THE EVOLVING NATURE OF FINANCIAL CRIME WITH THE INCREASE OF INTERNET CAPABILITIES. CHALLENGE IDENTIFICATION, LEGAL CONSIDERATIONS AND POLICY RECOMMENDATIONS

A Thesis submitted to the Institute of Advanced Legal Studies, School of Advanced Study
University of London
In fulfilment of the requirements for the degree of

Doctor of Philosophy

by

George Daoud

Thesis Supervisors:

Dr. Colin King (Institute of Advanced Legal Studies, University of London)
Dr. Andrew Campbell (School of Law, University of Leeds)

Key words: Crypto; blockchain; money laundering; terrorist financing; darknet; emerging technologies; qualitative research.

STATEMENT OF ORIGINALITY

I certify that the intellectual content of this thesis entitled, *The Evolving Nature Of Financial Crime With The Increase Of Internet Capabilities. Challenge Identification, Legal Considerations and Policy Recommendations*, is the product of my own work and that all sources and all assistance received in preparing this thesis have been acknowledged.

This thesis has not been submitted to the University of London or other institutions for any other degree or for any other purpose.

Submission date: 3 May 2023

George Daoud
University of London ID # 190299514

Abstract

As every industry benefitted from emerging technological advancements, so too have emerging frontiers of dark payments. Remarkably, the sophistication of money laundering and terrorism financing has evolved through internet protocols and cryptographic technologies in the 21st century. The manner, degree, depth and breadth of emerging, innovative, and infrastructural sophistication released new capabilities which deploy effective high-level command coordination to leverage regulatory confusions and operational frustrations in the current crypto arms race. Consequently, criminal enterprises leverage resourceful mechanisms and target(s) allocation to deploy techniques on the darknet in carrying out illicit activities through high-fault-tolerance blockchain capabilities. This thesis seeks to establish joint operational considerations, doctrinal legal scrutiny, and counter-intelligence cyber warfare to strike effective choke points on pressure points concerning hyper-velocity cross-border multi-jurisdictional cryptographic phenomena. In doing so, private enterprises can engage in safe and innovative market capitalizations, public bodies can regulate to minimize unintended consequences, and law enforcement/intelligence can apply maximum aggressive pressure to effectively blunt, misuse and abuse of emerging technologies in the context of disastrous and evolving illicit operational commands.

Table of Contents

Table of Figures

Chapter 1 – Introduction

The rise and globalized nature of the internet, affect the financing of, profiting off and *modus operandi* of different crimes.[1] The internet metamorphosed through various evolving forms, fueling the sophistication of money laundering. This research examines internet-exploiting emerging laundering mediums, crypto assets and currencies. Regulators are confronting the benefits of these lucrative and rapidly expanding assets as well as the disadvantages, especially their appeal to money launderers and other forms of criminal organizations and activities. This thesis examines the current regulatory status of cryptocurrencies and assets. It identifies areas for improvement in creating workable frameworks that minimize challenges to innovation and competition while addressing their illicit use. As cryptocurrencies and their associated technologies grow in market size and variety, one thing is clear: this technology's greatest strength is its greatest weakness, the pseudonymous, decentralized capability to send and receive financial value across borders within seconds and minutes. From a practical standpoint, there will always be misuse and illicit use of any payment infrastructure, globally; however, the critical question for consideration, is what more can be done effectively and efficiently to minimize illicit use.

Crypto products and services vary in degree, size, and structure yet present unique obfuscation capabilities alongside their high-velocity cross-border nature. In the crypto ecosystem, multi-national non-harmonized regulatory frameworks contributed to the current "wild west" regulatory landscape.[2] The international cooperation required to address a global

[1]FATF [No Date]. "Designated Categories of Predicate Offences." Glossary, d-i.
[2]FATF [No Date]. "Virtual Assets." Homepage, second paragraph.

internet-operative phenomenon is yet to be established. This thesis highlights emerging threats and risks and suggests how nations can deploy initiatives to address emerging frontiers of dark payments.

The crypto ecosystem has attracted interest from private players, public bodies and law enforcement agencies over the past decade, with the U.S taking a more proactive interest at the start of the February 2022 Russia-Ukraine war.[3] Comprehensive intelligence into illicit crypto use is not yet established as ”Blockchain analytics is probabilistic and data produced has an inherent level of uncertainty associated with it*.”*[4] There is a crypto arms race amongst nations to reign in this phenomenon,[5] while illicit use is leveraging the current confusion, lack of oversight and operational frustration through several techniques. Defi exchanges, mixers and tumblers, cross-chain bridges/ chain-hopping and cross-asset buy-and-hold strategies, ‘coin swap’ services, and privacy-enhanced coins present emerging frontiers in money laundering (ML), terrorism financing (TF), and proliferation financing related to weapons of mass destruction (WMD) risks. There were estimates relating to illicit use to be at least $4 Billion in 2017, to $14 Billion in 2021.[6] Reports suggest the extent of illicit use increased to over $20 Billion in 2022,[7] where “this is a lower bound estimate — our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that

[3] President Biden’s Executive Order, (March 9, 2022). White House, Press release.
[4] FATF (2021). “Second 12-month Review Virtual Assets and VASPs.” Paris, France. p.30.
[5] Raza, A. (2020). “Sweden piles on to the Crypto arms race, joins China and other countries.” InsideBitcoins.com; Mukherjee, A. (2020). “India must not drop out of Crypto arms race.” BNN. Bloomberg News; Beikverdi, A. (2020). “South Korea gears up for imminent Crypto-Arms Race.” Blockleaders; Cong, Lin and He, Zhiguo and Li, Jiasun, (2019). “Decentralized Mining in Centralized Pools.” George Mason University School of Business Research Paper No. 18-9,
[6] Chainalysis (2022). “2022 Crypto Crime Report.”
[7] Chainalysis (2023). “2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking.”

this figure doesn't capture proceeds from non-Crypto native crime (e.g. conventional drug trafficking involving Cryptocurrency as a mode of payment)."[8]

The most severe forms of crime enabled, expedited, and exacerbated by Crypto products include depraved cases of pedophilia and child Abuse,[9] extortion and ransom,[10] financing of weapons of mass destruction,[11] human trafficking,[12] organ trafficking,[13] darknet narcotics' amazon-prime-style trade and identity thefts,[14] and terrorist financing.[15] This list is not exhaustive, and is bound to increase with the increase of value attributed to crypto products, by society. In realizing such, I endeavored to undertake this timely thesis in order to shed light on crypto misuse and abuse. The unintended consequence of bullishly riding the wave of crypto value in the market, is the increased incentives criminals are given to readily exploit this new technology for their illicit purposes.

I endeavoured to explore practical aspects related to crime, crypto & regulatory and operational responses by interviewing high-level officials from the three primary stakeholders:

---

[8] Ibid.
[9] Department of Justice, Office of Public Affairs (2019). "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin."
[10] United States Department of Justice. (2021) "Department of Justice seizes $2.3 million in Cryptocurrency paid to the ransomware extortionists darkside."
[11] Nichols, M. (2019). "North Korea took $2 billion in cyberattacks to fund weapons program." U.N. Report, Thomson Reuters.
[12] Barr, Andy and Hill, French (2021). "Virtual currencies: Additional information could improve federal agency efforts to counter human and drug trafficking." GAO. U.S. Government Accountability Office.
[13] Akbarialiabad, H., Dalfardi, B. & Bastani, B. (2020). "The Double-Edged Sword of the Dark Web: Its Implications for Medicine and Society." J GEN INTERN MED Vol. 35, p.3346–3347.
[14] Department of Justice, Office of Public Affairs (2022). "U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud."
[15] Office of Public Affairs, (2020). "Global Disruption of three terror finance cyber-enabled campaigns." The United States Department of Justice; Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, (2019). "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats." Santa Monica, CA: RAND Corporation.

law enforcement/intelligence, public bodies/regulators, and private/reporting entities. The originality of this research thesis is in the qualitative comparative analysis across all three category groups with a sizeable collection from six countries of their views,[16] in particular, exploring their perceptions, approaches, and concerns from multiple vantage points. The findings are significant since the crypto arms race is bound to intensify, and as their popularity explodes, so do their risk parameters. As such, undertaking this type of research to highlight key choke points on pressure points is valuable to cut through the societal sensationalism and crude exaggerations of societal value attribution and crypto capital market fetishizations.

Of course, while there are contextual and nuanced variable differences, the respondents from the three category groups expressed views that assisted in highlighting commonalities *within* and *across* themes pertaining to all three category groups. These themes were central tenants, which were found over the course of the research, and were scrutinized to capture the breadth and depth of their efficacy. The implications of the findings will be able to contribute to knowledge for future scholars to build on this new area of knowledge, as well as being of interest to policymakers, regulators and enforcement enterprises.

In chapter 2, I begin with a description of the methodology I undertook for this thesis. I set out the literature concerning qualitative research, namely in the form of elite interviews, which encompasses fieldwork with high-level professionals. I set out the process by which I approached the fieldwork and the rationale for choosing such an approach. In doing so, the thesis's foundational theory is formed to set the stage for the subsequent fieldwork conducted.

[16] Canada, United States, United Kingdom, France, Israel and Australia.

In chapter 3, I analyze the fundamentality of crypto, and blockchain, through the first form of such distributed communication technology, the internet, being the primary communication system developed and used. In doing so, I highlight the historical foundation of the internet and briefly outline its technical and operational specificity. This is highly important as concepts later discussed in chapters 5 and 6 require this foundational understanding of what the internet fundamentally is. I then briefly discuss the conventional modus operandi of money laundering. This assists in then bridging the discussion to the sophistication of new frontiers of laundering operations, utilizing and facilitated by the internet. This chapter in and of itself is not an original contribution to knowledge but rather a descriptive and stage-setting chapter for what is to subsequently come.

In chapter 4, I shift the focus to a purely legal discussion and analysis of the current Crypto taxonomy. While, ironically, the global AML regime did not start primarily targeting money laundering per se, but rather, the cross-border narcotics trade. The good old days of black pepper to ward off detection dogs and rotten potatoes to mask cross-border narcotics trade have galvanized a few nations at first, and subsequent increase in nations, to conduct multi-joint operations to tackle the global narcotics trade. Subsequently, nations quickly came to understand the role of laundering in the lifecycle of crime and, over time, shifted their focus to encompass money laundering, terrorist financing and financing proliferation of weapons of mass destruction. I discuss the Crypto taxonomy with a view to provide a foundation to Chapters 5 and 6. A detailed discussion of all national-specific legislation is beyond the scope of this thesis, not least given that, there are 195 countries in the world and over 200

jurisdictions. However, analyzing the root and the umbrella of these national Crypto regimes assists in highlighting the rules for the playing field.

In chapter 5, the thesis's largest and most comprehensive chapter, I first set out briefly the fundamentality of crypto technology and its utility. I discuss legal considerations pertaining to it. As this area is new and continuously evolving, and its exact legal nature has yet to be determined, I was conscious of the multiplicity of different treatments it has across multiple sectors and nations. I then delve into the data gathered from the fieldwork. In particular, I highlight the themes identified in conjunction with views expressed, the knowledge presented, literature available, national and international operations conducted and a critical analysis of, fundamentally, how respondents engage with this new phenomenon and the extent of concerns present across the three category groups. The respondents presented interesting perspectives, offering invaluable insights relating to common misconceptions pertaining to crypto, from its financial payment(s) utility to sophisticated dark payment utilities. The integrated factors emergent were many, and I endeavored to capture the primary pressure points presented by all three category groups in order to undertake a fair analysis.

In chapter 6, the second largest chapter, discusses the considerations from the three category groups in terms of operational prioritizations, intelligence infrastructures and approaches to this phenomenon. Chapter 6 discussions are built on the themes identified in chapter 5 pertaining to the considerations of all three category groups in approaching this phenomenon. This chapter builds upon discussions in chapter 5 analyzing approaches undertaken by the three category groups and further pressure points expressed in moving

forward with this phenomenon.

In chapter 7, the conclusions are set out. I argue that the yellow journalism style fetishization of crypto products is not only unsophisticated, but quite, in fact, dangerous, as expressed by emergent consequences, rising illicit use, and dark figures of crime,[17] currently being investigated. The trend of the overall global AML regime pertaining to this phenomenon is currently described as the "wild west"[18] for a reason, in that, subject to some enforcement actions, it is a free for all. I argue that the themes identified can be addressed in several ways to fill gaps in the industry. As with any achievement in human history, findings of solutions is often a messy process of mistakes, albeit sometimes costly and irreversible, but nonetheless, "…there is no effort without error or shortcoming" as Theodore Roosevelt described in his 1910 speech, Citizenship in a Republic.[19] But for such effort to bear fruit, I was determined to speak to all three category groups in order to cut through the crypto noise and be able to present findings that key stakeholders with skin-in-the-game are urgently looking for in the ecosystem, and from each other, to bring order to the wild west.

[17] Dark figures of crime are the number of crimes committed which are not reported or discovered, which puts into doubt the effectiveness and efficacy of crime data. See Supra n.7 of crimes not yet discovered or taken into account relating to crypto.
[18] Supra n.2.
[19] Theodore Roosevelt, (1910). Address at the Sorbonne in Paris, France: "Citizenship in a Republic" by Gerhard Peters and John T. Woolley, The American Presidency Project.

Chapter 2 – Methodology

Introduction

This chapter explains the objective(s) in conducting the empirical fieldwork of the research, the methodology used, and the reasons for the approach. This chapter illustrates the steps in the methodology and data analysis considerations and concludes with the limitations and effectiveness of the methodology I undertook in this research.

The fundamental objective of my research is to highlight differences and similarities *across* and *within* three category groups, namely i) public/regulator, ii) private/reporting entity and iii) law enforcement agencies/intelligence, concerning the sophistication of laundering practices in crypto products. Primarily, I seek to scrutinize the views of high-level officials across all three categories. To explore this emerging phenomenon, where the regulatory environment is popularly termed as being a 'wild west.' Crypto products and services vary in degree, size, and structure, and they present unique obfuscation capabilities alongside their high-velocity cross-border nature. In the Crypto ecosystem, multi-national non-harmonized regulatory frameworks contributed to the current "wild west" regulatory landscape.[20] The international cooperation required to address a global internet-operative phenomenon is yet to be established. The Crypto ecosystem has attracted interest from private players, public bodies and law enforcement agencies over the past decade, with the U.S taking a proactive interest at the start of the Russia-Ukraine war.[21] There is a crypto arms race amongst nations to reign in this phenomenon, while illicit use is leveraging the current confusion, lack of oversight and operational frustration through several techniques. Consequently,

[20] FATF [No Date]. "Virtual Assets." Homepage, second paragraph.
[21] President Biden's Executive Order, (March 9, 2022). White House, Press release.

a body of knowledge is needed to perform a series of functions: assist private enterprises in safely navigating this new phenomenon, direct regulators to channel resources appropriately while avoiding unintended consequences of driving market participants underground and leverage law enforcement agencies/intelligence capabilities on illicit financial flows to protect society. We do not know the form that crypto products' regulation will take. Similarly, we do not know the full extent of innovative misuse of this phenomenon. Nonetheless, further scrutiny of the evolving nature of crypto related financial crime is in order; this empirical research thus offers valuable insights into this important, contemporary matter.

Objective(s)

There is research examining the governmentality of interaction between LEA and the private sector in the AML context.[22] There is empirical also research on AML in the property market.[23] Further, research is shown to analyze, qualitatively, non-oil products export risk in the context of money laundering.[24] Likewise, there is research which explores cryptocurrency abuse through ransomware and money laundering.[25] To my knowledge, there is a dearth of empirical research exploring high-level officials' views and approaches regarding this phenomenon. Furthermore, there is little empirical data which examines all three category groups, qualitatively, regarding their insights and knowledge of financial crime in this emerging sphere of crypto products. Thus, this thesis approaches an important gap in the AML literature.

