Clearing the crypto-laundering forest: a process-based view for cryptocurrency-based cyber-money laundering

Steven Meighan [1], Dionysios Demetis [2] and Gurpreet Dhillon [3]
[1, 2] University of Hull, [3] University of North Texas
s.meighan@hull.ac.uk

Abstract

This exploratory paper investigates the complex phenomenon of crypto-laundering through the lens of process theorising. Extensive data - discussing how to access darknets, obtain crypto-assets anonymously, and destroy any digital evidence linking online misbehaviour to real-world identities - was scraped from online forums using a simple Python script. This data was then analysed to describe a detailed process model that captures the eight main stages that criminals employ to preserve their online anonymity and obscure their illicit financial flows. The study highlights information security practices that are recommended within these criminal communities. The paper also examines and contrasts the on-chain blockchain data with off-chain digital and physical traces, which may facilitate law enforcement investigations. By mapping real-world friction points - where cyberspace meets the real world - the paper's findings offer investigation and policy development insights. The paper concludes with suggestions for further development to refine and validate the model developed, including expanded data collection, qualitative interviews, and case studies with law enforcement.

Introduction

The convergence of ransomware, crypto-assets, and crypto-laundering magnifies the risk to the financial system and defines the need for enhanced cybersecurity protocols and effective regulatory oversights. Introducing new digital technology requires intervention, usually in the form of regulation or legislation, to protect society from the harmful effects of its illicit usage. However, an understanding of how criminals misuse technology is a necessary first step. The best place to learn how criminals are misusing crypto-assets is from the criminals themselves. There are many online forums where people come together to discuss how to use (and misuse) crypto-assets to avoid the attention of law enforcement. It is from the advice contained in these forums that this paper attempts to understand this process by clearing the crypto-laundering forest to see the wood from the trees.

Literature Review

The introduction of all technology interacts with and affects the social ecology (Kranzberg, 1986). Digital technology is simply a tool that, depending on the intention of the user, can be used for legitimate and illicit purposes (Meighan, 2004b). All technology "can be of great benefit to society and be a force for good, and it can contribute to criminality that destabilises our common global security" (Goodman, 2015, p. 13). The rapid mobility of people, information, and money spurs innovation, efficiency, and inclusion while also creating new opportunities for criminals to exploit (Grabosky, 1998, 2001). The technology being discussed in this paper is crypto-assets which are defined as a private digital asset that are recorded on some form of digital distributed ledger secured with cryptography (the blockchain), are neither issued nor guaranteed by a central bank of public authority, and can be used as a means of exchange, for investment purposes, and/or to access goods or services (Houben and Snyers, 2020, p. 17). Emerging from obscurity in 2009 to achieving

almost universal acceptance today, crypto-assets have become a global phenomenon. Today, there are over 10,000 types of crypto-assets trading through 811 centralised exchanges, with a market capitalisation of approximately $2.75 trillion and a daily trading volume of almost $60 billion. The two biggest crypto-assets are Bitcoin and Ethereum, with market shares of 60.7% and 8.5%, respectively. The remainder of the other thousands of assets make up the remaining 30.9%.

Crypto-assets have many legitimate and positive uses. They are an efficient, reliable and cost-effective international payment method that can be used by all but in particular the 'unbanked' in the developing world (O' Sullivan, 2020, pp. 20–21). Online dark marketplaces took the lead in accepting anonymous payments through crypto-assets for criminal acts and services with relative ease (Popper, 2016; ElBahrawy et al., 2020). Crypto-assets can also be used to procure, commit, and finance criminal activity, such as ransomware attacks and a broader spectrum of cyber-criminality (Goodman, 2015; Furneaux, 2024). These crimes generate significant criminal profits, which are the primary motivation for nearly all crimes committed. Criminals are attracted to crypto-assets for many reasons such as (1) their perceived anonymity – the use of encryption to hide one's identity and frustrate law enforcement efforts to attribute a transaction to a real-world identity, (2) disintermediation – the ability to conduct a transaction in a peer-to-peer manner, decentralised manner without having to be physically present at a location and avoiding anti-money laundering (AML) measures, (3) being on an open network that is available 24/7/365 in every location across the world and on all devices including mobile phones, (4) the speed of transactions allowing money to be moved rapidly introducing may layers of transacting complexity easily, (5) their cross-border nature – the network is not constrained by sovereign boundaries and is available world-wide, and (6) irrevocable transactions (Filipkowski, 2008; Furneaux, 2018; Federal Bureau of Investigation, 2024).

In 2023, the Federal Bureau of Investigation received more than 69,000 complaints from the public concerning crimes that had a crypto-asset nexus and estimated losses of $5.6 billion (Federal Bureau of Investigation, 2024). Chainalysis, one of the major blockchain intelligence companies, estimated that in 2024 approximately $51 billion was received by public crypto-asset addresses they had identified as illicit, noting that this figure only covers on-chain criminality and not the majority of cases where profit is generated off-chain and moved into crypto-assets for transfer and laundering purposes (Chainalysis, 2025). Europol identifies crypto-assets as a cross-cutting facilitator of cybercrime and a challenger to criminal investigations (Europol, 2020). They also state that crypto assets are the de facto method of victim-to-criminal payments in ransomware and exploitation schemes, as well as criminal-to-criminal payments on the dark web (Europol EC3, 2021).

Unfortunately for criminals, the criminal profits generated also link the possessor of the funds to the crime. To avoid adverse law enforcement attention, a method is required to break that linkage – namely, money laundering. With the introduction of crypto-assets, criminals are now using a crypto-asset specific version of cyber-money laundering namely crypto-laundering – laundering the proceeds of crime through crypto-related digital assets. Crypto-laundering can be summarised as follows: (a) a predicate offence is committed in the real world (or online, with ransomware attacks being the most well-known vector of attack in this context); (b) proceeds of criminal conduct are accumulated and converted into crypto-assets if not already in that form while there will be some level of layering to obfuscate the financial trail (e.g. exchange to a different crypto-asset, using algorithmic tumblers or mixers, through gambling sites, etc.); (c) the 'cleaned' money is available for re-investment in further criminality or for the criminal to enjoy (most probably after they have been re-converted back to fiat currency) (Christopher, 2014; Brenig, Accorsi and Müller, 2015; Choo, 2015; de Andrade, 2017; Gifari, Anggorojati and Yazid, 2017; Mabunda, 2018; Custers, Pool and Cornelisse, 2019; Gonçalves, 2019). But to be clear, this is not necessarily a new phenomenon or method of committing money laundering; it is more like 'new wine in old bottles' (Grabosky, 1998, 2001; Meighan, 2004a). The advancement of technology and financial globalisation makes it easier to transfer funds illegally (Joveda, Khan and Pathak, 2019; Al-Tawil and Younies, 2021). Enforcement efforts, however, are caught in a game of catch-up with modern, rapidly changing, and sophisticated means of financial transfers, including the threats posed by crypto-assets (Grabosky, 1998; Goodman, 2015; Duff, 2019; Clark, 2020). Criminals are attracted to crypto-assets, just like the internet, not for its technological innovation, but because it offers a method to transfer funds pseudo-anonymously, disintermediated from traditional (human) AML controls, quickly, cheaply, and globally (Filipkowski, 2008, pp. 16–17; Demetis, 2010, p. 15). More privacy-friendly crypto-assets (e.g. Monero, Z-Coin) have increased the options for crypto-laundering and have made it more appealing, although their use is limited at present (Silfversten et al., 2020).

One particular cybercrime type illustrates the points made so far. Ransomware – malicious software that renders an infected system inaccessible by encrypting data - continues to be the prevalent cybersecurity threat to individuals, companies, and governments, with the most significant attacks being committed by major transnational organised crime groups, state-sponsored hacking groups, and hacking collectives (Furneaux, 2024, p. 28). While this threat vector has existed for decades, the introduction of crypto-assets has industrialised it and made it more effective with less chance of being caught (Carlisle, 2024, pp. 97–122). Payment of the ransom - to obtain a code to decrypt the data - is now always demanded in crypto-assets. There is often sophisticated 'customer care' available to assist the victim in converting fiat to crypto if they are unaware of how to do so. Due to recent law enforcement success and cases where no decryption key was provided, there appears to be a decrease in victims willing to pay despite almost immediate negotiation from the criminal (Chainalysis, 2025, p. 10). This perhaps indicates that entities are becoming more resilient and able to recover from an attack independently. Nevertheless, ransomware continues to be a significant crypto-enabled cybercrime with new, more effective strains emerging and approximately $813 million paid by victims in 2024. Once paid into the initial public address, the ransom is laundered. Understanding this process is critical and post-exploit behaviour offers law enforcement leverage to respond to the current incident and perhaps anticipate future threats that follow a similar pattern of behaviour. In 2024, the majority of ransoms were off-ramped to fiat currency through centralised exchanges. This allows law enforcement to identify the person behind the crime by utilising AML information held by a regulated exchange. Of course, sometimes the exchange may be located in an unfriendly jurisdiction that does not recognise law enforcement requests or court orders. Other destinations included being held in crypto-wallets or being transferred to mixers or bridges to obscure any follow-the-money investigative approaches (Chainalysis, 2025, pp. 10–17). The holding of funds in crypto is curious as ransomware is known to be carried out by financially motivated individuals. The holding of funds is either an indication of criminal caution in light of recent prosecutions or a new way of criminally exchanging funds using cold storage wallets as a commodity.

An IS-oriented process-theorising approach to crypto-laundering

In our field of information systems (IS), process theorising attempts to capture how phenomena unfold over time. It has been used on various occasions by scholars in this general spirit (Crowston, 2000; Niederman, 2021). The phenomenon of crypto-laundering lends itself to process theorising as it is both anchored on a fundamental procedural understanding of money laundering (i.e. the procedural flow in placing the illicit assets into the financial systems, layering them to complicate the money trail, and integrating them into the formal financial system), and it is also a complex phenomenon where a combined set of process theorising would benefit a deconstruction of it, as well as a better understanding of it.

In the broader context of process theorising, we will be applying a few different strategies for deconstructing crypto-laundering.

> S1: Sequence analysis where the scope and purpose are the identification and ordering of events where we can gain a deeper process-oriented understanding of the key steps that are prominent in the cryptocurrency laundering process.
>
> S2: Variability analysis, where we examine process variations and slight permutations that can branch out of the core steps of the sequence analysis and give us a more refined understanding of crypto-laundering.

Based on S1 and S2, we aim to develop a cryptocurrency-based cyber-money laundering process framework that will capture both key strategies as well as some variability, particularly when it comes to the operationalisation/execution of some steps. We should mention that other strategies connected to process theorising could emerge out of this process in future research as well. For example, scholars can explore modelling-based approaches that are inspired by our depiction of S1/S2 and might seek to simulate the dynamics of the crypto-laundering process, augmenting it with statistical patterns and quantitative analysis. In this paper, we are seeking to concentrate on S1/S2 and deconstruct the phenomenon itself. In what follows, we describe the distinct steps that we took to develop Framework 1 (Crowston, 2000; Niederman, 2021).

Steps Involved in Process Theorising

To operationalise process theorising in IS research connected to cryptocurrency-based cyber-money laundering, the following steps were followed:

1. Identification of the phenomenon of interest: the key focus on the broader phenomenon of interest in our case is cryptocurrency-based cyber-money laundering and so we are interested to see how end users (i.e. those engaged in cyber-ML) as well as exploited third parties (e.g. software providers) or willing participant institutions (e.g. consortia, platforms, algorithmic engines that are actively facilitating cyber-money laundering) participate in the crypto-laundering process. Thus, our key line of process-driven exploration is how users launder cryptocurrencies. This constitutes a clear and focused phenomenon that is amenable to process theorising.

2. Data Collection Process: our aim here has been to gather longitudinal data that can capture the crypto-laundering process, as well as refine it over time. We used a Python Scraping tool (see Appendix 1) to harvest dark-web text-based-only data from a few sources, and we augmented that with Reddit Forum data. While the core process (S1) came from the analysis of dark-web data and NVivo-based coding of a subset, we were surprised to see how many complementary insights we could gather from what was a very open discussion in the clear net on a well-established Reddit forum that has been operational for 16 years. Through Reddit API calls, we harvested the totality of the forum and used an LLM-based semantic analysis anchored on top of the S1-derived key steps to conduct variability analysis (S2). This allowed us to see how each key step might be variably expressed, instantiated and operationalised.

3. Development of Process: Here we identified the key steps in the process of how users launder cryptocurrencies; more specifically, we identify eight key events that delineate how users launder cryptocurrencies: 1) Access the Darknets, 2) Set up Anonymous Communication Channels, 3) Obtain Cryptocurrencies, 4) Mix Cryptocurrencies, 5) Move Funds to Secure Wallets, 6) Employ Obfuscation Techniques, 7) Use Privacy-Focused Hosting and Communication, 8) Dispose of Evidence. This is illustrated in Figure 1.

4. Comparative Co-Development of S1/S2: [This step will form part of the further research] In this step, one would typically compare different actual crypto-laundering cases as instances of the proposed process captured in Figure 1. Stress-testing the process with law enforcement staff that have expertise in handling crypto-laundering cases can both strengthen the generalisability of our process-driving findings, give us context in the development of the process, and provide insights into how a process-driven deconstruction can be beneficial for law enforcement. As this is still ongoing research, we have not completed this step yet but we plan to interview law enforcement experts to: a) enhance the generalisability of our findings, b) validate and corroborate the process-driven approach, c) build a complementary law-enforcement driven process that counteracts the crypto-laundering process and allows us to theorise both about the crypto-laundering process, as well as the counter-crypto-laundering process that Law Enforcement Agencies could use.

5. Analyse Variability: While we have already built in - as part of S2 - variability by looking at clear net discussions on crypto-laundering, we aim to further develop this approach once we validate the process with law enforcement. The scraping of additional forums and the ongoing semantic analysis for variability will help us build a more comprehensive account and pathways through which dominant or less prominent crypto-laundering processes occur. Further scholarly work here can look at user-adoption or success rates of disrupting crypto-laundering.

6. Developing a process model: Based on the analysis we describe above, we have created the model in Figure 1 to represent the key stages and decision points of the crypto-laundering process alone. This could be further enhanced by adding dynamics and feedback loops. More importantly, once we develop the LEA-oriented process, we can combine it with the process of crypto-laundering and showcase in a single framework how law enforcement can create user resistance in the crypto-laundering process that can lead to either complete disruption in the crypto-laundering process, delays for investigative opportunities, injection of honey-pot techniques across (some steps of) the process, etc.

In Figure 1 below, we showcase the current stage of development of the process for crypto-laundering. The process diagram derived from our analysis of the scrapped online forums reveals that criminals are interested in methods to preserve their sense of anonymity online and to transact with crypto-assets in a way that obscures their criminal origin. Below, we describe the key process aspects.

Real-world activity - criminal recommendations

Step 1. Accessing the Darknets: The entry point to the crypto-laundering process typically begins with accessing the darknet. It is worth noting that there is a multiverse of darknets and not just one. Many criminals will seek specific sites for information, illegal purchases, access to cyber-toolkits, as well as access to crypto mixers and tumblers. TOR, I2P, Freenet, Lokinet, Gnunet, Mysterium, Threefold, Utopia, Nym, are some of those darknet entry points we have encountered. Due to the need to build up a perception of anonymity, criminals will access services and marketplaces through these darknets, with TOR generally considered to be the most widely available option; however, a lot of discussion at this stage concentrates also in anonymity prerequisites. VPNs (e.g. OVPN, IVPN, Mullvad, and many more) are discussed as part of an effort to further preserve anonymity and mask the cybercriminals' real IP address (real-world identified and a friction point for law enforcement to investigate). Many VPNs also offer a no-log policy and accept subscriptions through cryptocurrency payments, further increasing the sense of security for the criminal.

Step 2. Enabling Communication Channels: Once online on the dark web, there is a need for criminals to exchange online messages for various coordination/buying-selling and other purposes. In this context, criminals set up anonymous communication channels and use encrypted messaging services (e.g. XMPP, IRC, Briar, DeltaChat, Cwtch, Jami, Session, Matrix/Element). This allows both criminal enterprises as well as individuals to communicate with a sense of security and away from the prying eyes of law enforcement. These are attractive and offer many advantages when compared with centralised services. In fact, we saw clear guidance amongst crypto-laundering advice that strongly suggested to "avoid centralised services like Discord, Telegram, WhatsApp, and Signal due to privacy concerns" even if many of these support end-to-end encryption and remain a very fertile ground for cybercriminal communications (e.g. Telegram). Distributed and/or decentralised messaging platforms/exchanges overcome privacy concerns around mainstream communications channels such as Signal and WhatsApp – which have complied with court orders in the recent past to provide information to law enforcement. Some criminals have purchased hosting services using crypto-assets and set up their own customised servers to increase privacy. Many of these can be used with secure encrypted/burner phones, however, their popularity is decreasing due to recent law enforcement infiltration of these supposedly secure networks.

Step 3. Obtain Cryptocurrencies: As seen from the above, these steps often require the purchase of services or tools. Criminals recommend the use of crypto-assets for this as any other payment method is subject to Anti-Money Laundering requirements, which provides law enforcement with opportunities to attribute the transactions (and the associated criminality) to a real-world identity. Criminals, therefore, need to obtain crypto-assets in as secure and anonymous a way as possible. Of course, the methods about to be discussed can be used to clean the dirty profits generated from off-chain crime and converted into crypto, as well as on-chain crime when the proceeds are already in that form.

Apart from on-chain crimes, obtaining cryptocurrencies forms a key component of crypto-laundering. This can be done through a centralised exchange; however, like a bank account, this leaves a financial footprint for law enforcement to follow. The usage of mixers and tumblers to obfuscate this trail has declined in recent years (Chainalysis, 2025). This leaves anonymity-seeking criminals a limited number of options: P2P exchanges, centralised exchanges in unfriendly countries, stealing the crypto, or using decentralised exchanges (DEX) where KYC requirements are non-existent (e.g. Bisq or LocalMonero). The data gained from the forums shows that criminals are ever on the hunt for newer privacy-focused crypto-assets, despite the continued popularity and acceptance of Bitcoin. Bitcoin enjoys strong acceptance and diffusion, is easy to use, but it requires additional laundering steps to prevent investigators from following-the-money. Privacy Enhanced Coins such as XMR and Monero, remain more technically difficult to use – however, user guides are readily available on the forums. Privacy Enhanced Coins offer strong privacy features with hidden senders, receivers, and amounts.

Step 4. Mixing Cryptocurrencies: The stage of mixing cryptocurrencies is a central and key stage in the crypto-laundering process and remains a key equivalent part of what traditional money laundering

positions as layering. The central objective of layering/mixing is the construction of cyber-complexity in the transacting crypto-asset trail. Thus, the step of mixing crypto-assets is an attempt to disguise their origin or rather to make tracing the origin using current techniques more difficult. While the use of mixers, joiners, and tumblers are readily available, criminals often use privacy features that they control locally using software such as the Wasabi Wallet. This is in response to recent cases where private companies, working with law enforcement, have developed algorithms to re-join or de-mix coins to show their true origin. The data scraped from the forums recommends using decentralised swap platforms such as AtomicDEX for swapping coins anonymously. However, they warn against sending cryptocurrencies directly to this service from a centralised exchange to avoid linking or clustering cryptocurrencies with KYC-enabled accounts.

Step 5. Moving Funds to Secure Wallets: A more recent development is the advice to move funds to secure off-line or cold wallets. There are many such devices readily available (e.g. Trevor), some of which have strong encryption and additional security features such as multi-signature and biometric security. The data suggests that criminals advise spreading funds across a variety of USB-style and mobile-based wallets, ensuring that any subsequent conversion to fiat is done in a series of staggered withdrawals. Interestingly, criminal groups are adapting to the financial practice of segregation of responsibility and using multi-sig to ensure that no one person can steal the funds – there is no honour amongst thieves. There have also been cases seen where a hardware wallet is exchanged as if it were cash, without the need to convert to fiat – this does involve an extraordinary level of trust amongst criminals, which could be obviated if there is ever a criminal-operated crypto-asset.

Step 6. Employing additional obfuscation techniques: Even after crypto-mixing and moving funds to secure wallets, crypto-launderers may seek to employ additional obfuscation techniques in order to conduct cyber-layering. The use of multiple wallets, rotating address, coin-swapping, and stealth transactions, all aim towards increasing the complexity of transactions. One example of this where Law Enforcement managed to disrupt the operations was in the use of Samourai Wallet's Stonewall feature that offered additional transaction obfuscation.

Step 7. Use privacy-focused hosting and communications: Often criminals want to utilise their own, customised hosting, web, and communication services on the dark web. Hosting, static site generators, and decentralised services with strong anti-censorship measures are available to purchase for crypto and is available to those with no technical expertise. This additional crime-as-a-service or criminal support is an evolving method of criminal assistance for which crypto is the main payment method accepted.

Step 8. Disposing electronic evidence: Crypto-launderers and cybercriminals are also sensitive to the real-world evidence that may link them to their anonymous cyber-life. For this reason, an increased use of LiveOS that leave no trace after shutdown and can be booted on any PC via a USB key are becoming prevalent e.g. Tails OS. The criminal fraternity also recommends having measures in place to prevent law enforcement gaining access to data on seized devices by availing of remote secure deletion (commonly known as 'bricking') and regular secure deletion of data using applications such as Bleachbit, Eraser, Secure Empty Trash, etc. Law enforcement regularly report attempts to remote wipe seized phones that are in their possession. A new recommendation from the forums is the use of disposable virtual machines (VMs) that 'self-destruct' after each use.

The data also suggests that common-sense information security should be adopted by people wanting to use crypto anonymous e.g. using different public addresses, avoiding re-use of chain addresses, using multiple wallets that can each handle multiple addresses, and the use of the techniques that we saw in the previous section for secure and one-time hardware use and internet access.

Evidence of illegal activity

Bearing the above in mind, the following physical and electronic evidence should be considered when searching a suspect location. Blockchain data is indicative of on-chain activity, while off-chain information includes physical devices, communication messages, and data sources that indicate crypto-activity:

- Seed phrases – a list of words (or mnemonic phrases) to recover a crypto-asset wallet (can be online or offline wallet)
- Wallet addresses and transactions
    - Paper wallets

  - Software wallets (seed phrases, apps on mobile phone)
  - Hardware wallets
  - Wallet.dat files
- VASP account information and documentation
- Bank account information and documentation
- List of websites visited
- Indications of interaction with TOR, dark net, dark net marketplaces
- Indications of/attempts at Data/Evidence Destruction
- Evidence of Private Messaging & Communication
- All mobile phone handsets
- Non-standard communication devices (e.g., similar to Encrochat devices)
- Internet routers

Real-world Friction Points represent investigative opportunities

Crypto-assets can be conceptualised as a self-governing information system that can be used as a means of value exchange. The fact that they are not backed by a government or central bank and were originally intended to not need any third party or government involvement fitted the cypher-punk, libertarian-inspired view that computer networks (information systems) could create order in society without transaction costs and, in turn, rebalance societal power dynamics. However, the reality is far from this ideal. Regulation and supervision are increasingly required from trusted third parties, and fiat money (government issued money) is needed to enter (purchase crypto-assets) and exit (sell crypto-assets) the system (Meighan, 2024 Pg. 65). Given the prohibitively high costs now associated with mining, the only realistic way to obtain crypto-assets is to get ones that are already held by another person by exchanging fiat for crypto at an exchange, using a crypto-ATM, locating a person with crypto-assets who wishes to sell them for fiat (P2P), receiving a salary in the form of crypto, accepting crypto in exchange for goods and services (both licit and illicit), through the proceeds of a cybercrime (e.g., ransomware proceeds), or stealing crypto-assets from an exchange (via a hack or exit scam) of from another user's wallet (e.g., investment fraud). These can be considered the interfaces or friction points between the real and the virtual/digital worlds. To exit the system, that is sell crypto-assets, one must do the opposite of the above or find an exchange that issues some type of credit or debit card that will allow the value of their held crypto-assets to be spent on goods and services in the real world (after conversion to a fiat equivalent value) (Meighan 2024, 66). The difficulty for the criminal in this situation is that the majority of the most used friction points are regulated by AML legislation that requires the entity to gather KYC information and monitor all transactions, allowing law enforcement to attribute an initial transaction to a real-world person. It is then easy, often through the use of blockchain analytical tools, to follow the money bi-directionally to or from a criminal act – obliterating the criminal's much-desired anonymity and exposing them to prosecution and asset seizure.

Next Steps

The exploratory study has laid a foundational process model for understanding crypto-laundering through a detailed analysis of scrapped forum data, essentially from the criminal mind directly. However, to further substantiate and refine this model, it is necessary to extend the empirical base. Future research will focus on broadening data collection by enhancing web scraping efforts to capture a wider array of cybercriminal narratives. Complementary qualitative methods—including in-depth interviews and focus groups—will elicit further insights into the decision-making and operational dynamics of the people behind these crime types. A targeted case study involving a law enforcement agency or Financial Intelligence Unit would validate the process model. This would assist in applying an external, practical perspective to theoretical underpinnings, thus aligning with real-world regulatory challenges.

The anticipated outcomes of these next steps carry significant practical implications. A detailed process-based perspective will inform policy development and provide operational advice for law enforcement and compliance professionals. Further, these insights could be used to enhance transaction monitoring, the crucial step in Anti-money Laundering (AML) that identifies suspicious activity and may prompt law enforcement to investigate. The enhanced study suggested in this initial research will contribute to better

regulatory frameworks for use in crypto-enabled cybercrime, leading to more efficient policy initiatives and law enforcement action.

Conclusion

This paper provided a process-based framework that outlines the main mechanisms underlying crypto-laundering. The data, scrapped from forums about the dark web and using crypto-asset securely, the research show a structured sequence for the criminal misuse of crypto-assets and for laundering the proceeds of crime through this medium. Future research, incorporating qualitative methods and more refined data, will be the next essential step to validate and expand upon this framework. This work contributes to a theoretical understanding of crypto-laundering and offers practical law enforcement guidance and pointers for regulatory development to combat crypto-enabled economic crimes - clearing the criminal forest to see the individual trees.

References

Brenig, C., Accorsi, R., & Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering. 23rd ECIS Münster, Germany (S 1–18).

Carlisle, D. (2024). The crypto launderers: Crime and cryptocurrencies from the Dark Web to DeFi and beyond. Wiley.

Chainalysis. (2025). The 2025 Crypto Crime Report. Chainalysis.

Choo, K.-K. R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In Handbook of digital currency (pp. 283–307). Elsevier.

Christopher, C. M. (2014). Why on earth to people use bitcoin. Bus. & Bankr. LJ, 2, 1.

Clark, R. (2020). UK Jurisdiction Taskforce Publishes Legal Statement on Status of Cryptoassets and Smart Contracts—Observations from Ireland. Commercial Law Practitioner, 27(1), 3–9.

Crowston, K. (2000). Process as Theory in Information Systems Research. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), Organizational and Social Perspectives on Information Technology (Vol. 41, pp. 149–164). Springer US. https://doi.org/10.1007/978-0-387-35505-4_10

Custers, B. H., Pool, R. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. European Journal of Criminology, 16(6), 728–745.

de Andrade, M. D. (2017). Legal Treatment of Crypto-Coins: The Dynamics of Bitcoins and the Crime of Money Laundering. Braz. J. Pub. Pol'y, 7, 44.

Demetis, D. (2010). Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach. Edward Elgar.

Duff, C. (2019). 'Dirty Money'—An Overview of the Irish Anti-Money Laundering Landscape. Commercial Law Practitioner, 26(5), 85–90.

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. Scientific Reports, 10(1), 18827.

Europol. (2020). Internet Organised Crime Threat Assessment. European Union Agency for Law Enforcement Cooperation.

Europol EC3. (2021). Bitcoin Guide for Investigators: Following the Money. Europol.

Federal Bureau of Investigation. (2024). Cryptocurrency Fraud Report 2023. Internet Crime Complaint Centre (IC3).

Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Techniques. International Journal of Criminal Justice Studies, 3(1), 15–27.

Furneaux, N. (2018). Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence. Wiley.

Furneaux, N. (2024). There's No Such Thing As Crypto Crime: An Investigative Handbook (1st ed). John Wiley & Sons, Incorporated.

Gifari, A., Anggorojati, B., & Yazid, S. (2017). On preventing bitcoin transaction from money laundering in Indonesia: Analysis and recommendation on regulations. 2017 International Workshop on Big Data and Information Security (IWBIS), 143–148.

Gonçalves, M. M. (2019). How Cryptocurrencies Enable Money Laundering. Malmo University.

Goodman, M. (2015). Future Crimes: Everything Is Connected, Everyone in Vulnerable and What We Can Do About It. Corgi.

Grabosky, P. (1998). Crime in cyberspace. Combating Transnational Crime: Concepts, Activities and Responses, 195–208.
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243–249.
Houben, D. R., & Snyers, A. (2020). Crypto-assets—Key developments, regulatory concerns and responses. 77.
Joveda, N., Khan, Md. T., & Pathak, A. (2019). Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information. International Journal of Economics and Finance, 11, 54.
Kranzberg, M. (1986). Technology and History: 'Kranzberg's Laws'. Technology and Culture, 27(3), 544–560. https://doi.org/10.2307/3105385
Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), 1–6.
Meighan, S. (2004a). An Examination of the Concept of Cyber-terrorism. Communique: The Management Journal of An Garda Síochána, June, 24–28.
Meighan, S. (2004b). Ireland's Response to Internet Child Pornography: A Critical Examination [M. Sc. In International Police Science]. University of Portsmouth.
Niederman, F. (2021). Process theory: Background, opportunity, and challenges. Foundations and Trends® in Information Systems, 5(1–2), 1–230.
O' Sullivan, J. (2020). After The Gold Rush. Gazette of the Law Society, 114(5), 20–25.
Popper, N. (2016). Digital Gold: The Untold Story of Bitcoin. Penguin.
Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes. RAND Corporation.

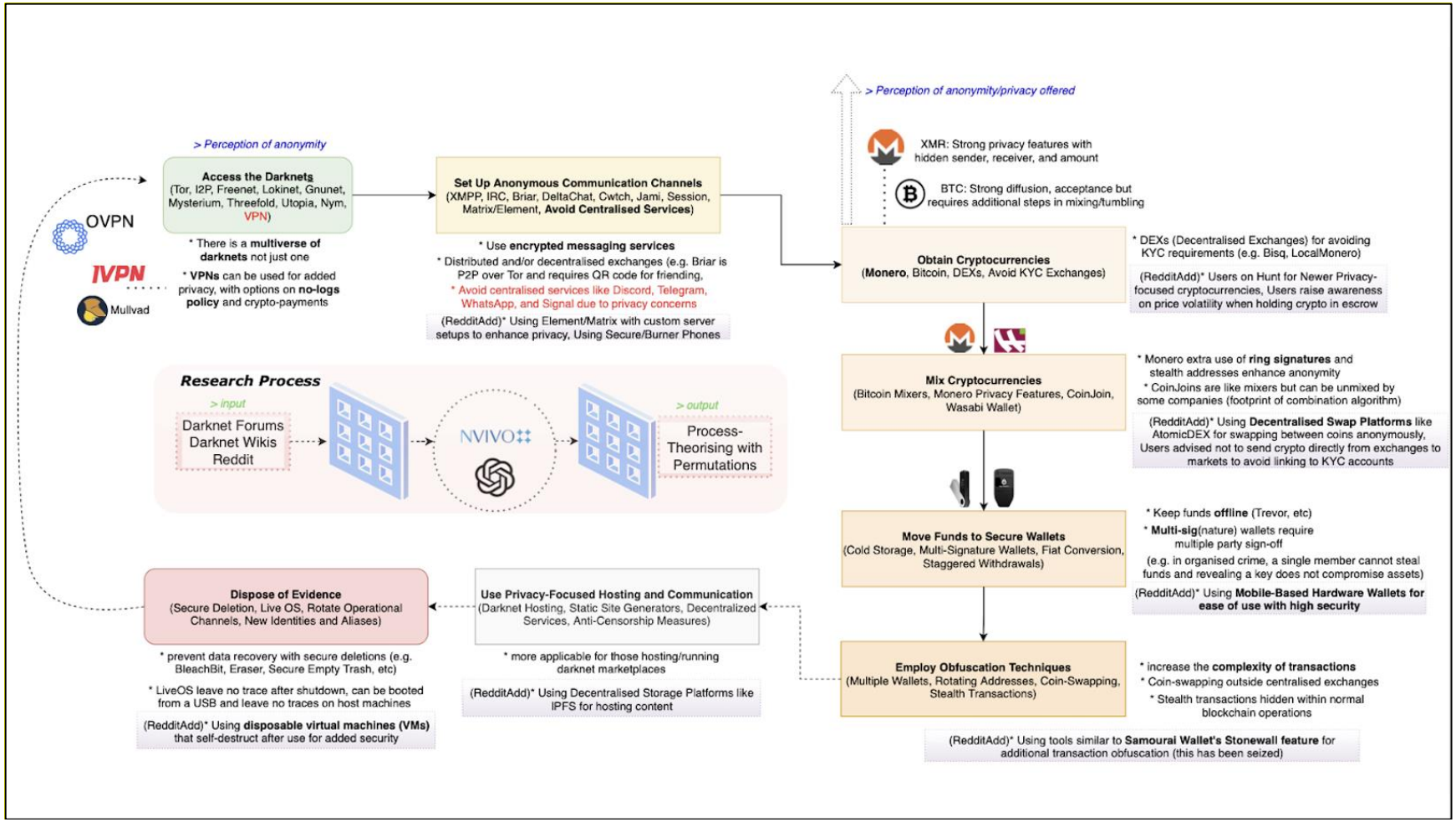

Figure 1: Criminal Crypto Process

Appendix 1 – Python Scraping Script

```
import praw
import prawcore
import os

def scrape_subreddit(subreddit_name, limit=1000, filename="output.txt"):
    try:
        reddit = praw.Reddit(
            client_id="**********",
            client_secret="**********",
            user_agent="**********")

        subreddit = reddit.subreddit(subreddit_name)

        with open(filename, 'w', encoding='utf-8') as file:
            post_number = 1  # Initialize post counter
            for submission in subreddit.hot(limit=limit):  # Fetch posts
                # Write post details with numbering
                file.write(f"Post {post_number}:\n")
                file.write(f"Title: {submission.title}\n")
                file.write(f"Author: {submission.author}\n")
                file.write(f"Score: {submission.score}\n")
                file.write(f"Subreddit: {submission.subreddit}\n")
                file.write(f"URL: {submission.url}\n")
                file.write(f"Number of Comments: {submission.num_comments}\n")
                file.write(f"Date Created: {submission.created_utc}\n")
                file.write(f"Content: {submission.selftext}\n")
                file.write("-" * 40 + "\n\n")

                # Fetch comments
                submission.comments.replace_more(limit=0)
                 comment_number = 1  # Initialize comment counter
                for comment in submission.comments.list():  # Flatten the comment tree
                    file.write(f"Comment {post_number}.{comment_number}: {comment.body}\n")
                    file.write("-" * 20 + "\n")
                    comment_number += 1  # Increment comment counter

                file.write("=" * 40 + "\n\n")  # Separator between posts
                post_number += 1  # Increment post counter

        print(f"Data has been successfully written to {filename}")

    except praw.exceptions.APIException as e:
        print(f"API error: {e}")
    except prawcore.exceptions.RequestException as e:
        print(f"Connection error: {e}")
    except prawcore.exceptions.NotFound:
        print("Subreddit not found.")
    except prawcore.exceptions.OAuthException as e:
        print(f"OAuth error: {e}")
    except Exception as e:
        print(f"An unexpected error occurred: {e}")

# Example usage: scrape_subreddit("darknet", limit=1000, filename="darknet_posts.txt")
```