groups. This dual-perspective approach enhances threat classification, improves investigative triage, and supports the development of targeted interventions.

The findings also highlight the critical importance of public awareness and prevention efforts. Because most sextortion campaigns rely on standardized psychological pressure rather than verified technical compromise, increasing public understanding of common scam scripts, false malware claims, and cryptocurrency payment demands may significantly reduce victim compliance and financial loss. Educational outreach, digital literacy initiatives, and rapid reporting mechanisms can therefore function as frontline defenses, complementing technical enforcement and financial monitoring strategies.

Policy and investigative efforts should prioritize cross-platform coordination among email providers, social media platforms, blockchain-analysis firms, and cryptocurrency exchanges, as offenders increasingly exploit multiple digital ecosystems. Strengthened KYC and AML controls, real-time suspicious transaction reporting, and improved spam filtering and authentication mechanisms can help reduce both high-volume and high-impact sextortion threats [38].

Finally, the analytic framework developed here establishes a foundation for comparative research across other crypto-enabled interpersonal crimes, including romance fraud, pig-butchering schemes, and hybrid extortion models. These crime types differ in their narrative strategies but often converge on overlapping laundering infrastructures. Future work should expand cross-chain analyses, incorporate larger datasets, and integrate offender-centric intelligence to refine early detection tools and support more effective disruption of emerging financial-exploitation networks.

Author Contributions: Conceptualization, K.-S.C., M.C. and S.B.; methodology, K.-S.C., M.C. and S.B.; software, K.-S.C., M.C. and S.B.; validation, K.-S.C., M.C. and S.B.; formal analysis K.-S.C., M.C. and S.B.; investigation K.-S.C., M.C. and S.B.; resources, K.-S.C., M.C. and S.B.; data curation, K.-S.C., M.C. and S.B.; writing—original draft preparation, K.-S.C., M.C. and S.B.; writing—review and editing, K.-S.C., M.C. and S.B.; visualization, K.-S.C., M.C. and S.B.; supervision, K.-S.C., M.C. and S.B.; project administration, K.-S.C., M.C. and S.B.; funding acquisition, K.-S.C., M.C. and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Naif Arab University for Security Sciences under Grant No. NAUSS-25-R15.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2023*; Publications Office of the European Union: Luxembourg, 2023. Available online: https://www.europol.europa.eu (accessed on 1 May 2025).
2. National Center for Missing & Exploited Children. *CyberTipline 2023 Data Report*; NCMEC: Alexandria, VA, USA, 2024. Available online: https://www.missingkids.org/gethelpnow/cybertipline (accessed on 1 May 2025).
3. Federal Bureau of Investigation (FBI). Sextortion: A Growing Threat Preying Upon Our Nation's Teens. Available online: https://www.fbi.gov (accessed on 20 March 2025).
4. Chainalysis. *Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth*; Chainalysis Inc.: New York, NY, USA, 2024. Available online: https://www.chainalysis.com (accessed on 21 March 2025).
5. Elliptic. *Typologies Report 2024: Preventing Financial Crime in Cryptoassets—Identifying Evolving Criminal Behavior*; Elliptic Enterprises: London, UK, 2024. Available online: https://www.elliptic.co (accessed on 20 March 2025).
6. United States District Court, District of Idaho. United States v. Olamide Oladosu Shanu, Case No. 1:23-cr-00203. 2023. Available online: https://www.pacermonitor.com/public/case/51399976/USA_v_Shanu (accessed on 27 February 2025).
7. TAKE IT DOWN act, S.146, 119th cong. Available online: https://www.congress.gov/bill/119th-congress/senate-bill/146 (accessed on 20 March 2025).
8. Walsh, W.A.; Tener, D. If you don't send me five other pictures I am going to post the photo online: A qualitative analysis of experiences of survivors of sextortion. *J. Child Sex. Abus.* **2022**, *31*, 447–465. [CrossRef] [PubMed]
9. United States Department of Justice. *Ogoshi Brothers Sentenced to Lengthy Prison Terms in Sextortion Scheme that Resulted in Death of Teen*; United States Department of Justice: Washington, DC, USA, 2024.
10. Regina, O.; Ramli, K.; Amarullah, A.H. Illicit Cryotocurrency Investigation Digital Forensic Framework: Integrating Off-chain and On-Chain Analysis for Two Types of Crime. *Int. J. Electr. Comput. Biomed. Eng.* **2025**, *3*, 411–432. [CrossRef]
11. Edwards, M.; Hollely, N.M. Online sextortion: Characteristics of offences from a decade of community reporting. *J. Econ. Criminol.* **2023**, *2*, 100038. [CrossRef]
12. Pethers, B.; Bello, A. Role of attention and design cues for influencing cyber-sextortion using social engineering and phishing attacks. *Future Internet* **2023**, *15*, 29. [CrossRef]
13. O'Malley, R.L.; Grosholz, J.M.; Ozuni, A. What predicts law enforcement reporting among male sextortion victims? *Crim. Justice Behav.* **2025**, *53*, 252–286. [CrossRef]
14. O'Malley, R. Short-term and long-term impacts of financial sextortion on victim's mental well-being. *J. Interpers. Violence* **2023**, *38*, 8563–8592. [CrossRef] [PubMed]
15. Tavakoli, H.; Tzani, C.; Ioannou, M.; Williams, T.J.V.; Drouin, M.; Fletcher, R. Dating applications: A honeypot for sextortion victims. *Deviant Behav.* **2024**, *45*, 1655–1666. [CrossRef]
16. Atanesyan, A.V.; Mkhitaryan, S.; Karapetyan, A. "Virtual Masks" and Online Identity: The Use of Fake Profiles in Armenian Social Media Communication. *J. Media* **2025**, *6*, 49. [CrossRef]
17. Pedersen, K.T.; Pepke, L.; Stærmose, T.; Papaioannou, M.; Choudhary, G.; Dragoni, N. Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments. *J. Cybersecur. Priv.* **2025**, *5*, 18. [CrossRef]
18. Babaei, R.; Cheng, S.; Duan, R.; Zhao, S. Generative artificial intelligence and the evolving challenge of deepfake detection: A systematic analysis. *J. Sens. Actuator Netw.* **2025**, *14*, 17. [CrossRef]
19. Bogos, S.; Balduzzi, M.; Ciancaglini, V.; Balzarotti, D. Dissecting encrypted messaging platforms: Crime ecosystems and underground social engineering. *Comput. Secur.* **2023**, *125*, 103049. [CrossRef]
20. Cross, C.; Holt, K.; Holt, T.J. To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. *Criminol. Crim. Justice* **2025**, *25*, 777–792. [CrossRef]
21. Whitty, M.T.; Buchanan, T. The online romance scam: A serious cybercrime. *CyberPsychol. Behav. Soc. Netw.* **2012**, *15*, 181–183. [CrossRef] [PubMed]
22. Federal Bureau of Investigation Internet Crime Complaint Center (IC3). *2024 Internet Crime Report*; FBI: Washington, DC, USA, 2024.
23. Paquet-Clouston, M.; Romiti, M.; Hashlhofer, B.; Charvat, T. Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem. In Proceedings of the AFT '19: 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, 23 October 2019; pp. 76–88.

24. Microsoft Threat Intelligence. *Phorpiex Morphs: How a Longstanding Botnet Persists and Thrives in the Current Threat Environment*; Microsoft Security Blog: Redmond, WA, USA, 2021. Available online: https://www.microsoft.com/en-us/security/blog/2021/05/20/phorpiex-morphs-how-a-longstanding-botnet-persists-and-thrives-in-the-current-threat-environment/ (accessed on 1 August 2025).
25. Global Coalition to Fight Financial Crime. Trends in Sexual Extortion and Digital Coercion. 2024. Available online: https://www.gcffc.org/ (accessed on 1 August 2025).
26. Homeland Security Investigations (HSI). *Cryptocurrency: Illicit Finance Risk Assessment*; U.S. Department of Homeland Security: Washington, DC, USA, 2022. Available online: https://www.ice.gov/about-ice/hsi (accessed on 20 March 2025).
27. Federal Trade Commission (FTC). *Consumer Fraud 2023: Cryptocurrency Payment Trends*; U.S. Government Publishing Office: Washington, DC, USA, 2023. Available online: https://www.ftc.gov/ (accessed on 20 March 2025).
28. Leukfeldt, E.R.; Kruisbergen, E.W.; Kleemans, E.R.; Roks, R.A. Organized financial cybercrime: Criminal cooperation, logistic bottlenecks, and money flows. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 961–980.
29. Turner, A.; Irwin, A.S. Bitcoin transactions: A digital discovery of illicit activity on the blockchain. *J. Financ. Crime* **2018**, *25*, 109–130. [CrossRef]
30. Trozze, A.; Davies, T.; Kleinberg, B. Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering. *Forensic Sci. Int. Digit. Investig.* **2023**, *46*, 301575. [CrossRef]
31. Bellei, C.; Xu, M.; Phillips, R.; Robinson, T.; Weber, M.; Kaler, T.; Leiserson, C.E.; Arvind; Chen, J. The shape of money laundering: Subgraph representation learning on the blockchain with the Elliptic2 dataset. *arXiv* **2024**, arXiv:2404.19109. [CrossRef]
32. Jensen, R.I.; Ferwerda, J.; Wewer, C.R. Searching for smurfs: Testing if money launderers know alert thresholds. *J. Quant. Criminol.* **2025**, *46*, 1–14. [CrossRef]
33. Chainalysis. *Crypto Crime Report 2023*; Chainalysis Inc.: New York, NY, USA, 2023. Available online: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/ (accessed on 1 July 2025).
34. Choi, K.S.; Back, S.; Toro-Alvarez, M.M. *Digital Forensics and Cyber Investigation*; Cognella: San Diego, CA, USA, 2022.
35. Wang, F. Breaking the silence: Examining process of cyber sextortion and victims coping strategies. *Int. Rev. Vict.* **2025**, *31*, 91–116. [CrossRef]
36. Financial Action Task Force (FATF). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*; FATF: Paris, France, 2022.
37. Mohamed, H. Decentralized Crime: Fraud, Cybercrime and Legal Enforcement. *J. Econ. Leg. Stud.* **2025**, *2*, 5–22. [CrossRef]
38. Lim, A.; Choi, K.S. Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization. *Int. J. Cybersecur. Intell. Cybercrime* **2025**, *8*, 4–25. [CrossRef]