[22] Favarel-Garrigues, Georges et al. (2011) "Reluctant partners?" Security Dialogue Vol. 42: 179 - 196.
[23] Zavoli, Ilaria and Colin King (2021). "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis." Modern Law Review.
[24] Tanabandeh, Maryam. (2021). "Identifying export risks of non-oil products related to money laundering and related strategies." International Journal of Islamic and Middle Eastern Finance and Management.
[25] Custers, B.H.M., Oerlemans, J.J., Pool, R. (2020). "Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies." European Journal of Crime, Criminal Law and Criminal Justice, Vol.28, p. 121-152,

The scope of this research is the sophistication of laundering practices through emerging technologies, specifically, crypto products.[26] My primary goal was to speak to a sample of respondents across all three category groups to gauge their views and extract insights, to be able to paint a more complete picture regarding this misuse of this phenomenon. While all three category groups have different objectives and methodologies in tackling crypto related crime, the spectrum where they operate is interwoven into the context of the sophistication of laundering practices with this phenomenon. Particularly, in speaking to all three category groups, a cross-sectional analysis helped me not only to triangulate pressure points but also to examine fundamental approaches and their efficacy from a high-level officials' lens.

During these interviews, I was aware of my own biases as a legal practitioner in the field of anti-money laundering and counter-terrorism financing compliance for national and international clients. This influenced *which* questions were asked and *how* they were presented during the course of discussions. I was cognizant of the risks associated with undertaking such research in my own field, and the possibility of misplacing objectivity. However, my practical background assisted in shaping the questions I should be asking, as well as engaging in professional-based discussions at a high level. Furthermore, my own experiences were helpful in gauging and scrutinizing the views of respondents within all three category groups and their understanding of the field. I was also keen on maintaining impartiality with respondents so as not to dilute the quality of the data gathered. Recognizing this, an interpretive model was used to

[26] The securities regulation, tax considerations, and market innovative functions of cryptography are beyond the scope of this research.

isolate variables, identify discrepancies and develop/test hypothesis since "words and events carrying different meanings in every case."[27]

In a basic sense, qualitative research *"…fundamentally depends on watching people in their own territory and interacting with them in their own language, on their own terms. As identified with sociology, cultural anthropology, and political science, among other disciplines, qualitative research has been seen to be 'naturalistic,' 'ethnographic,' and participatory."*[28] This approach requires a genuine interest in developing relationships and speaking with diverse groups of people to understand "what they think about the world and how they form ideas about the world."[29] This approach requires approaching every respondent with an open mind and seeking to establish rapport quickly, so as to provide respondents with a platform to speak freely and candidly. This was highly important for a number of reasons which include but are not limited to: the professional position of the respondents and their capabilities to disclose information, the legal safeguards surrounding secrecy, confidentiality and security, the comfortability of respondents to disclose genuine views as opposed to 'fluff', 'lies' and/or 'sound-bites' and, finally, the reliability of the researcher to be able to present the data as credible and valid.[30] In a world full of recording devices, media sensationalism, social media misinterpretations and/or tar-and-feather style swarming, I found it important to speak to high-level officials in this space, who may not be able to present their views publicly, in a confidential setting in order to do justice to their views and honorable efforts in addressing this phenomenon.

---

[27] Gary Thomas, (2009). "How to do your Research Project." London: Sage Publications, p.75.
[28] Kirk, J. and Miller, M.L. (1986). "Reliability and Validity in Qualitative Research." Beverly Hills: Sage Publications. p.9.
[29] Ibid.
[30] Webley, L. (2010). "Qualitative approaches to empirical legal research." In: Cane, P. and Kritzer, H. (ed.) Oxford handbook of empirical legal research Oxford University Press.

Nature

The nature of the data gathered is qualitative in nature; however, it did not preclude quantitative data gathered from the respondents and the overall research journey. As in much "qualitative research, the researcher is the data collection tool as well as the one who analyzes the data."[31] The qualitative research was supplemented by doctrinal analysis of corresponding legislation(s). As this sphere is rapidly developing, accurate quantitative data has been hypothesized, and is continuously shaped, by academics and respondents, later discussed in subsequent chapters of this thesis. I was determined to interview a sizeable number of respondents in order to portray a representative sample of key themes and hypotheses in order to test the validity of the views presented. I was aware that the sample does not have to be statistically representative as qualitative research does "not seek to reach findings that are generalizable to an entire population. Instead, focused, in-depth studies are designed to go beyond description to find meaning."[32] Of course, given the nature of this phenomenon and the multiplicity of stakeholders, overt and covert, it is impossible to fully capture all views. However, the interviews conducted assisted in identifying patterns, both known and unknown, in order to link themes and extract the nuanced essence of the field. While there are different types of variables present, such as dependent variables, experimental variables, controlled and un-controlled variables,[33] the importance of identifying them prior to formulating the research questions was paramount not only to the success of the interviews as a whole but also the overall validity of the data.[34] These variables were important in relation to the *relevancy* of the respondent's capability to engage in the subject matter.

[31] Webley, L. (2010). "Qualitative approaches to empirical legal research." In: Cane, P. and Kritzer, H. (ed.) Oxford handbook of empirical legal research Oxford University Press.p.923
[32] Ibid.p.922
[33] A.M. Oppenheim, (1992). "Questionnaire Design, Interviewing and Attitude Measurement." London: 2nd edition, Continuum International Publishing Group Chapter 2.
[34] Ibid. Chapter 7

Most notably, expertise in this space is scarce given the newness and novelty of sophisticated typologies developing. As an example, certain variables influenced the views of respondents to engage with the subject matter, for example, private/reporting entities respondents, particularly in blockchain forensic-based work and cryptography-based internal and external investigations, were more well-versed to speak on the technical aspects of this field more so than public/regulator respondents who were more likely to engage in the regulative theoretical and practical approaches to regulation infrastructures. As such, in order to qualify a respondent as an expert, I undertook a preliminary interview with each respondent to achieve two objectives: i) inform and explain the nature of the research and ii) understand their *extent* of involvement in this field to be able to engage confidently with this subject matter. Subsequently, if a respondent demonstrated a capability to engage with this subject matter, I undertook the actual interview on a date based on availability to ask a series of open-ended questions for semi-structured interviews. The purpose of open-ended questions is highly important so as to avoid asking leading questions or eliciting specific responses, which may jeopardize the objectivity of the data. The extemporaneity and rawness of respondent views were highly important in order to maintain consistency of, reliability and credibility.

Preliminary interviews

Prior to the fieldwork, I set out to conduct preliminary interviews to achieve disclosure regarding the nature of the research as well as to qualify respondents as experts. Due to the scheduling of high-level officials' calendars, it was not always possible to conduct separate preliminary interviews apart from the fieldwork. In my judgment, a decision had to be made with respect to the qualification of a respondent on-the-spot. By way of illustration, a respondent

expressed their field to be purely sanction-related with no prior involvement in crypto products or illicit financial flows and therefore was disqualified as an expert to be used in the fieldwork. In the same vein, a respondent who is a Director of an LEA/Intelligence had extensive experience (more than 20 years) in computer science investigations, LEA/Intelligence deep involvement as well as an impressive academic background specializing in the field, earning them the position of Director of LEA/Intelligence, which qualified them as an expert to continue in the fieldwork.

As I proceeded with the preliminary interviews, there were a number of considerations that had to be taken into account, namely, how structured should the interviews be? To what extent should I pursue questions? What exactly should the follow-up questions be during any given questions? How relevant is the data being presented? To what extent should certain subjects be addressed during the interview according to the responses from the respondents? How can I maintain impartiality? How can I minimize the risk of my influence on the responses? How long should I stay on a subject matter? When should I move on to the next question? This required primarily a balance to be struck before the preliminary interviews, during the fieldwork and subsequently as I moved from one respondent to another.

The preliminary interviews did not take longer than twenty minutes as I had conducted surface-level background research into a given respondent's background(s). This assisted in narrowing the focus of which respondents would participate in the research. An obstacle I encountered was some respondents' insistence to have advance notice of the questions for the fieldwork. This posed a challenge as presenting the respondents with the questions would dilute the rawness and reliability of the data to capture true views of the ecosystem. Another obstacle

was some prospective respondents engaged in the preliminary interviews, however did not proceed with the fieldwork due to a number of reasons known: comfortability with what the questions might be and uninterest in the subject matter, and reasons unknown and unverified: condescending arrogance (which was manifest through the unfriendly, harsh and discourteous tone in the preliminary interview), biases relating primarily to crypto fanatics (whereby in the preliminary interviews, it was expressed more than once by prospective respondents in the private/reporting category group that research of this kind is moot and that crypto-based products are free from any fault or illicit activity, the miracle holy grail of pureness of all that is good, which is not only a biased position to hold but more so, an unsophisticated approach to any phenomenon) and/or insecurity with engaging with the research due to the professional positions occupied – which is completely understandable and respected. After every preliminary interview conducted, I communicated the ethics and consent form which outlines the nature of my research, my contact information, my supervisor's contact information and the ethics committee's contact information. All consent forms were signed and stored. In order to be able to capture the breadth and depth of the data, transcriptions supplemented notes taken during the fieldwork itself.

The utility of the preliminary interviews assisted in several fashions, primarily, it helped filter a respondent's expertise and involvement in the space, which would qualify them to speak in relation to it. I was keen to avoid the bandwagon over-simplification of branding of any crypto products' espoused by any entity to 'sell' or advocate the validity of the subject matter. Rather, as a researcher primarily interested in the advancement of knowledge, my focus was on respondents who could provide genuine and balanced accounts of their experiences, views and expertise relating to this space. Despite the availability of prospective respondents known in the crypto field,

I was not interested in speaking to die-hard hyper-crypto fanatics. This would have compromised and made the data worthless. In a basic sense, if it is garbage in, then it is garbage out.

Preliminary interviews also assisted in establishing confidence in my approach, but, more importantly, highlighting the skills I would need to engage at a high level with all three category groups. In doing so, I was determined to sharpen and add to my own knowledge of the field in order to be able to properly engage with all three category groups.

The Fieldwork

Before embarking on the fieldwork, I underwent the ethics review procedure for the University of London, School of Advanced Study. This was an important step in the process not only from a procedural standpoint to commence with the fieldwork and pilot interviews, but, also to demonstrate my understanding of ethical behaviour when engaging with this type of research.

As I am deeply thankful to and blessed by all respondents who took part in the research, I must first address the responsibility I have as a researcher in pursuit of knowledge. It is paramount to recognize the ethics and the nature of academic freedom entrusted to researchers. Academic freedom has been expressed to be "the freedom to pursue truth wherever that may lead."[35] I was determined to pursue truth. While there is 'a truth' and 'The Truth', it was important for me to engage with every respondent in the same manner so as to maintain impartiality and fairness. Not every respondent had an answer and, likewise, not every respondent was obliged to give any detail or piece of information. It was clearly expressed to every respondent that: i) if they do not know

[35] Hogan, B. E., & Trotter, L. D. (2013). "Academic freedom in Canadian higher education: Universities, colleges, and institutes were not created equal." Canadian Journal of Higher Education, Vol. 43 Issue.2, p.70.

or have an answer, then that is fine to express so and ii) they are free to withdraw at any point without giving a reason.

At the outset, an obstacle I quickly encountered was the obvious issue of access. This is a well-established obstacle in many research endeavours not only from the standpoint of access to respondents but likewise access through gatekeepers: employing institutions who vetted my requests through legal safeguards. Originally, I had envisaged that a sample size of 18-20 participants would suffice. I had to be careful not to increase the sample size due to: i) the mootness of extensive data, ii) the practicality of time constraints, iii) constraints of word limits in the writing and iv) narrowing the focus. Resolving such, I was very particular in choosing a representative sample which would provide the avenue to express the real-world views of experts in the field. This is described as purposeful sampling.[36] In doing so, it assisted me in also applying the snowball sampling technique, whereby the respondents would suggest alternative or further prospective respondents to interview.[37] This was highly beneficial as high-level officials are more inclined to oblige each other's requests to speak with an unknown researcher, as opposed to my own experience during this research, where high-level officials will not likely respond to an unknown researcher randomly.

As a first step, I made a list of over fifty prospective respondents I had an established relationship with or knew on a surface level. Following approval of the research ethics by the University, I reached out to my contacts nationally and internationally in the public and private sectors. I also utilized LinkedIn as a medium to facilitate communication to break the ice in

[36] M.Q. Patton (2002). "Qualitative Research and Evaluation Methods." 3rd edn. London: Sage Publications.
[37] Supra n. 31. p.922.

reaching out to prospective respondents whom I did not know. Surprisingly, LinkedIn was the most effective approach to garnering prospective respondents in the private/reporting entity category group. The public/regulator and law enforcement/intelligence category groups were by far the most difficult to gain access to. This is due to a number of reasons which include but are not limited to: people in those fields do not regularly engage on social media; they are not always as publicly active as private/reporting entity respondents are; there are extensive professional obligations that bar or limit them from responding freely to random requests; and high-level officials in those category groups do not regularly oblige unknown person(s) requests for engaging in academic research; and time and scheduling constraints. The empirical research would not have been possible without those extensive relationships, nationally and internationally which have been developed through word-of-mouth efforts. Initially, I had hoped to interview undercover agents engaged in the field of cryptography investigations, but this was ultimately not possible. But this limitation was quickly overcome by the fact that high-level officials in the law enforcement/intelligence category group had a bird's eye view of the undercover operations conducted, which shaped the data collected. Another limitation was unawareness of whether my requests for engagement were actually circulated to the appropriate personnel through email/official channels or whether it was lost in communication/ignored. For illustrative purposes, **Figure 1** demonstrates the response rate received by all three category groups.

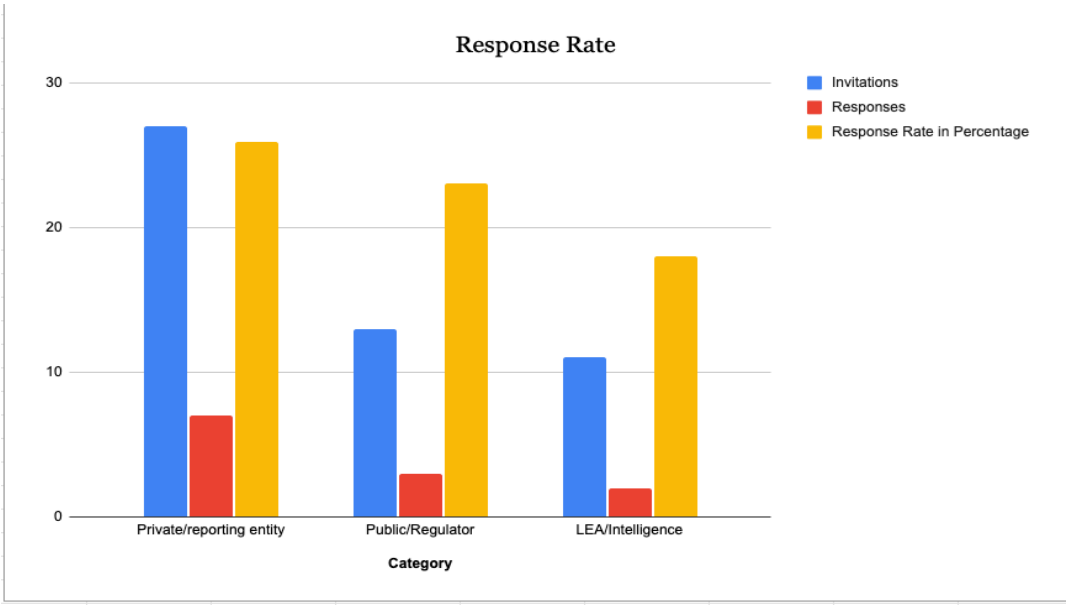


Figure 1: Response Rate

In total, I interviewed 10 respondents in the private/reporting entity, 4 respondents in the public/category, and 5 respondents in law enforcement/intelligence, along with 1 respondent who is a reputable Professor of Computer Science at a reputable University regarding the technical aspects of cryptography. In total, there were 20 respondents from Canada, the United States, France, Australia, Israel and the United Kingdom who engaged in this research. The interviews varied from a minimum of 1.5 hours to a maximum of 8 hours (spread across multiple interview cycles). This was based on the ability of respondents to divulge data as well as my judgment to proceed and/or stay on a given topic. The fluidity of the data and its spontaneous nature informed the flow of each interview, where themes were either re-occurring and/or brand new.

Overview of Respondents

It was important for me to select respondents with deep involvement in this field based on three factors: length of time in the field and degree of involvement (experience), academic background (education), and positions held (seniority). It was my initial intention to evenly capture

a numerical amount across all three category groups, however, ultimately, there were more respondents from the private/reporting entity category group. This is understandable, given the access issues previously discussed. Moreover, there was, understandably, a range of knowledge of experiences amongst respondents. For example, respondents in the private/reporting category group were more well-versed in speaking on the mechanical aspects of cryptography than the public/regulator category group. In the same vein, respondents in the LEA/Intelligence category group were more well-versed in the mechanics of real-world investigations and illicit-use effects than both other category groups. This provided a rich spectrum of data collected. It was also beneficial to the research that some private/reporting entity group members had experience in LEA/Intelligence. For illustrative purposes, **Figure 2** provides an overview of the respondents by the three factors outlined:

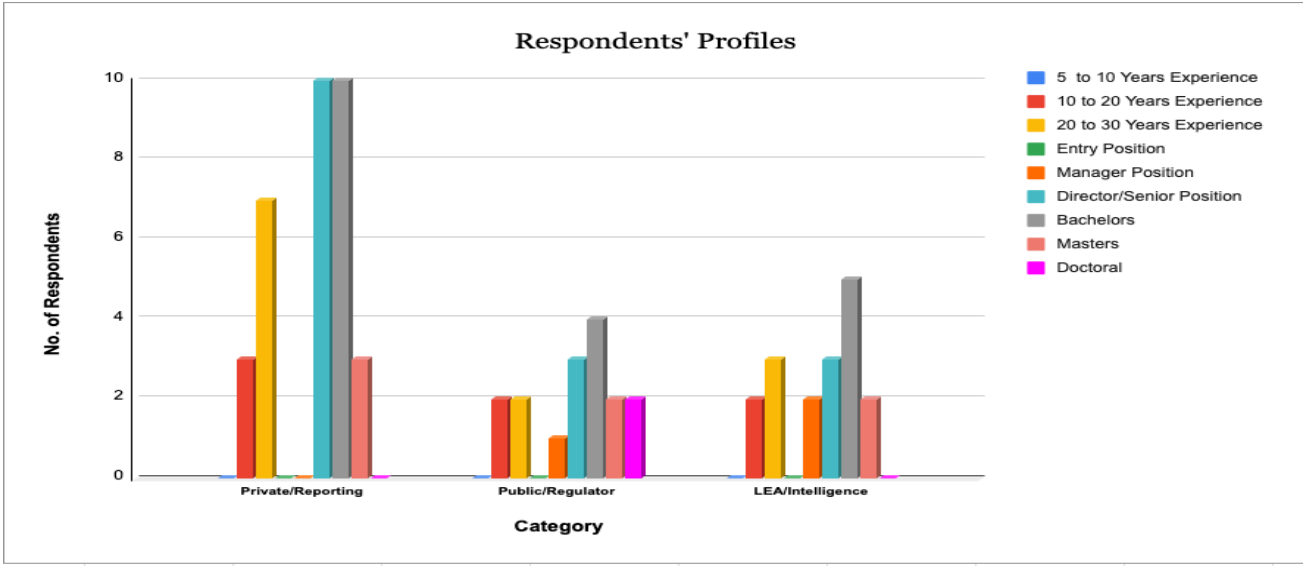


Figure 2: Overview of Respondents

Considerations regarding Anonymity and Confidentiality

It is generally accepted as unethical to reveal a respondent's name.[38] At the outset, it is important to note that confidentiality and anonymity are important in qualitative research. However, these two concepts are theoretically distinct.[39] Confidentiality pertains to the management of private information "that has been communicated in trust of confidence, such that disclosure would or could incur particular prejudice."[40] Where anonymity pertains "specifically to removing or obscuring the names of participants or research sites, and not including information that might lead participants or research sites to be identified."[41] In contrast, anonymity is taken as an ethical norm, whereby the objective is to avoid harm to participants as has been enunciated to have occurred in the past.[42] Examples have been listed whereby anonymization occurred, however, *recognition* still caused emotional harm.[43] As there are extensive factors inherent in fieldwork, anonymity does not necessarily guarantee confidentiality.[44] Even when anonymization is done, possible respondent identification through narrative is not an impossible task.[45] For such reasons, all respondents engaged in this study, to the best of my ability, have been treated with the utmost respect of confidentiality and anonymity.

---

[38] Van den Hoonaard WC (2003). "Is anonymity an artifact in ethnographic research?" Journal of Academic Ethics Vol.1, p.141–151.
[39] Tilley L and Woodthorpe K (2011). "Is it the end for anonymity as we know it? A critical examination of the ethical principle of anonymity in the context of 21st century demands on the qualitative researcher." Qualitative Research Vol.11: p.197–212.
[40] Giordano J, O'Reilly M, Taylor H, Dogra N. (2007). "Confidentiality and Autonomy: The Challenge(s) of Offering Research Participants a Choice of Disclosing Their Identity." Qualitative Health Research. Vol. 17 Issue. 2, p.264-275.
[41] Walford, Geoffrey. (2005). "Research ethical guidelines and anonymity." International Journal of Research & Method in Education. Vol. 28. p.83-93.
[42] Ellis C (1995). "Emotional and ethical quagmires in returning to the field." Journal of Contemporary Ethnography Vol. 24 Issue. 1, p.68–98; Whyte WF (1981). "Street Corner Society: The Social Structure of an Italian Slum." 3rd edn. Chicago: University of Chicago Press.
[43] Tolich M (2004). "Internal confidentiality: When confidentiality assurances fail relational informants." Qualitative Sociology Vol. 27, p.101–106.
[44] Nespor J (2000). "Anonymity and place in qualitative inquiry." Qualitative Inquiry Vol. 6, p.546–569.
[45] Mondada L (2014). "Ethics in action: Anonymization as a participant's concern and a participant's practice." Human Studies Vol.37, p.179–209.

Chapter 3 – Crypto Emergent Sophisticated Crimes

Introduction

Money laundering is an activity which has evolved over time, as either a reactive evolution or a proactive opportunism. Like many activities in the late 20th and early-modern 21st centuries, technology has fundamentally changed the laundering process and outcome, from reach to scale. To discuss the role of the Internet and its effect on the sophistication of laundering practices, first, a contextual analysis of the Internet and its emergence will be discussed. Second, Blockchain fundamentals will be outlined. Third, the Blockchain and the Internet's applicability in the financial sphere will be set out. Fourth, a brief discussion of conventional money laundering. Lastly, the fifth section will discuss the sophistication of laundering and sophistication of predicate offence practices as well as typologies using increased internet and technological capabilities.

The Internet, a Versatile Phenomenon

History

In order to understand the increasing capabilities of the internet and the use thereof for money laundering, a brief historical context about the origins of the internet, its utility and its application will first be discussed. The internet emerged from the computer science discipline, with a core objective of establishing a network of communication, presently named a wide area of networks (WAN). Endeavours by governments and researchers were motivated by militaristic ambitions as well as scientific curiosity.[46] For example, from the scientific curiosity standpoint, in 1960, J. C. R. Licklider independently published a research paper called "Man-*Computer Symbiosis*" which described a vision for a relationship between humans and computers, stating:

[46] Andrew L. Shapiro, (1999), "The Internet," Foreign Policy, no. 115, p.16.

"A network of such centers, connected to one another by wide-band communication lines [...] the functions of present-day libraries together with anticipated advances in information storage and retrieval and symbiotic functions…" [47]

In 1962, Licklider together with Welden E. Clark, published a second research paper called "*On-Line Man-Computer Communication,"* describing the future of greater networked capabilities:

> "Devise an electronic output surface on which both the operator and the computer can display, and through which they can communicate, correlated symbolic and pictorial information." [48]

From the militaristic standpoint, in 1962, a potential nuclear conflict between the United States and the Union of Soviet Socialist Republics (USSR) was escalating. The means of communication was through computer entity machines or servers (Nodes), communicating through Links, where a network of multiple nodes and links (Cluster) were centralized. For visual discerption, **Figure 3** show the three types of Networks. Centralized, Decentralized and Distributed, connecting the same geographical cluster of nodes.

[47] J. C. R. Licklider (March 1960). "Man-Computer Symbiosis". IRE Transactions on Human Factors in Electronics. HFE-1: 4–11.
[48] J.C.R. Licklider, W.E. Clark, (1962). "On-line man-computer communication, Proceedings of the May 1–3." Spring Joint Computer Conference, ACM, New York.

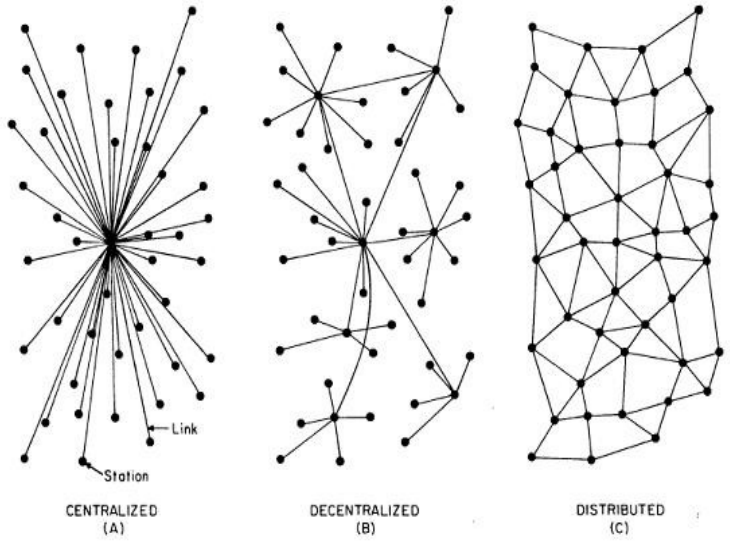


Figure 3: Types of Networks

The issue with a centralized cluster system, which was the most popular means of communication for militaristic use, was that if an enemy knocks out the centralized node, communication for the entire cluster would collapse. The decentralized, which was common for long distance telephone calls, posed a similar risk where multiple target nodes could be knocked out to collapse the entire network cluster. These two models posed a concern of military communication collapse should a nuclear strike take place. Paul Barren proposed an idea while working at RAND Corporation,[49] which he called "hot-potato routing" or distributed communication, where information from one node could jump to another effortlessly to reach intended destination even if centralized nodes or links were destroyed.[50] These structures of centralization, de-centralization and distributed have also manifested themselves today in our

[49] A think-tank founded in 1948 focused on Cold War related military utility and application research.
[50] Baran, Paul and Sharla P. Boehm, (1964) On Distributed Communications: II. Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network. Santa Monica, CA: RAND Corporation.

financial systems, centralized and de-centralized currencies and distributed ledger technology application which will be discussed further in this chapter.

In 1965, at the National Physical Laboratory (NPL) in the UK, scientist Donald Davies invented "Packet Switching", which allows a singular piece of data to be divided into packets, travel through multiple routs, and then recombine at the destination into the original piece of data. In 1967, Lawrence Roberts proposed a packet-based computer network utilizing a distributed system, known as Advanced Research Projects Agency Network (ARPANET), which was established and funded by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense and directed by Robert Taylor.[51] ARPANET was the first form of the theoretical and practical foundation of what we now know as the internet, a system of distributed communication which can segment and transmit data across multiple nodes, without disruption, if nodes or links were destroyed. The first contributions of Leonard Kleinrock in the early 1970s, which built on the previous theoretical foundations, alongside the development of the modern-day routers by Bolt, Beranek, and Newman (BBN Technologies), completed the internet. This new technology has radically and fundamentally shifted processes and outcomes in all areas of life. Particularly, it set the stage for the foundational aspects of crypto, using blockchain technologies, which we now turn to.

Crypto – Blockchain Fundamentals

At a fundamental level, blockchain is the underlying technology for which crypto products operate on. It is based on distributed ledger technology. It is a communication system which

[51] "A Flaw in The Design". The Washington Post. May 30, 2015.

enables the recording and transmission of data on an open ledger. Its purpose is the structured recording of data.[52] This is done on either a database or ledger and is typically placed into categories with "timestamped blocks" which are linked or chained mathematically to the previous block and back to the initial/genesis block.[53] There are public blockchains, which are controlled by all nodes,[54] and private blockchains where the manager has the ability to modify procedures and protocols for the transmission of data between nodes.[55] A visual representation of a basic block forming the blockchain is depicted in **Figure 4**.[56] Fundamentally, it is not the transfer of 'value', but rather is a communication system for the transmission and recording of data as discussed in this chapter.

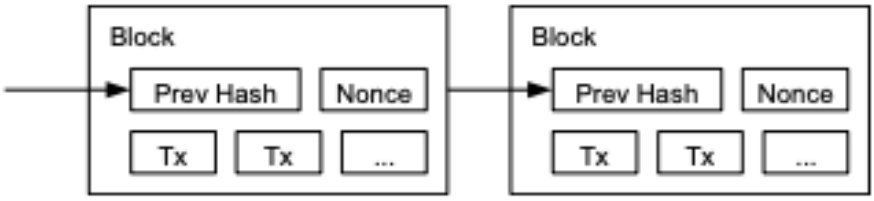


Figure 4: Satoshi Nakamoto Model of Block Chain

The schematics of blockchain utilization were presented as the 'original' Bitcoin in 2008, by an unknown entity with an alias of 'Satoshi Nakamoto,' which suggested that blockchain technology has the capabilities of transacting without a third party (i.e., a bank) by keeping transaction orders structured, while also eliminating duplicate payments in peer-to-peer distributed

[52] Law Commission. (2021). "Smart Legal Contracts: Advice to Government." Law Com No. 401.
[53] Ibid.
[54] Dominique Guegan, (2018). "The Digital World: II - Alternatives to the Bitcoin Blockchain." 16 Documents de Travail du Centre d'Economie de la Sorbonne 2; Dominique Guegan, (2017). "Public Blockchain versus Private Blockchain." 20 Documents de Travail du Centre d'Economie de la Sorbonne 3-4
[55] Karl Wüst, Arthur Gervais, (2018) "Do you need a Blockchain." Zurich: ETH, London: Imperial College.
[56] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Unpublished manuscript.

structures.[57] What is missing in Nakamoto's positive description of the blockchain and the justification for its use are claims about its safety and security and how it can help to detect or eliminate virtual currency crimes. This chapter will delve deeper into these unaddressed issues.

Blockchain technology presents challenges to conventional business operational flows because transactions which previously required a valid trusted third party, a centralized operated system, to verify transactions are now able to function without central governance, and still yield certainty and confidence.[58] The certainty and confidence, however, are limited to the transaction's expediency only. Initially, Bitcoin did not regularly trade, with the first purchase being two pizzas for 10,000 BTC on May 22, 2010.[59] As traction for bitcoin utility increased, so did its certainty and confidence. Equally as important, the hundreds of millions of users utilizing this technology do not conventionally discuss the safety of illicit transactions or security risks. Blockchain's espoused features are its transparency, depth, security, and ability to be easily audited. It is therefore an ideal system for banks permitting cooperation in one blockchain when dealing with customers' transactions. Recently, private enterprises have expressed willingness to invest in this type of technology because they find the decentralization prospects appealing and it reduces the cost of transactions since they are "inherently safer, transparent and in some cases faster".[60]

[57] Fran Casino, Thomas K Dasaklis and Constantinos Patsakis, (2019) 'A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open issues,' Vol. 36 Telematics and Informatics, p.56.
[58] Ibid.
[59] Kamau, R. (2022). "What is Bitcoin Pizza Day, and why does the community celebrate on May 9, 22." Forbes Magazine.
[60] Fran Casino, Thomas K Dasaklis and Constantinos Patsakis, (2019). "A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open issues." Vol. 36 Telematics and Informatics, p.56.

With its unique features, there are optimistic predictions that blockchain technology will store at least 10% of the world's GDP by the year 2025.[61] The certainty of blockchain in digital transactions is its most attractive feature. For example, expressing concerns over the threat of tampering with digital forensic data, Kusuma created a process for protecting forensic data and subsequently storing it using Blockchain technology.[62] However, what is pertinent is a thorough consideration by which this technology is safe from money laundering or other illicit use by cyber criminals and increasingly sophisticated criminals abusing this neutral technology.

Despite the market appeal and certainty in the underlying technology, regulators from virtually every nation became concerned about the exploitation of blockchain for illicit purposes.[63] At first, nations and legacy institutions attempted to brush off this technology and its utility, but with its growing reach and impact, ignoring it became impossible. Due to the potential dark utility growing year-by-year, including but not limited to sanction evasion, money laundering, illicit use, and darknet market operations, national enterprises and international regulators took a more hands-on approach to address this phenomenon.[64] In addition, the blockchain itself is self-regulating by the built-in consensus mechanism, which verifies blocks and stores them in the history of the blockchain. Consequently, self-executing smart contracts and complex data protection laws have become more challenging in this new digital age.[65] Given the utility of this technology, a new decentralized paradigm of finance has emerged, which we now turn to.

---

[61] Deloitte, (2018). "Impacts of the Blockchain on Fund Distribution."
[62] Renuka BS Kusuma, (2021) "Blockchain Based Digital Forensics Investigation Framework," Vol. 8 Issue. 6 International Research Journal of Engineering and Technology, p.4073.
[63] Cloud Security Alliance, (2022). "Blockchain/Distributed Ledger Technology (DLT) Risk and Security Considerations."
[64] Ibid.
[65] Blockchain: Legal & Regulatory Guidance. (The Law Society, 2nd Edition) 16.

Decentralized Finance

Decentralized finance (DeFi) is a subset of the utility of blockchain technology which is the use of the internet for sending money and all types of financial 'value' and services, even transactions without third-party interventions such as banks, payment services providers, and so on.[66] These types of transactions are "built on top of a blockchain.".[67] Jensen von Wachter, and Ross described decentralized financial applications as a "new breed of consumer-facing financial applications composed as smart contracts, deployed on permissionless blockchain technologies."[68] Decentralized financial applications have become new forms of transparent financial applications which are readily available to the public, globally, and more accessible than traditional finance due to the lack of barriers for access.[69]

Assets locked in DeFi applications' values grew from US$675m at the beginning of 2020 to US$40b by end of the first quarter of 2021 due to their rapid popularity and mass adoption.[70] The rapid growth of decentralized financial services is because anyone, anywhere in the world, with access to the internet, can utilize this service.[71] Another appealing aspect of DeFi is the fact that it is conducted without an institution or investment bank taking temporary custody of the funds. This is highly appealing to libertarians and traditional institutional cynics. Those using the service are said to have complete control of the funds and manage the transactions via the use of smart contracts which are "written into lines of code".[72]

---

[66] "Decentralized Finance (DeFI) – A New Fintech Revolution?: The Blockchain Trend Explain." (2020). Bitkom.
[67] Ibid.
[68] Johannes Rude Jensen; Victor von Wachter and Omri Ross, (2021). "An Introduction to Decentralized Finance (DeFI)." Article 150 Issue. 26 Complex Systems Informatics and Modeling Quarterly, p.46.
[69] Ibid.
[70] Ibid.
[71] Iwa Salami, (2021) "Challenges and Approaches to Regulating Decentralized Finance." Vol. 115 AJIL Unbound, p.425.
[72] Ibid.

Decentralized finance originated out of cryptocurrencies which were introduced in 2009 alongside bitcoin. [73] As mentioned earlier, a cryptocurrency is a digital currency that is not issued nor administered by a centralized regulator. It can, however, be exchanged from fiat currencies, and more recently, for other services and products which accept cryptocurrencies as a method of payment. Transactions that can be used with decentralized finance include loans, savings, investments, insurance, derivatives and increases in trade-functions as the basic functions of money, unit of account, in-store value and medium of exchange, discussed later in this chapter.[74] In effect, DeFi services are "birthing a parallel financial system,"[75] but are also facilitating the access to many parties, discussed later in this chapter and chapter 6, to the financial system and enabling access to financial services without satisfying traditional "onerous requirements as is currently the case in traditional finance" [76]

Given this threat to traditional financial systems, there are extensive issues for regulators to consider,[77] which will be outlined further in this chapter and chapters 4-6. Briefly, these issues include but are not limited to: illicit finance, taxation, oversight, and any other form of regulation applicable to 'money.' Given these emergent issues, nations have consequently flirted with Central Bank Digital Currencies (CBDC) to counteract this emergent technology and have been forced to consider stable coins, which can be "centralized, crypto-backed and algorithmic stable coins."[78] Crypto capital market considerations, utility and popularity, and the reasons for it are beyond the

[73] Salami et al (n.71).
[74] Unit of account, in-store value and medium-of-exchange
[75] Salami et al (n.71). p.425.
[76] Salami et al (n.71). p.426.
[77] Salami et al (n.71). p.426.
[78] Salami et al (n.71). p.425.

scope of this research, but in essence, there are risks associated with stability. However, as a brief example of stability issues, crypto-assets suddenly dropped in value on Black Thursday in 2020 as the COVID-19 pandemic started. Nonetheless, for the purposes of this research on illicit use, a primary problem is the vetting which traditional banks employ, or at least have the means to, to frustrate illicit use and laundering processes. As traditional oversight frameworks of financial services are in place, DeFi services so-called regulation is that of digital assets rather than financial assets.[79]

Internet Financial Utility and Application

Financial systems

Internet capabilities, utility and application were emerging phenomena near the end of the 20th century. In contrast, financial institutions, the very concept of money and the use of metal coins as a medium of exchange, unit of account or in-store value,[80] go back centuries, to the classical foundations of capitalism. A brief historical context will be given to demonstrate the evolution of traditional financial institutions and how they adapted to internet technology. Historically, bankers, persons in charge of financial lending and receiving, sat in public on formal benches.[81] While there is evidence of early banking activities[82] (for example as early as 2000 BC in Assyria, India and Sumeria, to the later eras of ancient Greece and the Roman Empire),[83]

[79] Salami et al (n.71). See discussions in chapters 4, 5 and 6 relating to regulatory oversights and confusion caused.
[80] Medium of exchange substitutes the need for barter of goods and services. Unit of account is the comparison of the value of different goods and services, costs, incomes and profits, the basis for accounting and economic decisions. In store value is used to accumulate savings, where money is the liquid reserve capable of conversion into any type of good or service.
[81] The Italian word for 'Bench' is 'Banco' which transformed into the work 'Bank'. Thus, when the 'bank' would go into liquidation, the bench would be broken, which would translate in Italian as 'Bancarotta' meaning 'Bankrupt'.
[82] Merchant trading, grain loans to farmers, record-keeping referred to in the 'Code of Hammurabi'.
[83] Rollinger, Robert, Christoph Ulf, and Kordula Schnegg (2004). "Commerce and Monetary Systems In the Ancient World: Means of Transmission and Cultural Interaction." Stuttgart, Steiner.

historians position important developments in the banking industry in the medieval and renaissance Italian cities such as Florence, Venice, Genoa and Lombardy.[84] The oldest bank in the world was the Medici Bank, founded in 1397 by the Medici family, which ceased operations in 1495. In 1472, the oldest bank still operational today was established and is called the 'Monte dei Paschi of Siena.'[85] In the 14th century, Italian bankers[86] had a working relationship with the British Crown,[87] lending money to Edward I, Edward II and Edward III, who defaulted on his loan and caused the crash of the Bardi and Peruzzi families. During this time, banks' financial transactions were done through bills of exchange, letters of credit, record-keeping and book entry, which were innovative ways, at that time. The Goldsmith bank founded in 1692, began the practice of money backed by a physical commodity, the 'gold-standard,' where the bank would lend borrowers bank notes, each with a variable value according to the terms of the agreement. These banknotes were in lieu of legal tender, gold coins and silver, and were formally issued by the Bank of Sweden in 1661.[88] The world stopped using this gold-standard in the early 20th century and now uses central backed money, fiat currency, which is not backed by a physical commodity such as gold or silver but by the government which issued the currency. The rationale of fiat currency is that it is stable since it follows principles of supply and demand, however it carries risks since it is only as good as the faith held in, as well as the stability of, the issuing government. Excessive supply of fiat currency causes inflation which devalues currency, or hyperinflation which makes it worthless. A government which is unstable and decides to print large sums of cash in order to inject the economy with money causes inflation and higher interest rates and higher default risks. That is why the

[84] Hoggson, N. F. (1926). "Banking Through the Ages." New York, Dodd, Mead & Company.
[85] Ibid.
[86] Primarily the two most powerful banking families, the Bardi and Peruzzi Famalies.
[87] Financing their military campaigns and war operations.
[88] William N. Goetzmann; K. Geert Rouwenhorst (2005). "The Origins of Value: The Financial Innovations that Created Modern Capital Markets." Oxford University Press. p. 94

stability of a government's national currency, independently as well as in relation to goods and services offered by other countries traded with, rests on the currency being stable through the Consumer Price Index not varying substantially and the currency's Purchasing Power performing all its functions namely; unit of account, medium of exchange and in-store value.

The growth of utility in deposits, credit and lending was due to industrialization in the 18th and 19th century. Corporate structures, large scale manufacturing and export-led growth prompted financial institutions to evolve and expand services offered, through various banking institutions performing different functions.[89] Legal tender is still fiat currency, but the way such currency is delivered, held, and received changes and continues to do so from traditional forms of physical cash, to digital representations of value through mobile payments, to credit cards, and internet based payments and, more recently, decentralized payment systems which do not use fiat currency but cryptography to create new digital currencies known as cryptocurrencies. Although emergent forms of digital representations of value change and evolve, the means of digital financial interaction are currently done using the internet. The financial systems now use internet finance, which includes payment, loans, security purchase, offering funds, settlement, peer-to-peer (P2P) lending, crowdfunding and electronic cash. Internet finance itself is a combination of information technology, big data and cloud computing. This concept of finance and financial interaction enhances and promotes potential financial inclusion, assuming internet is available.

[89] Central Banks, Commercial Banks, Merchant/Investment Banks, Savings Banks, Cooperative Banks, Mortgage Banks, Giro banks and National Savings Banks, Credit Unions, and Islamic Banks

Substantively, financial inclusion increases access to financial services at affordable and sustainable costs by individuals or low- income companies.[90] Financial technologies (FinTech) provide such opportunities and the potential to reach underserved individuals and communities through a range of products and services, including mobile money and e-wallets, person-to-person (P2P) lending, equity crowdfunding, alternative credit scoring, cross-border remittances, digital KYC processes and regulatory technology (RegTech).[91] As financial and technological evolution takes place, those who are left behind bear the brunt of not benefiting, and, worse, elevated poverty takes place due to financial exclusion.[92] While the introduction of new technologies can have a significant impact on developing countries in terms of improvements in living conditions,[93] there are practical barriers too with regard to implementation. Notably, infrastructure,[94] development capacity,[95] policy and regulation[96] as well as institutional governance.[97]

[90] Muzigiti, G., and O. Schmidt. (2013). "Moving Forward." Bonn: D+ C Development and Cooperation.
[91] D.W. Arner, J. Barberis and R. P. Buckley (2016), "The Evolution of FinTech: A New Post-Crisis Paradigm?", Vol. 47 Issue, 4 Georgetown Journal of International Law, p.1271.
[92] Shiimi, I. (2010). "Financial Inclusion –An Imperative Towards Vision 2030" Speech at the Governor of the Bank of Namibia, at the Governor's Annual Address, Windhoek.
Vision 2030." Annual address by the Governor of the Reserve Bank of Namibia. Windhoek,
[93] Muzigiti, G., and O. Schmidt. (2013). "Moving Forward." Bonn: D+ C Development and Cooperation.
[94] Backbone hard and soft infrastructures like electricity, high-speed reliable internet connectivity, and digital skills. See "Technology is the key to transforming least developed countries. here's how" (2022) World Economic Forum.
[95] Bubou, Gordon. (2009). "Technology Development Capacity Building: Critical Issues of Strategic Management of Research and Development (R&D) and Innovation. "
[96] Normative working groups. See Kavanagh, C. (2019) "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace.
[97] World Economic Forum, (2018) "Agile Governance: Reimagining Policy Making in the Fourth Industrial Revolution."

The emergence of Fintech and alternative payment products has redefined the role of conventional financial intermediaries, delivery of services, and compliance.[98] **Figure 5** shows the payment aspects of financial inclusion (PAFI) fintech wheel, based on a 2016 CPMI-World Bank report.[99]

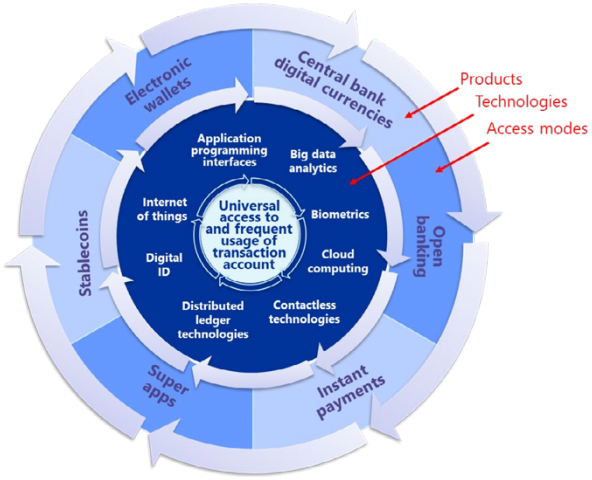


Figure 5: Payment Aspects of Financial Inclusion (PAFI).
Source: CPMI-World Bank.

These types of technologies address the arguably core problem of financial inclusion, borrowers' cash flow mismatches. Illustrations of such mismatches can be seen in both developing countries, as well as developed, whereby craftspeople and small business entrepreneurs have a need to manufacture, produce, and deliver products while competing in the market, but lack the cash flow to purchase raw resources, hire staff, and rent spaces. Underwood commented on the utility of Fintech and its role in financial inclusion, stating:

> "Distributed ledger technology is expected to revolutionize industry and commerce and drive economic change on a global scale because it is immutable, transparent, and

[98] Haddad, C., & Hornuf, L. (2018). "The emergence of the global fintech market: Economic and technological determinants." Small Business Economics, Vol. 53 Issue. 1,81–105.
[99] Committee on Payment and Market Infrastructures and World Bank (2020) 'Payment Aspects of Financial Inclusion in the FinTech era.'

redefines trust, enabling secure, fast, trustworthy, and trans-parent solutions that can be public or private. It could empower people in developing countries with recognized identity, asset ownership, and financial inclusion" [100]

Like all payment structures, fintech safeguards its processes through Digital Identification. Digital ID refers to a set of electronically captured and stored attributes and credentials that can uniquely identify an individual or legal person and is used for electronic transactions.[101] A person's digital identity may be composed of a variety of attributes, including biometric data (fingerprints, iris scans, handprints) and biographic data (name, age, gender, address) as well as other features related to what the person does or what is known about them. Digital ID is a substantial consideration in technologies and money/cyber laundering, which will be elaborated on further in subsequent chapters.[102]

Conventional Money-Laundering

According to Jeffery Robinson, "Money laundering is called what it is because that perfectly describes what takes place – illegal, or dirty, money is put through a cycle of transactions, or washed, so that it comes out the other end as legal, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income."[103] Money laundering, where the conversion of illicit proceeds from criminal activity to legitimate proceeds, generally

[100] Underwood, S. (2015). "Blockchain beyond Bitcoin." Communications of the ACM, Vol.59 Issue. 11, p.15.
[101] Mittal, A (2018). Catalog of Technical Standards for Digital Identification Systems, World Bank Group.
[102] The occurrence of identity theft, where criminals acquire monetary value by stealing another person's details, like a credit card or account number, is also a risk associated with digital ID.
[103] Robinson, J. (1997). "Laundrymen: Inside money laundering, the world's third-largest business." W Norton. p.3

revolves around a three-stage process.[104] The first is placement, where illicit funds are generally used to make a purchase in the legitimate and/or illegitimate economy. The second is layering, where through repeated transactions, the source(s) of the funds are obfuscated. The third and final stage is integration, where the funds are re-integrated into the legitimate economy. This three-step process is aimed at 'washing', or 'cleaning', illicit proceeds and can be by a range of actors, from small-time drug dealers, nefarious actors, sophisticated criminal enterprises or corrupt heads of state. The volume of traffic, scale of operations and typological diversity cannot all be discussed in this thesis, but rather classified into generic techniques.[105]

Beare classified money laundering into four typologies. The first is Simple-limited, where laundering occurs with relatively small volumes of transactions and small cash-based transactions.[106] The second is Simple-unlimited where large volumes of cash are laundered through small volumes of transactions through companies with unclear resources, materials and service costs. The third is Serial-domestic use large volumes of transactions for large amounts of proceeds through a network of multiple banks. The fourth is Serial-international use large volumes of transactions, large amounts of proceeds as well as international services, where funds are channeled through big banks in North America and Europe.[107] These generic typologies are not a closed list of patterns. While each typology varies, the following discussion will focus on what can be described as 'conventional' money-laundering methods and their characteristics, specifically cash money laundering, legal entities, third-party, financial and non-financial

[104] This is not a closed list. An example would be tax evasion where money is placed from one country to the other, as this is a 'legitimate' source of funds, whereby failing to disclose income on tax returns, laundering is in-effect done.
[105] "[I]t is impossible to identify all the laundering possibilities - from cults to marathons and beyond" Margaret Beare (2015). "Criminal Conspiracies - Organized Crime in Canada." Oxford University Press, p.243-44
[106] Can also be used for "Smurfing" where large proceeds are broken into smaller proceeds to evade detection.
[107] Margaret Beare (2015). "Criminal Conspiracies - Organized Crime in Canada." Oxford University Press.

instruments. I am not intending to provide detailed analysis of such conventional methods,[108] but rather an overview, and will then move on to emerging methods – which are the focus of this thesis.

Traditionally, proceeds from criminal activities were cash. The notion of 'dirty' cash/money stemmed from the practice of an anonymous paper trail. Predicate offences such as drug, human, and/ or firearms trafficking were and are primarily cash-intensive businesses.[109] Likewise, legally established corporations, non-profit organizations, shell companies and trusts are all methods conventionally and presently used for money-laundering. The primary advantage of using legal entities, whether off-shore or national, for money-laundering is concealment of beneficial ownership and layering of illicit funds.[110]An example of where shell-companies can be used for illegitimate means is where real estate is purchased using illicit funds, then resold to a criminal's shell corporation, and then resold again to an innocent third party,[111] at the original purchase price or higher and then such corporation dissolved or sold.[112]. Non-profit corporations and charitable organizations or legitimate operating corporations are also used to camouflage illicit

[108] Conventional methods are cash-based money laundering, legal entities, third-party and financial and non-financial instruments.

[109] The proceeds, were either smuggled, converted or structured to provide a mask of legitimacy. Cash smuggling was traditionally aimed at moving the proceeds as far away from law enforcement and the place of criminal origin, for example through cargo ships, car tyres, airplanes, dead bodies, United Parcel Service (UPS) and Federal Express (FedEx). Cash conversions occurred where some illicit activities did not generate the cash required for placement into a financial system, the illicit proceeds, foreign currency or fiat, were used to obfuscate the paper trail. Cash structuring/smurfing is an evolution of the two preceding methods, to overcome monetary thresholds for cash deposits that might give rise to possible suspicion. Cash structuring involves depositing funds that fall below the prescribed thresholds, or purchase bank cheques/bank drafts, and multiple deposits of the funds into multiple branches of the bank. Likewise, opening different accounts and using third parties, such as smurfs, were used to make multiple deposits. The cash-based methods are utilized by criminals so as to avoid reporting, detection/investigation and record-keeping requirements.

[110] While shell companies may, of course, have legitimate uses, they can also be used for illegitimate means.

[111] Money-laundering Integration where the funds are now mixed in the economy and 'washed' of illicit trace.

[112] This not only poses an effective layering method but also makes it difficult for law enforcement to access records and determine the identity of the beneficial owner. Such difficulties are enhanced given the diversity of multi-jurisdictional options for trusts and corporations to be owned by one or more trusts or corporations in other jurisdictions

funds derived from another source of illegal activity whereby such funds are channeled through the legally established and operating entity.[113] the trustee to transfer assets when receiving notice of law enforcement inquiry.[114]

Third-party money laundering involves the use of 'gatekeepers' (such as lawyers or accountants) and/ or 'nominees' (such as agents, close associates or family members) for the benefit of the beneficial owner. The FATF has recognized gatekeepers to be "essentially, individuals that 'protect the gates to the financial system' through which potential users of the system, including launderers, must pass in order to be successful."[115] As "those professionals, such as lawyers, accountants, company formation agents, auditors, and other financial intermediaries who can either block or facilitate the entry of organized crime money into the financial system."[116] Extensive work has been done on specifically this subject matter of lawyers as facilitators of money laundering.[117]

[113] While such entities are effective at placement, layering and integration of illicit proceeds of crime, other entities, such as specific trusts, are designed to safeguard against enforcement mechanisms. See Lilley, P. 2006. "Dirty dealing: The untold truth about global money laundering, international crime and terrorism." 3rd ed. London: Kogan Page.
[114] Known as 'Flee Clauses' where a triggering event transfers assets and administration to a 'safe' jurisdiction. Baker, R. W. (2005). "Capitalism's Achilles Heel: Dirty Money and How to Renew the. Free-Market System." p. 37.
[115] FATF (2010) Global Money Laundering & Terrorist Financing Threat Assessment A view of how and why criminals and terrorists abuse finances, the effect of this abuse and the steps to mitigate these threats, p. 44
[116] Moscow Communiqué 1999 para. 7
[117] Benson, K. (2020). "Lawyers and the Proceeds of Crime: The Facilitation of Money Laundering and its Control" (1st ed.). Routledge.

Financial and non-financial instruments' money-laundering include gambling, securities,[118] and insurance policies,[119] which are all industries by which laundering has capitalized on. Gambling through casinos, horse racing and lotteries have traditionally been utilized successfully to wash illicit proceeds from criminal activities.[120] This can be done by using illegal funds to purchase casino chips, which are then traded in for cheques or casino cash.[121] Horse racing and lotteries also work in a similar way where illicit proceeds are used to purchase tickets which can be claimed back or by collecting a cheque from the track while also avoiding taxes on the winnings,[122] as well as purchasing winning tickets from the winners as they arrive to a lottery office.[123]

21st Century Money Laundering Technologies and New Frontiers of Money Laundering

With the advent of the internet, and the communication pathways provided through it, 21st century criminals are now even more equipped with sophisticated channels and the ability to coordinate more effectively and profoundly to not only maximize predicate offences but also to enhance laundering operations. The mechanics and extent of such capitalization through crypto

[118] The securities market has provided an attractive hub for launderers looking to layer and integrate the illicit proceeds and avoid traceability by purchasing and reselling a given security. See Reuter, P., and E. M. Truman. (2004). Chasing dirty money: The fight against money laundering. Washington, DC: Peterson Institute for International Economics. p.29

[119] With regards to insurance policies, illicit funds can be used to fully pay a premium and its corresponding fees and penalties, and redeem the full policy at a discount, which is a useful method for integration. See Lawrence, S. (2008). Money laundering and the insurance industry. AIR insights. p.82

[120] FATF (2009) "Report on Vulnerability of Casinos and the Gaming Sector." p. 9

[121] This type of gambling has been exacerbated by the evolved nature of online casinos and gambling, which have multijurisdictional characteristics. See Pillai, K., and A. Julian. (2008). Prevention of money laundering legal and financial issues. New Delhi: The Indian Law Institute. p. 133

[122] Reuter, P., and E. M. Truman. (2004). "Chasing dirty money: The fight against money laundering." Washington, DC: Peterson Institute for International Economics. p.31

[123] Ibid. p.29

products will be discussed further in chapters 5 and 6, but it is necessary first to provide a brief discussion of the internet's money laundering capabilities. There have been a variety of reports internationally which identify unusual transactions using virtual currencies and their blockchain wallets.[124] Virtual currencies such as bitcoin and the use of a mixer (such as tornado cash) of virtual currencies have presented significant opportunities for laundering practices, where ChipMixer laundered $3 billion worth of bitcoin since 2017.[125] Thus, this section will consider crypto laundering capabilities, followed by crypto evolutionary techniques and lastly, cases of crypto laundering typologies.

Crypto Money-Laundering Capabilities

Crypto's money laundering capabilities was apparent as early as 2014, with the arrest of Charlie Shrem for laundering $1 million through Silkroad.[126] Not only money laundering, but evolving typologies of ponzi schemes and cybercrimes, emerged, including US$350 million stolen from Mt. Gox between 2011-2014,[127] and US$5 million stolen from Bitstamp in 2015.[128] As recently as the 4th Quarter of 2019, cryptocurrency financial fraud was spearheaded by Ponzi schemes.[129] On April 25, 2019, the Attorney General in New York filed a complaint against Bitfinex and Tether's parent company for an alleged loss of US$850 million in assets to Crypto

[124] Hossein Nabilou (2020) The dark side of licensing cryptocurrency exchanges as payment institutions, Law and Financial Markets Review, Vol.14 issue.1, p.39-47; Robert Stokes (2012) Virtual money laundering: the case of Bitcoin and the Linden dollar, Information & Communications Technology Law, Vol.21, issue.3 p.221-236; Chainalysis (2022) Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity.
[125] United States of America v. Mingh Quoc Nguyen, 14/03/2023, United States District Court for the Eastern District of Pennsylvania criminal complaint, Case no. 2:23-mj-00528
[126] Kyle Russell, (2014). Meet the "Bitcoin Millionaire" Arrested for Allegedly Helping Silk Road Launder $1 Million, Bus. Insider.
[127] Todayonline (2014) 'Website of Bitcoin exchange Mt Gox offline.'
[128] Zack Whittaker (2015). "Bitstamp exchange hacked, $5M worth of bitcoin stolen"
[129] Ciphertrace. (2020) 'Cryptocurrency Anti-Money Laundering Report, 2019 Q4', Cipher Trace Cryptocurrency Intelligence, p.4.

Capital based in Panama. For the year 2019, the total losses in cryptocurrencies due to various types of cybercrimes were estimated to be US$4.5 billion, being a significant increase from 2018 (533%).[130] Given the manner and degree of evolving crypto laundering and cyber-based crimes, there is a need for regulation and security measures if crypto assets are going to continue to be a part of stable and healthy financial transactions.

The need for regulation is now apparent; however, that was not always the case. As recently as 2014, money laundering in crypto was not truly a concern for regulators. According to Paesano, the only case of concern at that time was Silk Road,[131] a darknet marketplace. [132] Although the Silk Road bitcoin issue was isolated at the time, the US Department of Justice subsequently auctioned recovered bitcoin to receive approximately US$50 million.[133] This isolated case demonstrates how damaging the problem with money laundering in cryptocurrencies can be. If an isolated incident can cause losses of US$50 million, the losses in several incidents of money laundering can be excessive, as will be demonstrated later in chapter 6. At the time, a working group on money laundering in crypto was established by INTERPOL and Europol. More recently, however, ML concerns have become much more prominent in the crypto sphere.[134]

[130] Ibid.
[131] An amazon-prime style darknet marketplaces openly exchanging narcotics, and other forms of criminal activity in the form of weapons, sexually exploitive materials, organs, etc.
[132] Federico Paesanao (2021), 'Cryptocurrencies and Money Laundering Investigations,' BASEl Institute on Governance, Quick Guide Series, 01.
[133] Ibid.
[134] Federico Paesanao (2021), 'Cryptocurrencies and Money Laundering Investigations,' BASEl Institute on Governance, Quick Guide Series, 01.

As the cryptocurrency market expanded rapidly,[135] in 2013, the market was US$1.5 billion and by 2018, the Cryptocurrency market increased to US$795 billion. Before 2010, Bitcoin was worth US$0.8 per Bitcoin and by 2017, a Bitcoin was worth US$17,000.[136] Ordinarily, the drastic and rapid expansion and growth of Cryptocurrencies or any item of monetary worth would be the subject of optimism. However, there is a significant downside, as Xie pointed out: "While Cryptocurrencies have campaigned for revolutionizing financial transactions, the Crypto-market is plagued by nefarious minds, fleecing investors in frauds and Ponzi schemes."[137]

Over the last few years, Bitcoin has received significant criticism and has been called "public enemy number one for everything from financing terrorism to drug dealing with money laundering."[138] Although money launderers and other cybercriminals are attracted to Bitcoin due to its pseudonymity, Silk Road proved that money launderers could be caught on Blockchain distributions because each of the transactions are visible using traditional law enforcement techniques and open source intelligence. This, however, is not a one-size fits all statement, as emerging techniques have effectively operated with impunity. Where even if monies were captured, and criminals, some of which have not been prosecuted, have been identified, the damage to the victims nonetheless cannot be undone, as will be demonstrated in chapters 5 and 6. The transparency of the Blockchain ledger distribution led to the identification of the launderers in the Silk Road scandal. However, the lack of centralization makes prosecution difficult because of the

[135] Rain Xie, (2019) 'Why China had to "Ban" Cryptocurrency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China.' Vol.18 Issue.2 Washington University Global Studies Law Review, p.457
[136] Ibid.
[137] Rain Xie, (2019) 'Why China had to "Ban" Cryptocurrency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China.' Vol.18 Issue.2 Washington University Global Studies Law Review, p.1
[138] Gaspare Jucan Sicignano, (2021) 'Money Laundering Using Cryptocurrency: The Case of Bitcoin!' Vol.7 Issue.3 Athens Journal of Law, p.253.

high-velocity cross-border nature of cryptocurrency transactions.[139] The criteria by which a certain currency's attraction to bad actors can be narrowed down to a currency's level of perceived anonymity, its usability, security, acceptance in the marketplace, reliability, and overall volume.[140]

With respect to attraction to bad actors, the US Department of the Treasury assessed the risk of money laundering in cryptocurrencies in February of 2022.[141] According to this report, money laundering by cybercriminals exceeded US$4.1 billion for the year 2020. This number reflected an increase in ransomware attacks in which both US businesses and citizens were held hostage for sensitive data in exchange for payment. The COVID-19 pandemic did not deter the increase in money laundering attacks over the Internet.[142] It appears that money laundering increased exponentially during the pandemic because criminals, like everyone else, had to find innovative methods to generate revenue.[143]

Regarding the illicit use, a 2019 Congressional Research Report, acknowledged that money laundering was a key feature of virtual currencies.[144] Indeed, for the past ten years, federal prosecutors and security regulators have dealt with many cases involving unlawful activities using virtual currencies. In particular, federal prosecutors filed charges involving money laundering activities using virtual currencies.[145] Charges have been brought against marketplace creators

[139] Ibid, 259-260.
[140] Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats," The RAND Corporation, 2019, available at https://www.rand.org/pubs/research_reports/RR3026.html.
[141] Department of the Treasury. (2022). 'National Money Laundering Risk Assessment.' National Money Laundering Risk Assessment (treasury.gov).
[142] Ibid.
[143] Ibid.
[144] Congressional Research Service, (2019) 'Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals.' CRS Report
[145] Department of Justice. (2022). Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency.

online who permitted their services to be used as a means of exchanging virtual currency for unlawful goods and services.[146] The validity or enforceability of a contract between parties in an unlawful transaction is therefore called into question on many levels. Despite its innovation, virtual currency arguably entails too many high risks and its proper regulation for market profit-driven utility should be secondary to identifying methods for making these transactions safer. Currently, virtual currencies have appeals that match the needs and desires of cybercriminals, privacy and cross-border reach. The peer-to-peer functions, privacy wallets and mixers, and the nature of some virtual currencies together with the lack of borders, ensures that cybercriminals find these payment options useful for money laundering and financing/profiting from illicit operations. Moreover, criminals may carry out these transactions pseudonymously, obfuscate and mask identities, and therefore significantly reduce the risk of getting caught.[147] The following discussion focuses on some of these obfuscation methods.

Crypto Laundering Evolution

During a bitcoin transaction, a person uses a wallet which contains one or more bitcoin addresses. Wallets and addresses are not linked to a name or an identity, which enhances anonymity.[148] However, all bitcoin or virtual currencies transactions occur on the Blockchain, which is a public ledger of information of such transaction, and therefore they are traceable.[149]

---

[146] Department of the Treasury. (2022) 'National Money Laundering Risk Assessment.' National Money Laundering Risk Assessment (treasury.gov).

[147] European Parliament. (2018). 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses. Study for the TERR Committee.

[148] De Jong: 'The technology behind bitcoin makes it possible to transfer funds anonymously. The risk of money laundering is thereby increased.' R.J. de Jong (2017), 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', TBS&H, no. 1, p. 5. See also A.B. Schoonbeek, W.M. Shreki and M.T. van der Wulp, (2017) 'Bitcoins, witwassen & integriteitsrisico's', Tijdschrift voor Compliance, p. 95 and Nieuwsbrief banken (2014), 'DNB warns banks and payment institutions of integrity risks with virtual currencies.'

[149] http://walletexplorer.com is a website used to see all transactions that have been conducted with a particular wallet, and in theory, can trace when a particular virtual currency came into existence.

Unlike traditional cash laundering, which offers an incentive of leaving virtually no 'paper trail', virtual currencies do not have the logistical storage problems, and transactions can be done in a matter of seconds, anywhere in the world, without identification information shared compared to bank transactions which happen in traditional financial markets. Darknet markets pose a different opportunity which utilizes virtual currencies. Trading in darknet markets like DeepDotWeb, which acted as a gateway to AlphaBay, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D's, Wall Street Market, and Tochka Market, have used bitcoin currency,[150] and the majority of goods purchased on the dark-web market places are illegal.[151] A bank account is required in order to purchase and sell bitcoin through bitcoin exchange offices[152] or bitcoin exchanges.[153] When bitcoins are sold, the equivalent value is transferred to the bank account by the exchange office or exchange, whereby the identity of the account holder is known to the bank, which then triggers a series of legal obligations related to compliance, due diligence and beneficial ownership requirements, which will be discussed in chapters four and five. This, however, poses a lack of anonymity, which was the original intent and *modus operandi* of decentralized virtual currencies. This interplay between the banks and virtual currencies has created a market for middlemen, who accept the cash-out for their own account.[154] These traders have a large number of bitcoins in their possession, large volume exchanged, and large amounts transferred to their bank account from exchanges or exchange offices. The connection between the

[150] Press Release, (2019) "Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," U.S. Dept. of Justice.
[151] Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. Survival, Vol. 58 Issue.1, p. 15-22.
[152] Bitcoin exchange offices buy and sell bitcoins for their own account and risk, whereby they issue purchase and sale prices against which bitcoin can be bought or sold from them. Examples of such offices are Bitonic and BTCdirect.
[153] Bitcoin exchanges are marketplaces where parties can buy and sell bitcoins to and from one another, acting as an intermediary to bring together supply and demand. Examples of such marketplaces (exchanges) are Kraken and BitStamp.
[154] These middlemen are bitcoin traders who purchase/sell bitcoins for cash on a commercial basis, from their own account, and risk.

trader and the seller of a bitcoin is the surface web[155] or dark web/bitcoin platforms. From a physical interaction scenario, the seller transfers bitcoins to the wallet of the trader, and the trader gives the market value, or placed value, to the seller in cash. From a non-physical scenario, the trader utilizes surface websites to offer to purchase bitcoins at set rates (exchange rates) and within set limits. The cost of using a trader is higher than going through exchange offices or exchanges,[156] but it is offset by the anonymity protection offered through traders.

Likewise, the use of bitcoin mixers,[157] where bitcoins are exchanged for other currencies against the payment of a commission to the mixer,[158] has been said to "render your bitcoins completely untraceable, even to the most persistent forensic investigator".[159] Van Wegberg, Oerlemans and Van Deventer explain that "Bitcoin mixing services are services that aim to disassociate bitcoins from their often-criminal source."[160] Since usual blockchain transactions are stored on public blockchains, the user of mixers obscures the identity of ownership of the select currency in question, by working through a Tor network,[161] in jurisdictions with little to no judicial oversight. [162]

[155] Surface web is the legitimate use of web activity, such as localbitcoins.com
[156] A trader can charge 7%-15% of the transaction value while exchange offices charge approximately 0.3% as shown by criminal investigations money laundering teams of FIOD Haarlem and FIOD Zwolle and by the Central Netherlands Police Force. See also the press release on the website of the Dutch tax authorities, '10 arrests in international bitcoin investigation', 20 January 2016
[157] Bitcoin mixers such as Bitlaundry are virtual solutions run by unknown users where users mix their virtual currencies with other users in order to preserve privacy and obscure the ties between bitcoin addresses and real-world identities.
[158] Whether mixing on the Clearnet or on the hidden web using TOR. See J. Redman, (2016) 'Tumbling Bitcoins: A Guide Through the Rinse Cycle.'
[159] See https://bitlaunder.com/launder-bitcoin
[160] R.S. van Wegberg, J.J. Oerlemans and M.O. van Deventer (2017), 'Bitcoin Money Laundering: Mixed Results? An explorative study on money laundering of cybercrime proceeds using Bitcoin', Journal of Financial Crime, p. 2.
[161] Tor is a free and open-source software which enables anonymous communication
[162] S. Eikelenboom and J. Dobber, (2017) 'Bitcoin is reservemunt van de onderwereld geworden', Het Financieele Dagblad.

Similar to the use of mixers, the use of Wasabi Wallets via Tor networks to completely conceal identity ownership presents further avenues for virtual currency laundering. Wasabi Wallets use a method called "CoinJoin," which is different from mixers in that it combines transactions from multiple users into one transaction with multiple inputs and outputs, thus making it difficult for outside parties to associate payments of parties and recipients with their actual origin. The *modus operandi* is that the more users CoinJoin has, the more anonymous and reliable it becomes. It adds a layer of "block filters" that downloads data blocks, effectively obfuscating which wallet address investigators should focus on. Europol recognized that such Wasabi wallets are "very effective decentralised Bitcoin mixer with many privacy-focused options [and] provides possibly the most convenient and secure way to mix Bitcoins."[163] Since such wallets are open-source and non-custodial, they are not a service that holds users' funds since users keep wallet seeds and private keys locally, where even the administrators and developers of Wasabi have no way of accessing a user's balance or funds. Blind signatures, like ring and schnorr signatures discussed further in chapter 5, ensure that even Wasabi operators cannot link inputs and outputs. This, arguably, is outside the scope of EU 5AMLD, which will be further scrutinized in chapter 4. Likewise, in terms of virtual currency and asset laundering typologies, Darknet Marketplaces, Unregistered Foreign-Located Money Service Providers (MSB), Virtual Assets Service Providers (VASPs), Universal Access Device (UAD), Unregistered Peer-to-Peer (P2P) Exchangers, Peel-Chain, Chain/Channel Hopping, the Silk Road, Cold & Hot Wallet Storage, and CVC Kiosks/Automated Teller Machines will be further scrutinized in detail in chapters 5-6. The following examples illustrate different means of laundering via crypto, demonstrating the

[163] Europol, The Hauge (2020), Intelligence Notification No. 08/2020, Cyber Bits, European Cybercrime Centre EC3.

sophistication of the laundering capabilities and the quasi-integration with conventional financing methods.

Crypto Laundering Evolving Typologies

Gate.Io Hack

In April 2018, North Korean hackers accessed a crypto exchange through an email phishing campaign. This led to an employee's emails being compromised along with corresponding wallet keys, and the theft of US$230m consisting of Bitcoin, Ethereum, Litecoin, Dogecoin and various other altcoins. The criminals then laundered the stolen cryptocurrencies through automated scripts and over-the-counter brokers to exchange the stolen cryptocurrencies into fiat currencies. The hackers employed obfuscation typologies like peel chains, which sends extensive amounts of cryptocurrencies to wallets that the hackers' control at multiple exchanges. [164] Subsequently, the U.S. Department of Justice's civil forfeiture action against two Chinese nationals showed that their help was needed to cash out stolen cryptocurrency into fiat currency worth US$100 million on behalf of Pyongyang.[165] This method of laundering is relatively unsophisticated, as the focus is on speed of conversation of assets to fiat as fast as possible as opposed to obfuscation. Given blockchain forensics capabilities to trace the funds, regardless of their speed of movement, criminals have become more aware of obfuscation necessities.

[164] This is done to minimize suspicion from exchange compliance personnel and avoid suspicious transactions red flags.
[165] U.S. Department of Treasury (2020), press release, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group."

Ryuk Ransoms

2018 was the first appearance of these types of ransom hacks.[166] These hacks are from an organized and high-level community of hackers who focus primarily on high-value targets to encrypt files until ransom is paid. The ransom utilizes large sums of cryptocurrencies, $4million Bitcoin as of 2021,[167] to be used on another blockchain such as Ethereum. Generally, blockchains are not interoperable.[168] However, through decentralized cross-chain bridges, decentralized custodians can exchange one crypto asset for another, and they can be used as collateral to borrow through lending protocols. Decentralized cross-chain bridges, such as Ren, allow for assets on a blockchain to be represented as a token on another blockchain, much like regulated exchanges offering this service.[169]

Dragonex Hack

In March 2019 a similar phishing campaign was carried out against DragonEx, a Singapore exchange. This resulted in approximately US$7m stolen including several cryptocurrencies. Relative to the other examples, this is small in value. However, the sophistication of the laundering technique used in this case is remarkable. More emphasis was placed not on speed, but obfuscation. The hackers held the stolen assets in a single unhosted wasabi wallet for approximately two months and then deposited the assets into a mixing service over a period of several months. In doing so, they were able to cash out stolen cryptocurrencies into fiat during a high exchange rate period in August 2020, while conducting layering transactions to divide and recombine stolen Bitcoin to

[166] Constantin, Lucian (2020). "Ryuk ransomware explained: A targeted, devastatingly effective attack". CSO Online. International Data Group.
[167] Goodin, D. (2019) New ransomware rakes in $4 million by adopting a "big game hunting" strategy, Ars Technica.
[168] For example, Bitcoin cannot be transferred to an Ethereum account and used on a decentralized exchange.
[169] Centralized exchanges and custodians have extensive obligations for KYC/transaction monitoring/reporting/seizure while decentralized applications do not.

conceal the sources of funds. Not only did they employ sophisticated layering techniques, but they also deployed a buy-and-hold strategy in awareness with crypto markets to maximize high potential cash outs.

KuCoin Hack

In September 2020 a breach in the cybersecurity of a Singapore based crypto exchange resulted in theft of more than US$280m consisting of Bitcoin, XRP, Litecoin, Tether, Chainlink, and Ocean Protocol. The criminals used a series of mixers and decentralized finance blockchain services to mix and wash the stolen assets. These techniques are relatively more sophisticated and solve a common problem for criminals, namely, the avoidance of frozen tokens at any point in time. The solution, as in this case, is to convert the stolen cryptos into native blockchain assets, such as Bitcoin or Ether, since they are not issued by a central authority and cannot be unilaterally frozen. Thus, they are outside the reach of authorities. In this case, three professional mixers were utilized. Wasabi Wallet and ChipMixer to wash the stolen Bitcoin, and Tornado Cash to wash the stolen Ethereum. From a practical level, the user(s) in this case deposited stolen cryptocurrency in Tornado with various increments of equal value held in a single address. Positively linking a deposit with a withdrawal becomes challenging for law enforcement, and the longer the user(s) keeps the funds in the DeFi applications, the greater pseudonymity is achieved. What is unique about Tornado Cash is its utility of a cryptography called "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" to obfuscate source of funds through the smart contracts, effectively breaking the on-chain link between source and destination.[170] The sophistication of these laundering techniques by the Lazarus Group, a cybercrime group, expressed an appreciation

[170] In doing so, user(s) can leave out third parties such as custodians or exchanges that may have knowledge of the transactions or who can steal/freeze the funds.

for evolving capabilities of this technology and the creativity associated with it. It is noteworthy, then, that the U.S. Treasury has recently sanctioned Tornado Cash on the grounds that it "has been used to launder more than $7 billion worth of virtual currency since its creation in 2019."[171]

Crypto Terrorism Financing

Terrorist enterprises have also been known to leverage cryptos. Al-Qassam Brigades (Hamas's military wing) advertised several requests for bitcoin donations to support violent causes on official websites and social media – claiming that these styles of donations are untraceable. In their publications, they provided instructional videos on how to make such donations.[172] Al-Qaeda and its affiliates successfully operated a bitcoin money laundering network through social media applications and encrypted messages applications, where in some cases, they posed as charities,[173] to be "an independent charity organization that is benefiting and providing the Mujahidin in Syria with weapons, finical [sic] aid and other projects relating to the jihad. You can donate safely and securely with Bitcoin."[174] Lastly, ISIS affiliates deployed sophisticated techniques of marketing fake personal protective equipment, to leverage the covid-19 pandemic,[175] where ISIS facilitators "sent more than $150,000 to shell companies, including companies in Turkey that were fronts for ISIS, and attempted to travel to Syria to join ISIS"[176] where "more than a dozen fraudulently obtained credit cards to purchase approximately $62,000 in Bitcoin, which she converted back to

[171] U.S. Treasury sanctions notorious virtual currency mixer Tornado cash (2022) U.S. Department of the Treasury. Available at: https://home.treasury.gov/news/press-releases/jy0916.
[172] The United States Department of Justice. (2020). "Global Disruption of three terror finance cyber-enabled campaigns."
[173] Ibid.
[174]United States of America v. Facemaskcenter.com and four facebook pages. United States District Court for the Central District of Colombia (May 8, 2020) Civil Complaint, Case 1:20-cv- 02142-RC. p.15
[175] Ibid.
[176] United States of America v. Facemaskcenter.com and four facebook pages. United States District Court for the Central District of Colombia (May 8, 2020) Civil Complaint, Case 1:20-cv- 02142-RC. p.5

fiat currency to send to the shell companies."[177] Similar complaints emerged of $35,000 ISIS funded "crowdfunding network used cryptocurrency, Bitcoin wallets, GoFundMe, and PayPal to collect and raise blood money to support ISIS."[178] **Appendix I** portrays the terrorist-related advertisements and solicitations for Cryptos to donate anonymously.[179]

Crypto Ransomware and Extortion

Ransomware is particularly concerning and unique because it can make the victim an unknowing participant in a money laundering scheme. Ransomware is malicious software that attacks and immobilizes the files and data of a computer blocking the user's access to the data.*[180]* Decryption equipment is denied to the user until a ransom demand is paid. When a ransomware attack occurs, the assailant will typically demand that payment is made through cryptocurrency because this payment method is difficult to track.*[181]* As acting U.S Attorney for the northern district of Colombia stated "Cyber criminals are employing ever more elaborate schemes to convert technology into tools of digital extortion"*[182]* The United States Secret Service expressed further concerns with these crypto-enabled transnational crimes.*[183]* For visual representation, **Appendix II** demonstrates typical extortions of ransomware payments demanding crypto for payment.

---

[177] Ibid.
[178] United States Department of Justice. (2020) Press release, "Four defendants charged with conspiring to provide cryptocurrency to Isis" Eastern District of New York.
[179] United States Department of Justice. (2020) "Global Disruption of three terror finance cyber-enabled campaigns."
[180] Alliance for Healthier Communities (2019). 'Cybersecurity and Ransomware: Alliance Member Case Studies.'
[181] Ibid.
[182] United States Department of Justice. (2021) "Department of Justice seizes $2.3 million in Cryptocurrency paid to the ransomware extortionists darkside."
[183] "It provides a ready means for transnational criminals to convert to and from fiat currencies as well as transfer and launder proceeds of cyber-enabled crimes. Cyber criminals have additionally developed substantial networks of money mules and various digital money laundering services, such as over-the-counter brokers or exchange services and other unlicensed money services, to launder illicitly obtained funds." United States Secret Service (2022), U.S. Secret Service Launches Cryptocurrency Awareness Hub.

These attacks can be ethical,[184] in the sense that they are "often identified with hackers that abide to a code of ethics privileging business-friendly values"[185] or unethical.[186] For further context demonstrating the seriousness of this matter, in 2020, US authorities charged six Chinese nationals with laundering cartel funds via cryptocurrencies and bribing authorities.[187] The continuous movement of crypto-based profiting through ransomware and extortion reveal illicit enterprises' appreciation for evolving forms of dark payments. As drug cartels have moved away from using banks to launder money, American authorities suspect that they have turned to Chinese cybercriminals for aid. An analysis conducted by Chainalysis revealed that US$28 billion in Bitcoins were transferred from criminal actors and at least 50% were navigated by two Chinese exchange processes: Binance and Huobi.[188] Over 810 accounts absorbed US$819 million in Bitcoins that originated from criminals.[189]These money laundering crimes were facilitated by Over-the-Counter brokers who break the link between the vendor and the purchaser. By using over-the-counter brokers, the purchasers and vendors can remain distanced from the transaction(s). The fact that cryptocurrencies permit these kinds of transactions attracts Mexican drug cartels who depend on Chinese cybercriminals for the completion of money laundering activities. Other criminal organizations are also looking to Chinese cybercriminals for assistance in the illicit movement of cryptocurrencies.[190]

---

[184] [In the sense that a group like Darkside's hack of Colonial pipeline] on May 7, 2021, to which they stated "We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for our motives…Our goal is to make money, and not creating problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future." See also **Appendix II**, Darkside mission statement.
[185] Jaquet-Chiffelle, DO., Loi, M. (2020). Ethical and Unethical Hacking. In: Christen, M., Gordijn, B., Loi, M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham.
[186] For example, University of South Carolina Hospital attack where 1.14 million in Bitcoin was extorted.
[187] Eleonora Vassanelli, (2020) 'Money laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels,' Crossfire KM Money Laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels.
[188] Ibid.
[189] Eleonora Vassanelli, (2020) 'Money laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels,' Crossfire KM Money Laundering and Cryptocurrencies: A Case Study of Mexican Drug Cartels.
[190] Ibid.

Crypto Darknet

Darknet crimes are another source of concern for authorities and financial market regulators. Darknet crimes vary in severity and scale.[191] As darknet crimes are diverse, attacks on blockchain networks,[192] crypto jacking,[193] sanctions evasion, identity theft, illicit financing and extortion are all now more readily accessible through the multiple capabilities of this technology. For example, "laundering of $3 billion worth of bitcoin through ChipMixer,"[194] where a "large percentage of that $3 billion represents the proceeds of ransomware payments, thefts, darknet marketplace payments, nation-state criminal activity, and other illegal activity."[195] Similarly, the FBI seized over $112 million in funds linked to cryptocurrency schemes 'Sha Zhu Pan,' which is "a Chinese phrase that loosely translates to "pig butchering," scammers often target their victims through social networking and online communications platforms, dating websites, and phone calls and text messages that are meant to appear to have been misdialed. After gaining the trust of their victims – sometimes over a period of months – scammers eventually introduce the idea of trading in cryptocurrency. They then direct victims to cryptocurrency investment platforms or to co-conspirators posing as investment advisors or customer service representatives. Scammers control websites that are built to look like legitimate trading platforms, applications that victims download onto their phones, or malicious smart contracts accessed through cryptocurrency wallet software."[196]

---

[191] Staff Reporter (2021). 'Cryptocurrencies and the World of Darknet Markets and Scams.' Blockonomist. Cryptocurrencies and the World of Darknet Markets and Scams | by Blockonomist Staff | Geek Culture | Medium. Refer to Note.487 for further examples of darknet marketplaces.
[192] Spartan protocol (Pool token acquisition, asset balance inflation, liquidity extraction), 51% attacks.
[193] Use of malware or infected websites to unauthorized usage of mining equipment.
[194] United States of America v. Mingh Quoc Nguyen, 14/03/2023, United States District Court for the Eastern District of Pennsylvania criminal complaint, Case no. 2:23-mj-00528
[195] Ibid.
[196] United States Department of Justice (2023). "Justice Dept. seizes over $112M in funds linked to cryptocurrency investment schemes, with over half seized in Los Angeles case." Central District of California.

Regulatory Responses

The evolution of not only the utility of money in conjunction with technology,[197] but also the laundering utility of it, has promoted a series of aggressive calls for modernizing regulation and oversight of virtual currencies.[198] As a result, the FATF put forth guidance to assist nations in approaching this 'wild west' phenomenon.[199] However, given the multiplicity of innovative functions of crypto, the standards, arguably, caused more confusion than clarity, which will be discussed further in chapter 5 with qualitative data. The gap between regulation and financial innovations is further widening,[200] and the dynamics of regulatory action is reactive to past financial crises.[201] This, however, does not offset the potential of new technologies for consumer protection, market oversight and opportunities for prudential regulations.[202] By way of example, the Financial Conduct Authority (FCA) hosts "Tech Sprints", or hack-a-thons,[203] to encourage competition to solve select compliance problems, a model followed generally by financial institutions and RegTech firms to build more accurate transaction monitoring systems.[204] Simply put, given the multiple stakeholder interest in new emerging technologies, regulators will not be able to draft concrete rules without cooperating with stakeholders in new emerging technologies.[205] This collaborative approach is further outlined in the overarching AML/CFT global legal

[197] Where paper ledgers are now computerized, value is not only exchanged physically but digitally, double-spending and counterfeit notes are computerized to alleviate risks.
[198] This is discussed further in chapters 4, 5 and 6 and the corresponding FATF responses.
[199] FATF (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris.
[200] Brummer (2015); McGuire (2016); Vermeulen, Fenwick, and Kaal (2016); Zetzsche et al. (2017).
[201] Kaal, W. A. (2013). Dynamic regulation of the financial services industry. Wake Forest Law Review 48:791–828.
[202] Ibid.
[203] Alongside this is "Sand boxes" which tests fintech products and services in the real market.
[204] Crane, J. M. A. (2017). RegTech: Bending the risk/cost curve or breaking it? Fintech Law Report E-Banking, Payments & Commerce in the Mobile World 4:1–11.
[205] Shin, D.-H., and M.-K. Lee. (2017). Public value mapping of network neutrality: Public values and net neutrality in Korea. Telecommunications Policy 41 (3):208–24.

framework in chapters 5 and 6, through reporting obligations and key oversight parameters of interested parties,[206] and ultimately, the ethos and mechanics of global AML/CFT standards.

There is a lot of room for improvement in virtual currencies. Security risks must also be a major concern, particularly where virtual currencies cross borders. Security risks are particularly important in these circumstances because it is not altogether clear how legal rights of the parties are protected in terms of jurisdiction and applicable law. Therefore, the safety and security of the virtual currency user must at least be protected. This is a major risk, as has been demonstrated by the preceding sophisticated hacks on exchanges.

In the meantime, the use of cryptocurrencies will continue to grow because it facilitates international and national trade for those who would like to participate in virtual currency markets and are unable and/or are skeptical to participate in conventional markets. It is important to remember that the inability to participate in the conventional market is a major driver towards this new market. When regulating restrictions on the extent to which consumers may participate in virtual currency trading, especially where the risk of money laundering and other high crimes are possible, the risk of emerging capabilities of money laundering and the direct/indirect roles various users have must be considered. Where the value of a particular Cryptocurrency inflates, so does its attractiveness for profit by sophisticated criminal enterprises.

[206] Regulatory reporting or compliance oversight through language-data stored in financial sectors has not only been streamlined through Fintech but also enhanced through machine-readable monitoring mechanisms, application programming interface and uniform data formats. See chapter 6 discussions on the role of blockchain forensics.

Chapter 4 – Crypto Regulatory Dynamics

Introduction

Since the creation of Bitcoin in 2009, opportunities for carrying out financial transactions with crypto currencies and assets have grown exponentially. According to Perkins, by March 2020, there were 5,100 cryptocurrencies in the global market worth US$231 billion.[207] This number has grown exponentially to include more than 20,000 cryptocurrencies in existence in 2022.[208] At a fundamental level, crypto currencies are appealing because of the espoused ability to conduct the transfer of assets and payment, without a centralized party, on a public ledger pseudonymously. Moreover, crypto currencies are decentralized, and their transactions are free of the authorization and protocol checks associated with conventional money transactions. However, there are significant concerns about the security risks associated with the use of crypto currencies and assets. For example, FATF expressed concerns about this emerging space:

> "The virtual asset ecosystem has seen the rise of anonymity-enhanced Cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows, as well as the emergence of other virtual asset business models or activities such as initial coin offerings (ICOs) that present ML/TF, fraud and market manipulation risks. Further, new illicit financing typologies continue to emerge, including the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner."[209]

[207] David W Perkins (2020), 'Cryptocurrency: The Economics of Money and Selected Policy Issues,' Congressional Research Service. CRS Report
[208] Cryptocurrency prices, charts and market capitalizations (no date) CoinMarketCap.
[209] FATF (2021), "Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers." pg. 2.

The Bank for International Settlements reports that in 2019 alone approximately 1.1% of all virtual currency transactions or about US$11 billion dollars in value were illicit.[210] Similarly, in another report referenced by the Bank for International Settlements, Bitcoin alone was linked to US$3.5 billion in illicit transactions.[211] While these figures may seem low in the grand scheme, it is contended that this chapter will outline the variance in delta with this figure and conduct a deeper dive into illicit utility. This chapter will thus outline that the risk of money laundering as the central issue.[212]

As "a single Cryptocurrency emerge that provides widespread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this Cryptocurrency, as well as the potential for its use by terrorist [or criminal] organizations, would increase."[213] The main challenge for regulators in this context is how to maintain the distinguishing and appealing features of virtual currencies and assets, improving their integrity and security, while avoiding counter-productive regulation which can detract from their appeal and deter engagement. The current practice of primarily relying on existing anti-money laundering laws is unsatisfactory, given the cross-border and speed of movement of illicit crypto currencies and assets. This chapter explores these challenges. The chapter is divided four parts which starts with a background of Crypto currencies and assets. The second part deals with the taxonomy of Crypto. The third part discusses the legal framework and classifications. The fourth part outlines approaches to the Crypto phenomenon.

[210] Rodrigo Coelho; Johathan Fishman, and Denise Garcia Ocampo (2021). "Supervising Cryptoassets for Anti-Money Laundering." Bank for International Settlements.
[211] Ibid.
[212] Theft, fraud, hacking, identity theft are all examples of other security concerns which will be briefly mentioned and/or discussed when appropriate.
[213] The RAND Corporation, (2019). "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats."

Cryptocurrencies and Assets

As already stated, that are a plethora of crypto currencies in use, with yet more continually being invented. Fundamentally, crypto currencies, like Bitcoins, are seen as a virtual currency, marking ownership of transactions.[214] As Bitcoin is not issued by an entity such as a central bank, it (Bitcoin) is a mined 'asset' by miners (computer systems who solve blocks on the chain) who issue bitcoins in return for the resolution of complicated mathematics with software applications. The process of mining is not done manually but continuously and takes approx. 110 Terawatt Hours per year, which is the equivalent to the annual energy draw of small nations like Sweden or Malaysia, and this figure has been steadily rising.[215] For visual illustration, The Cambridge Bitcoin Electricity Consumption Index demonstrates the rising usage, as can be seen in **Figure 6**.

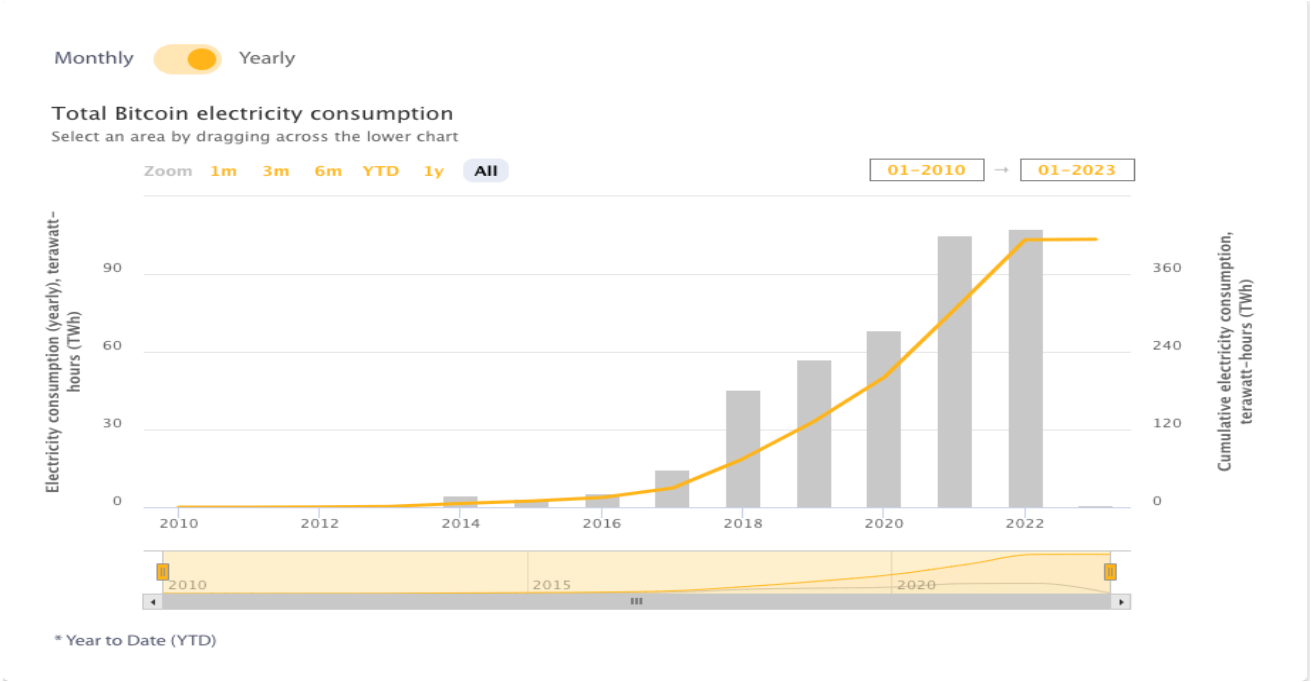


Figure 6: Cambridge Bitcoin Electricity Consumption index 2010-2022.

[214] James Gatto and Elsa S. Broeker, (2015) "Bitcoin and Beyond: Current and Future Regulation of Virtual Currencies." Vol.9 no.2 Ohio St. Entrepren Bus LJ p.429

[215] For hourly, and daily tracking, see Cambridge Bitcoin Electricity Consumption Index https://ccaf.io/cbeci/index

In 2020,[216] Central Backed Digital Currencies (CBDC), first crystalized, though arguably the first CBDC was in 1993 through the Bank of Finland utilizing the "Avant Smart Card." With the popularity of Bitcoin expanding, it has been made possible for Bitcoins to be converted to "government-issued legal tender (commonly referred to as fiat currency)" or any other form of virtual currency.[217] This is highly important and will be discussed further in analysis regarding usage in laundering and illicit finance. Furthermore, Bitcoins, as many other virtual currencies and assets, now have purchasing power as they can also be used to purchase any goods, anywhere, by anyone over the Internet.[218]

Cryptocurrencies are thus viewed as cyber funds that are alternatives to cash or conventional money.[219] The currencies are developed for the express purpose of getting around the scrutiny and requirements of conventional banking transactions, through trustless verification protocols in the blockchain.[220] For instance, in a conventional banking transaction, a sender will move funds from one person to another through a bank or a money transfer institution such as Western Union or Moneygram. These transactions are carried out with the aid of a third party and will involve due diligence checks and prudential standards. The relative lack of checks and prudential standards opens up virtual currencies and assets to clients who would not otherwise be qualified, as in capable to access traditional financial systems (whether through capital restraints, lack of paperwork, and/or loan/interest requirements) to use conventional transaction processes. At one end of the spectrum, so-called TradeFi thus can exclude poverty stricken third-world country

[216] Bahamas Sand Dollar in the form of Central Backed Digital Currencies.
[217] James Gatto and Elsa S. Broeker, (2015) 'Bitcoin and Beyond: Current and Future Regulation of Virtual Currencies,' Vol.9 no.2 Ohio St. Entrepren Bus LJ p.429
[218] Ibid.
[219] International Monetary Fund Staff Discussion Note. (2021) 'Virtual Currencies and Beyond: Initial Consideration'. SDN/16/03.
[220] Ibid.

citizens while, at the other end, it can also impact criminals trying to use the legitimate financial system.[221] Therefore, the financial inclusion potential of virtual currencies is appealing to many users. In addition, the lack of protocols and due diligence checks improves the speed of these kinds of transactions. However, at the same time, there are concerns about the exploitation of these forms of financial transactions by terrorists, money launderers, tax evaders, and fraudulent enterprises.[222] In addition, there are concerns that once these technologies become more popular and in wider use, security risks to financial stability will become a more serious concern.[223] While the crypto realm continues to evolve and expand, the regulation of virtual currencies and assets is in its infancy,[224] partly due to its development stage and new real-world use cases.[225] Moreover, regulation of virtual currencies and assets is challenging because these transactions take place in borderless and non-indexed environments on the internet.[226] Conflicts of laws and jurisdictions will always present difficulties for regulators and those who seek to enforce crypto transactions or who have legitimate complaints and losses. As well as the scarce regulations present, discussed later in this chapter, guidelines are issued for virtual currency transactions. These guidelines are typically issued by national agents, and international regulatory agencies, like FATF, that facilitate the use of virtual currencies and are based on existing regulations and laws dealing with financial

[221] Ibid.
[222] Corbet, S., A. Urquhart, and L. Yarovaya (2020). 'Cryptocurrency and Blockchain Technology.' Berlin, Boston: De Gruyter.
[223] James Gatto and Elsa S. Broeker, (2015) "Bitcoin and Beyond: Current and Future Regulation of Virtual Currencies." Vol.9 no.2 Ohio St. Entrepren Bus LJ p.429
[224] Later discussed in this chapter. For further discussions see Egan, Mo. (2018). A Bit(Coin) of a Problem for the EU AML Framework in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018)
[225] Only a handful of legacy institutions embrace, let alone recognize, crypto as a positive replacement for traditional banking. Combined with security threats and concerns over its illicit potential, regulators are approaching this technology with a high degree of caution.
[226] Non-indexed portions of the internet are the primary location where current illicit transactions are taking place. This makes it challenging for law enforcement to detect and trace the crime and the funds associated with it and deters regulators from embracing it.

transactions.[227] At this particular time, models for the creation of hybrid frameworks have been suggested such as the one offered by the United States National Institute of Standards and Technology that suggests treating virtual currencies as one would government-issued currencies and therefore departing from the decentralized themes of Cryptocurrencies.[228] This however is counterproductive to the very attractive nature of the usage of virtual currencies, the removal of institutional traditional third-party bodies to transact peer-to-peer. Before turning to the current legal framework, the next section outlines the basic taxonomies and national considerations of these virtual currencies.

Taxonomy of Cryptocurrencies

A 2020 Deloitte report lists five basic taxonomies for digital assets and currencies.[229] The five basic categories are:

1) Security Tokens: Due to their "special characteristics", they are "similar to traditional instruments like shares, debentures, or units in a collective investment scheme".[230] Science Blockchain Token is an example. Tokens in this category are regulated extensively due to their treatment as securities.[231]

2) Cryptocurrencies or Exchange Tokens: By far the most popular form of virtual currencies readily available for public use, such as Bitcoin, and their security is based on the

[227] Iwa Salami, (2021). "Challenges and Approaches to Regulating Decentralized Finance." 115 AJIL Unbound, p.428
[228] Peter Mell; Aurelein Delaitre; Frederic de Vaulx and Philippe Dessau, (2019) "Implementing a Protocol Native Managed Cryptocurrency." The Fourteenth International Conference on Software Engineering Advanced.
[229] Deloitte. (2020). "A Market Overview of Custody for Digital Assets: Digital Custodian Whitepaper."
[230] Ibid.
[231] European Union: regulated by MiFID II and require a prospectus Directive; Germany: MiFID licenses issued by BaFin; United Kingdom: regulated by FCA under specified investments; Switzerland: regulated by FINMA; United States: Regulated by SEC; Canada: Regulated in part by CSA; Brazil: must be registered and approved by CVM; Australia: regulated by ASIC; Isreal: regulated by ISA; Singapore: regulated by MAS and Securities and Futures Act; Japan: regulated by FIEA; Hong Kong: regulated by SFC; Malaysia: regulated by Securities Commission Malaysia.

utilization of cryptographic functions.[232] More on these functions will be elaborated on later in the chapter.

3) Stable Coins: Stable coins "attempt to stabilize its volatility by typically pegging themselves to a stable asset such as the US Dollar or gold".[233] This is favorable to risk-averse investors.[234]

4) Utility Tokens: These tokens attempt to provide value to investors through exposure to future products or services.[235] This can be done through a typical start-up company whereby investors are provided with utility tokens to use at some point in the future for access to a product or service, an example of which would be Filecoin.

5) E-money Tokens: These tokens have "an electronically (including magnetically) stored monetary value as represented by a claim on the issuer, issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a person other than the issuer."[236] The two features which define them are that they maintain a stable value by reference to the value of one fiat currency, and they use DLT or similar technology. Some stable coins could be considered e-money tokens.

Further taxonomies and lists are emerging to expand on these basic categorizations.[237] These basic categorizations have sought to fulfil basic functions of money. For a contextual discussion, building on the basic functions of money, its foundation, and regulation, conventional payment options will be briefly discussed to highlight the challenges with regulating various and

[232] Deloitte n.229.
[233] Deloitte n.229.
[234] Deloitte n.229.
[235] Deloitte n.229.
[236] The UK Electronic Money Regulation 2011, s.2(1)
[237] Group of Thirty, (2020) 'Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead.'

expanding categories of virtual currencies and assets. In a conventional payment system, there is a front-end transaction where the payment is initiated and a back end where the funds are settled and cleared. For example, a payment of rent to a landlord can be initiated by a check and ends with the funds described in the check being credited to the landlord's bank account and removed from the tenant's bank account. The funds might pass through the central bank as they move from one bank account to another. The funds are always characterized by government-issued currencies or fiats as a means of establishing exchange values.[238]

In contrast, virtual currencies, as is their appeal, move between parties without the need for third-party central institutions.[239] As an example, Bitcoin moves between peers through a "cryptographic scheme" that "do not require identification".[240] All cryptocurrencies offer customers some degree of pseudonymity reflected by the cryptographic system used. However, it is not complete anonymity as is commonly touted.[241] Cryptocurrencies use several different methods for completing or settling transactions whereas conventional payments pass-through permissioned systems which rely on a central authority for finalizing the settlement or clearance of a payment transaction. Meanwhile, crypto currencies and coins pass through permissionless systems with no centralized authority for clearance and settlement. What is interesting is the need for an exchange, in most cases, to hold onto the private keys which control the coins.[242]

[238] Ibid.
[239] Group of Thirty, (2020) "Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead." p.2
[240] Ibid.
[241] This will be further elaborated on in chapter 5 with regard to attributions and heuristics.
[242] "Not your keys, not your coins". This will be elaborated on further in this chapter and chapter 5.

Thus, in recent years, many nations view such technology as a threat and have started exploring CBDCs, through "seeking to preserve key aspects of their traditional monetary and financial systems, while experimenting with new digital forms of money."[243] CBDCs can take different forms also. [244] Indirect CBDCs are much like existing two-tier systems with the customer holding an intermediary claim and the central bank directing attention to the wholesale account inclusive of intermediary accounts with the central bank. For example, an intermediary will issue a token to a customer which is an intermediary claim and deals with due diligence clearance (Know Your Customer/KYC). In essence, "the customer claims on the intermediary are fully backed by intermediary claims on the central bank".[245] This allows for a nation to maintain a relative form of hegemony over the currencies utilized and, importantly, the taxation of such use. For a nation to allow a system to be used without reaping revenue-generating taxation would not only be foolish, but also counter-productive to the financing of government operations.

A second form of CBDCs is direct CBDCs, which are capable of taking two forms.[246] The first form involves all parties having central bank accounts where transactions involve transferring payment from one account to the other. In the second form, tokens are issued from the Central Bank and a permissioned system clears the transaction. Finally, there are hybrid CBDCs, where the claim resides with the Central bank, but intermediaries play a more significant role in managing and clearing the transaction.[247]

[243] Atlantic Council (2022) "Transcript: Central banks from Stockholm to Beijing are about to change the way the world uses money." Kristalina Georgieva IMF Managing Director, in an address to the Atlantic Council
[244] Ibid.
[245] Group of Thirty, (2020) "Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead." p.2
[246] Ibid.
[247] Group of Thirty, (2020) "Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead."

From a regulatory standpoint, governments, legislators, central banks, and policymakers must think about whether they want to encourage or discourage new digital currencies or do they want to create a central bank specifically for digital currencies rather than extending current frameworks for each digital currency or token. Secondly, if the decision is made to encourage new currency technologies, there are many options for specific frameworks. For example, permissioned systems permit access to private data while permissionless systems have the advantage of protecting privacy, but not always, although they come with greater security risks. Thirdly, governments want to be in a position to collect revenue from taxes, ensure that regulations are enforced, and place constraints on unlawful transactions. Governments cannot "idly allow a large fraction of their economy's payments to be made through vehicles that are excessively costly to audit, either because of technology or because their key data are kept by a foreign government or a private entity outside their regulatory reach".[248] With the Central Bank's increased involvement in digital currencies, more issues are expected concerning whether the data collected by the Central Bank is used appropriately and whether private entities are encouraged to continue to be innovative. Finally, Central Banks' involvement inevitably comes with increased authority to examine transactions to identify and/or prevent theft, malicious activities, such as activities by terrorists, sophisticated launderers, cybercriminals, and so on. As advances in technologies will place a significant security risk and costs on Central Banks, there must be proportionality in returns on investments with respect to this new phenomenon.[249]

One of the most important considerations for monitoring and regulating digital assets and currencies involves considering and changing the role and responsibilities of custodians. In the

[248] Group of Thirty, (2020) "Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead."
[249] Later discussed in "cultures of compliance" section in chapter 6.

conventional sense, the custodian is an institution with physical custody of the assets or funds.[250] The custody of digital assets is typically represented by blockchain or distributed ledgers with a series of binary symbols. Digital assets represent various values. For example, a Bitcoin will not typically reflect any real-world asset. Other digital currencies or tokens may represent that the owner holds some form of a physical asset such as a shares in a corporation or real estate. This has been done through the 'toxenization' of assets, whereby a share in a corporation or a parcel of land is claimed by the tokens underlying them.[251] Others reflect the right to gain access to some service such as the right to execute a smart contract on a certain blockchain platform.

Digital custodians have the same responsibilities as conventional custodians where "custodians operate in a similar fashion to traditional financial markets in that their primary role remains the responsibility for, and the safekeeping of customer's digital assets. This is achieved through safe key management, which allows the assets to be cryptographically secured. However, unlike for traditional assets, an entity has custody of a digital asset simply by holding the private key on behalf of the asset holder, ensuring that it cannot be accessed by any other party".[252] Like conventional custodians, digital custodians are required to ensure the safety and security of the assets in question. The only difference is that the digital custodian is not in physical possession of the actual asset, but rather, the digital custodian holds the safe key which permits the "assets to be Cryptographically secured"[253] and, unlike conventional custodians, the digital custodian has custody of the asset by simply holding the private key on behalf of the asset holder.[254]

---

[250] Debevoise & Plimpton, (2018) "Custody of Digital Assets: Centralized Safekeeping of Decentralized Assets under the Investment Advisers Act." Debevoise in Depth.
[251] Polymath tokenized billions of real estate in New York and Ontario as an example.
[252] Deloitte. (2020) "A Market Overview of Custody for Digital Assets: Digital Custodian Whitepaper." p.7.
[253] Ibid.
[254] The deeper distinctions of the fundamentality of the purpose of such private keys - i.e., not your key, not your coin - will be elaborated on later in this chapter and chapter 5.

The problematic approaches for the regulation of both digital assets and custodians revolve around the fact that there is no single or harmonized taxonomy applicable to each form of asset which impacts the roles and responsibilities of their custodians. In other words, it is difficult to create standardized laws for defining the role and duty of digital custodians since they have different responsibilities. To overcome these difficulties, some governments, including the UK, have attempted to narrow the classification of digital assets as a means of regulating them more profoundly and effectively.[255] The three categories established by the UK are exchange tokens, security tokens, and utility tokens.[256] Still, the narrowing of the taxonomy of digital assets fails to facilitate a satisfactory recognition of their full features and functions and as a result, the proper regulation of the assets is challenging. At a basic level, the functions of cryptographic-based tokens are increasing in style and form. Rather than focus on the form of the asset, regulators should pay greater attention to the "substance of the underlying asset and the rights associated with it" unless the form "changes the substantive nature of the asset".[257]

Exchange and utility tokens are unregulated tokens.[258] As stated previously, utility tokens are used for purchasing services. Exchange tokens are used for making exchanges that include crypto assets such as Ether, XRP, and Bitcoin. Security tokens are similar to shares and debentures

[255] Allen, Jason G and Rauchs, Michel and Blandin, Apolline and Bear, Keith, (2020). "Legal and Regulatory Considerations for Digital Assets." CCAF Publications.. And see Treasury, H.M. (2018) Cryptoassets taskforce: Final report.
[256] HMRC (2021) "Cryptoassets Manual 'CRYPTO10100 - Introduction to Cryptoassets: what are Cryptoassets." - internal manual.
[257] Allen, Jason G and Rauchs, Michel and Blandin, Apolline and Bear, Keith (2020). "Legal and Regulatory Considerations for Digital Assets." CCAF Publications.
[258] HM Treasury. (2021). "UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence"; Allen; