Fighting Crypto-laundering: The case of Ireland's Financial Intelligence Unit

Steven Meighan
University of Hull
s.meighan@hull.ac.uk

Dionysios Demetis
University of Hull
d.demetis@hull.ac.uk

Abstract

In this paper, we present an analysis of crypto-asset related suspicious transaction reports (STRs) that have been submitted to Ireland's Financial Intelligence Unit (FIU Ireland) by private-sector Money Laundering Reporting Officers (MLROs) who have identified customer activity they believe to be indicative of (crypto-) money laundering. By analysing the 2,719 cryptocurrency-related STRs received in 2021 – the year in which crypto-assets were first regulated in Ireland for Anti-money Laundering (AML) – we contribute a customised socio-technical conceptual framework that helps to organize the complex phenomenon being studied and reflect on its interacting components as society attempts to combat the phenomenon.

Introduction

While traditional criminality operates in the shadows of the physical world and in the corners of the financial system, cyber-criminality and new digitally-enabled forms of crime, operate in ways that challenges the study of these phenomena and their detection and pursuit. The exploitation of crypto-assets (most notably Bitcoin) plays an important role in facilitating the transfer of criminal profits across all cybercrime areas. Crypto-assets have become the *de-facto* method of victim-to-criminal payments in ransomware/exploitation, as well as criminal-to-criminal payments on the Dark web (Europol, 2020). With this change, criminals are using a crypto-asset specific variant of cyber-money laundering: *crypto-laundering* (i.e., laundering proceeds of crime through crypto-related digital assets). In this paper, we organise the broader socio-technical system of crypto- laundering and its detection and pursuit and try to understand the basic systemic constitution of this phenomenon.

Literature Review

Money Laundering and Anti-Money Laundering

Certain criminal activities generate huge amounts of illicit proceeds (Conteh, 2018, pp. 2–4; Government of Ireland, 2016). The aim of these criminal activities is often greed which in turn provides power and opportunities for the (organised) criminal to enjoy a lavish lifestyle or to 'reinvest' into further criminality (Cassara, 2020, pp. 2–3; Newburn, 2017). Money laundering (ML) is the illegal processing of 'dirty' money, through legitimate banking and business channels and professionals, to conceal its criminal origins and make it appear to have come from a legitimate source. This breaks the link between the money and the criminality that generated it, frustrating the 'follow the money' approach of financial investigators (Connell, 2018, p. 71; Horan, 2011, p. 23.01; OECD, 2009, p. 15; Schott, 2006, pp. I1-7; Walsh, 1999, pp. 204, 212, 216). ML is recognised as 'an important contemporary phenomenon and a challenging problem area, with few prosecutions and convictions' (Demetis, 2010, p. 1) that features highly on the international and domestic political agenda (Stessens, 2000, pp. xiii, 90). There are myriad ways that criminals commit ML, ranging from small cash deposits in unremarkable bank accounts to the purchase of luxury items or property. It is a constantly changing criminal phenomenon, with updated modus operandi and business models (Demetis, 2010, pp. 11–12; Foley et al., 2019, pp. 3–4; Schott, 2006, pp. I9-10; van Wegberg et al., 2018, p. 421). For example,

money can be laundered by Organised Crime Groups purchasing exclusive London properties through (criminal) special purpose vehicles that operate through the exclusive, elite private banking system (see for example Burgis, 2020), via various online schemes that can be purchased from other criminal groups on the dark web (Bartlett, 2015; Goodman, 2015; White, 2020) or through more 'traditional' cash-based schemes (Robinson, 1995). Anti-Money Laundering (AML) is the series of preventative and repressive measures and efforts put in place by governments, in cooperation with international organisations and private entities, which aim to prevent, disrupt, detect, investigate, and prosecute ML (Duff, 2019, p. 88; Forsman, 2020, p. 26; OECD, 2009, pp. 15–16). Like ML, it represents a complex dynamic system that seeks to gather as much information for the national authorities as possible, using the national Financial Intelligence Unit (FIU) as a conduit between the private and public sectors, allowing the identification of the criminal and the owner of the assets. In simple terms, the FIU is a most critical authority: it acts as the central national agency responsible for receiving, analysing, and disseminating disclosures on suspicious transactions, made by the private-sector financial institutions and other entities, to law enforcement authorities to enable them to identify ML, criminality, and trace the proceeds of crime (Gleason & Gottselig, 2004; Stessens, 2000, pp. 143–145).

Crypto-laundering

More recently, due to the rise of ransomware attacks and a broader spectrum of cyber-criminality, money has been laundered using crypto-assets such as bitcoin, with online dark marketplaces taking the lead in accepting anonymous payments through bitcoin for criminal acts and services with relative ease (ElBahrawy et al., 2020; Popper, 2016). 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 (probably after they have been re-converted back to fiat currency) (Brenig et al., 2015; Choo, 2015; Christopher, 2014; Custers et al., 2019; de Andrade, 2017; Gifari et al., 2017; Gonçalves, 2019; Goodman, 2015; Mabunda, 2018). But to be clear, this is not necessarily a new phenomenon or method of committing ML; it is more like 'new wine in old bottles' (P. Grabosky, 1998; P. N. Grabosky, 2001; Meighan, 2004). The advancement of technology and financial globalization makes it easier to transfer funds illegally (Al-Tawil & Younies, 2021; Joveda et al., 2019). 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 (Clark, 2020; Duff, 2019, p. 85; Goodman, 2015; P. Grabosky, 1998). 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 (Demetis, 2010, p. 15; Filipkowski, 2008, pp. 16–17). 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).

Crypto-asset Service Providers

At the heart of many crypto-asset transactions one can find businesses that are referred to as Crypto-asset Service Providers (CASPs) or Virtual Asset Service Providers (VASPs).[1] On 23 April 2021, Ireland introduced legislation that regulated all VASPs for the purposes of AML. Essentially, it defined them as 'designated persons' which imposed traditional AML requirements on them. All VASPs legally operating in Ireland are required to be authorised by the Central Bank of Ireland, implement a risk-based approach to AML, to perform customer due diligence, and to report suspicious transactions to the FIU. Even though the crypto-asset system is considered to be a closed system (i.e., to get into it one must either create value - through mining: both legal and illegal such as crypto-jacking - or obtain value that already exists), in most cases, a business that exchanges fiat currency for crypto, or vice versa, is required to launder the proceeds of criminal conduct. Overall, the ways in which crypto-assets are involved in crypto-laundering are as follows : (1) (cyber)criminals accept crypto-assets in exchange for goods and services (illegal services are usually found on the dark web); (2) receive salary in the form of crypto-assets (oftentimes for providing 'Crime as a Service' to other criminals); (3) exchange fiat

[1] Depending on national legislation. In Ireland they are referred to as VASPs and this paper will adhere to that designation for consistency.

currency for crypto-assets at an exchange; (4) exchange cash for crypto-assets at a crypto-ATM (e.g. Bitcoin ATM[2]); (5) locate a person with crypto-assets who wishes to sell for fiat currency (P2P exchanges, e.g. kucoin.com); (6) steal crypto-assets from an exchange (via a hack or exit scam) or from a user's wallet; (7) purchase crypto-assets from a traditional financial institution; or, (8) through the proceeds of cybercrime (e.g. ransomware and sextortion ransoms paid and received in crypto-assets). There are many businesses in operation that can be considered full service VASPs. These allow the user to set up an account much like a regular bank account. This account can receive credits by way of electronic transfers from other credit and financial institutions (including from third parties). It can also receive crypto-asset transfers, including those that do not come through a VASP, making AML controls redundant. The account allows the user to purchase many different types of crypto-assets and place the value from these in their account. The balance of the account can be transferred to other accounts, to other crypto-asset public addresses, or can be spent using an issued debit-card. The potential for criminal exploitation of these accounts to launder illicit proceeds of crime is readily apparent.

Socio-technical Systems Theory

The interplay between ML, AML, and its constituent parts are a complex socio-political and economic milieu in which changes introduced (such as the introduction of crypto-assets and their regulation) oftentimes have unintended or unforeseen consequences that may present practical difficulties to the financial and non- financial sectors (Demetis, 2010, pp. 1–3). For that reason, and to help us organise the ways in which the broader crypto-laundering system works, as well as the ways in which the FIU-oriented detection and pursuit system attempts to counteract crypto-laundering, a suitable theory was required to make sense of their respective complexity; socio-technical systems theory (STST) is proposed. Bostrom and Heinen (1977) conceptualised a STST framework (see **Figure 1**) for describing and understanding complex systems. It "assumes that an organisation … can be described as a socio-technical system …. [which is] made up of two jointly independent, but correlative interacting systems – the social and the technical … [where] the outputs of the [organisation] are the result of joint interactions between these two systems" (Bostrom & Heinen, 1977, p. 17 original emphasis), into an environment that is made up of "the context, surroundings, and conditions within which the open socio-technical system operates and is situated " (Abbas & Michael, 2022). "The technical system is concerned with the processes, tasks, and technology needed to transform inputs into outputs" (Bostrom & Heinen, 1977 ibid.). This sub-system is further broken down into 'Technology' – the hardware and software (algorithms) that make up and control the system - and 'Task' – the procedures that govern how the system is used and operated (Abbas & Michael, 2022; Bostrom & Heinen, 1977). "The social system is concerned with the attributes of people (e.g., attitudes, skills, values), the relationships among people, reward systems among people, and authority structures" (Bostrom & Heinen, 1977, p. 17). This sub-system is broken down into 'Structure' – the formal organisation and management of the system including policies, procedures, rules, and regulations – and 'People' – which represents how the people who use and operate the system communicate, relate to each other, share information, and resolve difficulties (also known as the informal structure). It is important to remember that all the elements of the model are structurally coupled and interact with each other and the (external) environment. While the theory originally focussed on heavy industry, it has since been applied to a range of more modern disciplines such as "office-based work and services", business, management, and complex information systems, while remaining faithful to its original core principles (Davis et al., 2014; Morris, 2009; Mumford, 1983, 2003).

[2] The majority of crypto-ATMs in operation only deal in Bitcoin and operate unidirectionally i.e., fiat to crypto – where the users deposits cash and an equivalent value of bitcoin, minus a fee, is deposited to a supplied Bitcoin public address. Less commonly, there are some bi-directional crypto-ATMs and some that deal in more than one crypto-asset.

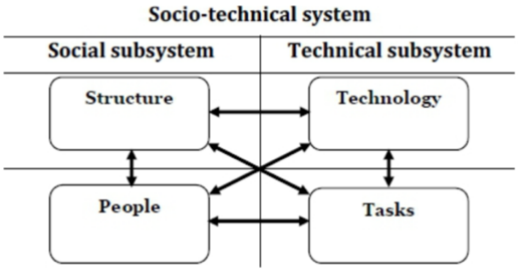

Figure 1: Socio-technical system

Research methodology

The research in this paper is based on a realist ontology, following an interpretivist epistemology (Klein & Myers, 1999; Walsham, 1995, 2006) with an inductive/deductive double loop of reflection reasoning (Dewey, 1910)). The research is theoretically underpinned by socio-technical systems thinking principles (Emery, 2016; Mumford, 2006; Trist, 1981; Trist & Bamforth, 1951). The research design involves a single case study approach of FIU Ireland that helps us to understand how crypto-laundering occurs and how the FIU, as an integral part of the wider AML system, attempts to detect and pursuit it. The case study covers the period immediately before and after the AML regulation of crypto-assets was introduced in 2021. Ireland is a suitable site for study as it is a recognised hub for techno-financial innovation. The primary data source for this research was a download of ~2,700 anonymised Suspicious Transaction Reports (referred to as STRs from hereon in line with Irish legislation) from FIU Ireland that concerned crypto- assets received in 2021. Secondary sources were AML legislation, FATF and Central Bank of Ireland documentation, and various internal procedure/process manuals. The data analysis involved uploading relevant data to NVivo software and using coding to organise and present the data in a way so that conclusions and insights could be safely developed (Edhlund & McDougall, 2020, p. 14), allowing the project to move "from the data to the idea, and from the idea to all the data pertaining to that idea" (Richards & Morse, 2012, p. 137). Each row (or NVivo case) represented a single crypto-asset related STR that was received at FIU Ireland during the period under review. The data fields (aligned in columns and described in Table 1 below) contained information about the STR and were categorised as: (1) codable fields that contained textual content for coding and analysis, and (2) classifying fields that contained meta-data (case classifications in NVivo) describing the STR. Classifying fields, or attributes, provided context to the codable fields and were later used to build case structures that grouped codable context.[3] In 2021, Irish regulated obliged entities (designated persons) submitted 38,712 STRs to FIU Ireland where they suspected their customer of being involved in ML or terrorist financing. Of these, 57 entities submitted 2,719 STRs (7.02% of total STRs submitted) related to crypto-activity. Of additional interest was the 51 non- VASP regulated entities who submitted 1,703 STRs that related to crypt-assets to FIU Ireland in 2021 (e.g., banks that had suspicions related to transactions involving crypto-assets). **Figure 2** illustrates the extraction process and the breakdown of the STRs analysed.

[3] Coding is the process of gathering material by topic, theme, or case. NVivo uses nodes as containers for coding where related material is gathered in one place where it can then be examined for emerging patterns and ideas. Cases are containers for coding that represents 'units of observation' e.g. people, places, etc. which can be classified if required (adapted from Edhlund & McDougall, 2020). The researchers began with the codes most aligned with STST: structure, people, technology, task, environment. Others were added as appropriate as the STRs were analysed to enhance the models devised.

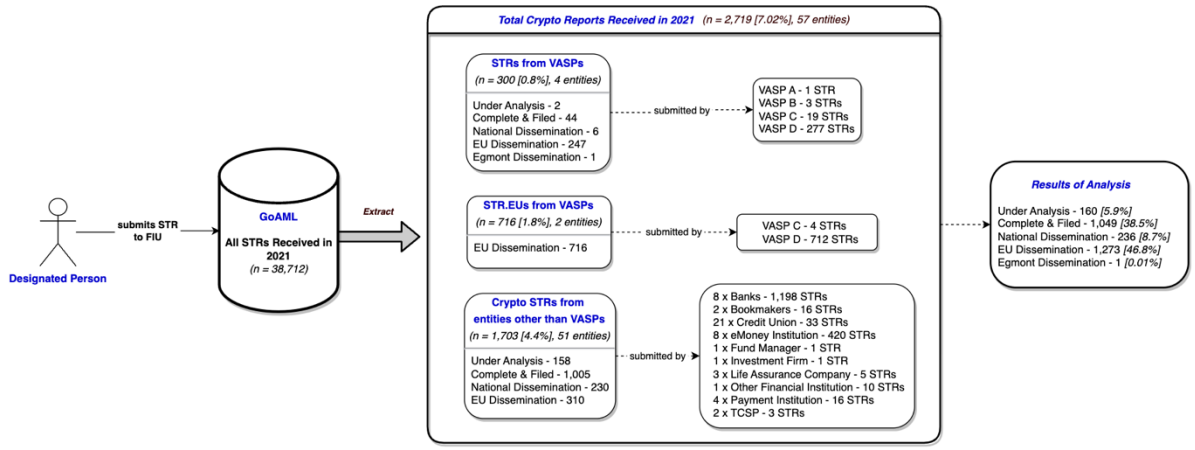

Figure 2: Breakdown of Crypto-related STRs & STR.EUs received in 2021[4]

Discussion

Of the 2,710 crypto-related STRs that were received by FIU Ireland in 2021, nearly half were filed for intelligence (available to law enforcement on request as required) and nearly half were disseminated to law enforcement, mostly abroad, as intelligence packages for consideration for investigation and recovery of criminal assets. 1,016 were filed by VASPs and the remainder by non-VASP designated persons, although this figure must be slightly reduced as some of the STRs captured in the word search designed to identify the crypto-related STRs from non-VASPS did not relate to crypto-assets.[5] A large number of the crypto-STRs received had no nexus to Ireland which is not surprising given the inherent makeup of crypto-assets and their lack of geographic restriction, however it does raise a question of AML efficiency with excess bureaucracy where submission to FIU Ireland necessitates forwarding the STRs to another FIU for further action. The majority of STRs received were well structured and contained enough detail for FIU analysis. There was also sufficient detail in the 'reason for suspicion' and 'action taken' fields to extrapolate the two STST models laid out below (see **Figure 3**). From our analysis, crypto-asset misuse supports all forms of regular criminal activity - drugs, gambling, CSEM, human trafficking. Criminals, well versed in social engineering and the use of spoofed telephone numbers, use them to lure fraud victims. An analysis of the crypto-STRs shows that crypto-launderers are not wedded to crypto-asset technology; one could say that crypto-launderers simply operationalise crypto-assets as a method of value transfer, and consequently, they view crypto-assets as useful due to specific features that they find attractive; similarly, the use of privacy-oriented tools such as VPN, TOR and the dark web, allow for a greater sense of anonymity and comfort. Despite having sufficient detail for FIU analysis and for constructing the STST models, the STRs were not without fault. Many entities submit STRs merely on the basis that a LEA made a request for information (e.g., data protection request or service of a court order) which is not a correct use of an STR unless further analysis determined suspicious activity not disclosed to the authorities or could be found by the authorities 'following the money'. Also, many STRs from our sample were submitted with a significant time-lag to the FIU, raising questions about the perceived pressure that obliged entities might feel to 'investigate'

[4] An STR.EU is a specific type of STR, generally submitted by an entity that is passporting their services to the EU, that has no nexus to Ireland and is required as a matter of EU law to be sent to the appropriate EU FIU. For the purposes of this research, the two were considered indistinct as the 'reason for suspicion' was the most important field for analysis and creation of the STST frameworks.

[5] The VASP STRs were readily identifiable as the entity concerned registered as a VASPs with the FIU. The non-VASP STRs were identified using a key work search with terms such as 'bitcoin', 'crypto', 'virtual', 'digital', 'Ethereum', etc. which inadvertently captured regular STRs that contained phrases such as 'virtual account' and 'digital TV'. This reduced the number of non-VASP Crypto-STRs to 971 and the total number of crypto-related STRs considered in this study to 1,987 which was sufficient for developing our models.

cases on their own before submitting a (typically sub-standard) report to the FIU. As we shall see, key crypto-related information that would be considered to be basic in reporting (e.g., a Bitcoin public address, account information, customer due diligence information, etc.) is often unreported by banks which creates additional bureaucracy as the FIU must then use its coercive powers to seek the required information.

Insights from VASP reporting of STRs

The two most important fields on an incoming STR are 'reason for suspicion' and 'action taken'. These are free-text fields where the MLRO from the reporting entity outlines the reason they found their customer's activity or transaction(s) suspicious and what action they took on foot of this suspicion. Based on our analysis, the STRs submitted by VASPs demonstrated a strong understanding of the underlying crypto-asset infrastructure and operation. The appreciation of ML risk involving the misuse of crypto- assets was appropriately nuanced. The STRs generally displayed a good level of detail that demonstrated the use of sophisticated transaction monitoring systems and processes to identify customer IP and MAC addresses, the use of VPN software, and interaction with mixers, tumblers, gambling sites, TOR, and dark web marketplaces. From this, the research was able to conclude that blockchain analytics, including 'address dusting'[6], was being performed by the VASPs and/or the commercial analytic software they were using. Evidence of cross-chain activity, the transfer of assets from one type of crypto-asset to another, was readily apparent. For example, the proceeds of an invoice re-direction fraud were converted to bitcoin at an exchange, co-mingled with the proceeds of additional frauds, and then converted to other crypto-assets before being withdrawn in fiat cash. However, there was almost no STR reporting that we have seen involving privacy- enhanced coins like Monero or ZCoin. This may raise significant concerns over a black hole in reporting. These privacy friendly crypto-assets utilise additional cryptographic techniques to disguise the publicly available blockchain information (Furneaux, 2018), which further frustrates law enforcement efforts. Police around the world have serious concerns around a growing dark crypto-laundering community promoting their use. Our analysis of STRs showed that, in most cases, the entire transactional behaviour and external business conduct of their reported customer was reviewed before a STR was submitted, but even in those cases, there were many instances where basic information was missing from the submitted reports e.g., current balances, other accounts held at the same institution, serial numbers of account opening documents, etc. It is readily apparent that VASPs are being operated in the same manner as a bank account i.e., a user sets up an account, provides the appropriate identification documentation, and uses the account as a vehicle to store and transfer value. This means that the concerns about the exploitation of basic gaps where the AML regime does not extend to the entire gamut of crypto-asset activity are somewhat misplaced. Unfortunately, this fact does not seem to have hampered crypto- asset misuse for the purposes of ML. As the free-text fields of an STR are filled by the MLRO, we could observe that when a new MLRO is appointed, their individual reporting style, presentation of information, and risk level of suspicion is reflected in the STR. This is worrying as it signifies that the underlying institutional reporting procedures are not well established and something so fundamental in terms of ML risk communicability like the STR can change dramatically from one MLRO to another. In many instances, the reason for submission is wholly unsubstantiated, even when we account for the necessary subjective nature in the construction of ML suspicion. There was also an uneven knowledge of what ML is among MLROs, with some appearing to have a rudimentary knowledge of key concepts such as layering and rapid transfers without any understanding that the source of funds must be criminal in nature. In some cases, customers were reported for breaking up their legitimately held assets into multiple crypto-assets, holding them for a short time, and recombining them back in one place before being converted to cash. This is certainly indicative of ML layering and integration, but only if the source of funds is illegal in the first instance. The majority of VASPs entering the Irish market are relocating from the UK and slowly transitioning to the Irish AML regime. This is apparent by the frequent reference to UK legislation (e.g., requesting consent to carry out a transaction when Ireland does not operate a consent regime), incorrect terminology, 'cut and paste' from reports submitted to the UK FIU, and no understanding of the crime reporting requirement under section 19 of the Criminal Justice Act, 2011. In many cases, STRs were submitted too late for any action to be taken by the police i.e., the funds had already dissipated to zero which raises a question of when are customer accounts frozen/blocked? In some instances, 60-100 transactions occurred over a normal period (i.e., not rapidly) but a delay in

[6] 'Address dusting' is where tiny amounts of crypto-assets are sent to suspect cryptocurrency addresses to track, trace, or cluster suspect addresses and attempt to attribute them to a real-world identity (the process can be considered a form of 'coin- tainting', or more accurately, 'address-tainting').

submission of the STR meant that the balance of the account at the time of submission was zero. This could indicate an issue with transaction monitoring or role creep where the level and intensity of 'investigation' by the VASPs is too detailed, takes too long, and is not disclosed to the police. Many VASPs are made up of different entities, some with different MLROs for each entity; this makes it more challenging to handle different aspects of their business. For example, one VASP has one e-money entity for its fiat business that also interacts with its VASP entity for its crypto-business. This results in different and multiple reports to the FIU from transactions that often cross-reference each other, creating unnecessary duplications in investigations. Depending on where the particular entity is located, this can result in multiple STRs being made to different FIUs. On the positive side, VASPs although suspectable to money muling had strong controls to identify this behaviour based on transactional activity, customer demographics, and expected account usage. Many excellent STRs were submitted that demonstrated how crypto-laundering was taking place which has been built into our two structurally coupled STST models to describe the phenomena in an easy-to-understand manner.

Crypto-STRs from non VASPs

Traditional credit and financial institutions had a much less developed appreciation of the risk of crypto- laundering. In many cases, STRs were made merely because their customer had purchased crypto-assets through an exchange, even well-known and regulated ones. In some instances, STRs were made because a business was operating as a VASP and in one case because a business was providing blockchain education. However, it was evident, that the traditional entities were becoming more risk-tolerant of crypto-assets towards the end of 2021. It was obvious from our analysis that all VASPs need a credit or financial institution to hold and transact their fiat funds. This produces an interesting fiat/crypto interface for financial investigators to explore. Traditional transaction monitoring systems was often confused by payments to exchanges, as it would involve medium to large transactions to a bank account in a foreign jurisdiction, usually activity outside that expected of their customer. The STRs showed interesting, although not illegal activity, namely in some cases people were pooling funds from multiple places and family members to purchase crypto-assets for investment purposes. In some cases, it was apparent that people had taken large loans to invest in crypto-assets, some of which were investment scams. The STRs also showed that some early adapters of crypto-asset technology generated staggering profits, which trigged suspicion of behaviour outside their expected, legitimate income and gave rise to tax evasion concerns (a predicate offence for ML in Ireland). In one case an STR was made because the branch official was suspicious of ML as the account was being used for crypto-investment and not being used for its intended purpose which raises the question was any account envisioned to be used for crypto when it was opened? Other non-financial businesses and professions similarly struggled in determining their risk appetite for crypto-activity. Entities were presented with customers who had earned large profits from crypto-investment and made STRs as they were unable to verify their customer's source of funds. Oftentimes, as with the traditional banks, STRs were made merely on the basis that their customer was involved with crypto-assets in some way.

Two Socio-technical System Models operating in a complex environment

The FIU is a part of the larger Irish and even-larger International/Supranational AML systems. As an organisation, it can be conceptualised as a system using the Katz and Kahn (1966) model which shows STRs received as inputs, the analysis of STRs as the throughput, and the disseminated intelligence packages as the output. The environment includes all of the other elements outside the system that have the potential to affect it. Feedback can include the information that is provided to the designed persons who make STRs (as outreach, presentations, training, and in the course of public private partnerships). The FIU is made up of constituent elements, all of which are systems themselves, and is deeply influenced by its external environment, which is everchanging due to technological advancements, such as evolving crypto-assets technology, and legislative changes, such as the expansion of AML regulations to include entities that deal with crypto-assets. As a socio-technical system, described using the Bostrom and Heinen (1977) model see **figure 3**, it is made up of a combination of social and technical elements. Its stated purpose is to prevent and detect ML, which it does by transforming STRs received from the private sector (inputs) into actionable intelligence for law enforcement (outputs). The technical components of the FIU system include the hardware, software, and algorithms that are designed to analyse and process the STRs. FIU Ireland uses a technology called GoAML, a UNODC software product, to perform its main purpose i.e., receive STRs, analyse all information available, determine if the information is indicative of ML or other criminality, and, if so, disseminate intelligence reports to law enforcement. FIU Ireland also utilises other technology to fulfil its role. The social component includes the people who use and interact with the FIU, such as FIU analysts, managers, and

stakeholders e.g., MLROs and law enforcement. They interpret the information generated by the technical sub-system and make decisions on how to progress activities that have been designed as 'suspicious' and indicative of ML. The structural component is made up of the formal and informal roles and relationships that govern how the FIU operates. The formal part is made up of the policies, procedures, and legislation; while the informal side is determined from the interaction of the people that operate the system, including FIU management and national (e.g., the AMLSC), supranational (e.g., the EU), and international bodies (e.g. other FIUs and the FATF). External to the FIU is its everchanging and evolving environment which represents the broader context in which it operates and includes PESTLE factors, such as the global economy, cultural considerations, and the political and legal systems, that influence the operation of the FIU. Included in this environment is the ML socio-technical system, which has adapted over recent years to accommodate crypto-laundering through the misuse of crypto-assets. Its technical component refers to the technology, especially crypto-assets, that is used to perform the task of moving and concealing the proceeds of criminal conduct using the myriad of methods available. It also crosses into civil society with tasks such as misusing the legitimate financial sector to move money, obfuscating the financial trail, and concealing its illicit origins. The social subsystem contains the people and organisations involved in the ML process, for example organised criminal organisations, money launderers, and corrupted/compromised insiders. These people use their connections and influence (formally and informally) to facilitate ML at evert stage. Another cross-over with civil society can be found in the structure sub-system. In here are the policies and legislation put in place to prevent and detect illicit activity, of which the criminal is well aware and is anxiously attempting to circumvent e.g., by the use of new technologies or an insider.

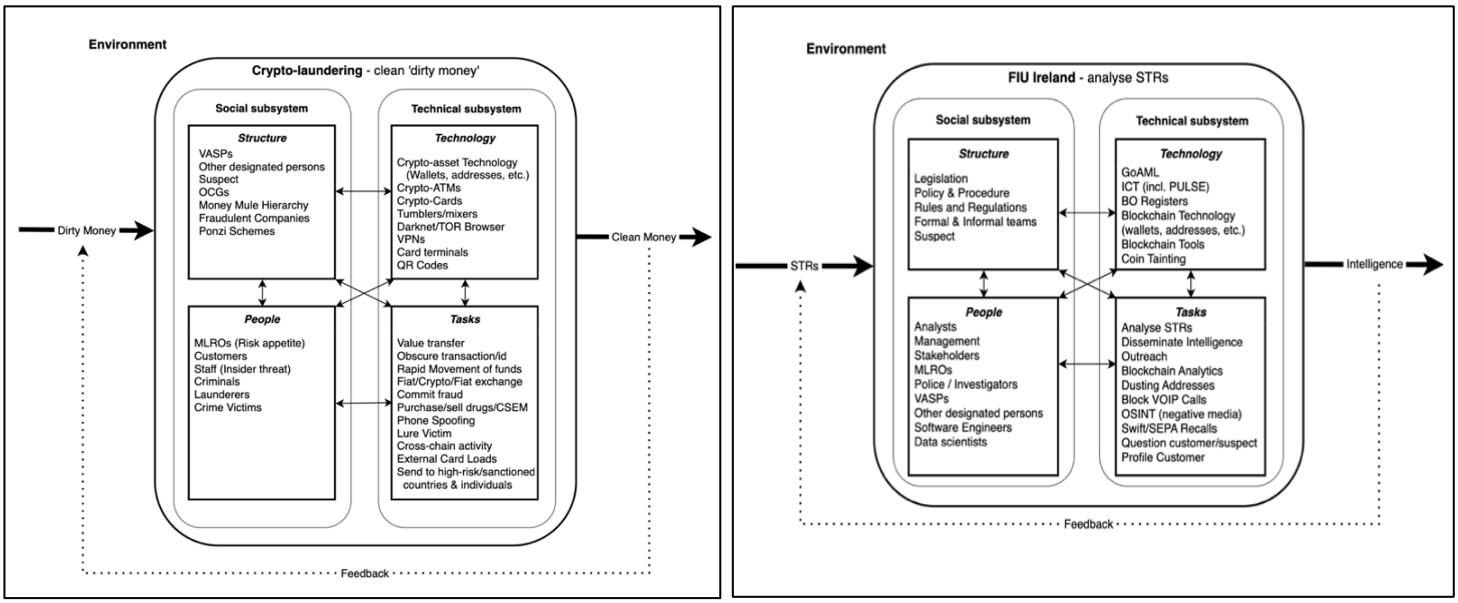

Figure 3: Crypto-laundering and AML (focussing on the FIU) as STST models

Limitations

The main limitation of this research is that we only see what is reported to FIU Ireland in an STR. We are not seeing the results of any investigations triggered by an FIU dissemination, nor are we seeing any other crypto-crimes that are initiated by or reported directly to law enforcement. Also, the timeframe of one year does not allow any longitudinal comparisons and analysis to be carried out. Future research could incorporate these limitations which would allow our STST models to be further refined and allow for temporal comparisons to be made to indicate how criminal behaviours changes over time and with new technology developments.

Conclusion

This paper has analysed the crypto-STRs submitted to FIU Ireland in 2021, a time when VASPs were brought into the AML regulatory regime. We have attempted to deconstruct a complex phenomenon, crypto- laundering, and provided a theoretical contribution by presenting two customised theoretical frameworks in the sociotechnical tradition of both the phenomenon studied (crypto-laundering) as well as its detection and pursuit by the FIU. This helps us to organise the phenomenon being studied as a

complex sociotechnical system and reflect on its interacting components as well as render the AML system as an equivalent and structurally coupled sociotechnical system that attempts to combat the phenomenon. The two STST models interact with each other in ways that may be exploited – criminals try to understand AML controls to defeat them, civil society tries to understand criminal behaviour to control it – indeed the most interesting lessons might be found in the middle space between them.

References

Abbas, R., & Michael, K. (2022). Socio-Technical Theory: A review. In S. Papagiannidis (Ed.), *TheoryHub Book*. http://open.ncl.ac.uk

Al-Tawil, T. N., & Younies, H. (2021). The Implications of the Brexit from EU and Bitcoin. *Journal of Money Laundering Control*, *24*(1), 137–149.

Bartlett, J. (2015). *The Dark Net*. Windmill Books.

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory. *MIS Quarterly*, *1*(4), 11–28.

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

Burgis, T. (2020). *Kleptopia: How Dirty Money is Conquering the World*. William Collins.

Cassara, J. A. (2020). *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails*. Independently published.

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.

Connell, D. (2018). Do EU Regulations Combating Money Laundering and the Financing of Terrorism Adequately Tackle Cryptocurrencies? The Case of Ireland. *Irish Journal of European Law*, *21*(1), 68–90.

Conteh, J. D. (2018). *Anti-Money Laundering and Combating the Financing of Terrorism*. Sondiata Global Media Ltd.

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.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2), 171–180.

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.

Dewey, J. (1910). *How We Think*. D. C. Heath.

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

Edhlund, B. M., & McDougall, A. G. (2020). *All about New NVivo Mac: The 2020 Edition of the Global Success in Qualitative Analysis*. Lulu.com.

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

Emery, F. (2016). Characteristics of socio-technical systems. In *The Social Engagement of Social Science, a Tavistock Anthology, Volume 2* (pp. 157–186). University of Pennsylvania Press.

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

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

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

Forsman, M. (2020). 30 Years of Combating Money Laundering in Sweden and Internationally – Does the System Function as Intended? *Sveriges Economic Review*, *1*, 24–55.

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

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.

Gleason, P., & Gottselig, G. (Eds.). (2004). *Financial Intelligence Units: An Overview*. International Monetary Fund : World Bank Group.
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.
Government of Ireland. (2016). *National Risk Assessment for Ireland: Money Laundering and Terrorist Financing*. Government Publications.
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.
Horan, S. (2011). *Corporate Crime*. Bloomsbury Professional.
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.
Katz, D., & Kahn, R. L. (1966). *Ths social psychology of organizations*. Wiley.
Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67–93.
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. (2004). *Ireland's Response to Internet Child Pornography: A Critical Examination* [M. Sc. In International Police Science]. University of Portsmouth.
Morris, A. (2009). *Socio-technical systems in ICT: A comprehensive survey*.
Mumford, E. (1983). *Designing human systems for new technology: The ETHICS method*. Manchester Business School.
Mumford, E. (2003). *Redesigning human systems*. IGI Global.
Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, *16*(4), 317–342.
Newburn, T. (2017). *Criminology* (3rd ed.). Routledge.
OECD. (2009). *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*. OECD.
Popper, N. (2016). *Digital Gold: The Untold Story of Bitcoin*. Penguin.
Richards, L., & Morse, J. M. (2012). *Readme first for a user's guide to qualitative methods*. Sage.
Robinson, J. (1995). *The Laundrymen* (New ed. edition). Pocket Books.
Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combatting the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX* (2nd ed.). The International Bank for Reconstruction and Development, The World Bank, The International Monetary Fund.
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.
Stessens, G. (2000). *Money Laundering: A New International Law Enforcement Model*. Cambridge University Press.
Trist, E. L. (1981). *The evolution of socio-technical systems* (Vol. 2). Ontario Quality of Working Life Centre Toronto.
Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. *Human Relations*, *4*(1), 3–38.
van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin. *Journal of Financial Crime*, *25*(2), 419–435.
Walsh, E. J. (1999). The Enforcement of Money Laundering Legislation. *Irish Criminal Law Journal*, *9*(2), 204–217.
Walsham, G. (1995). Interpretive Case Studies in Is Research: Nature and Method. *European Journal of Information Systems; Abingdon*, *4*(2).
Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330.
White, G. (2020). *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Global* (New Edition). Reaktion Books.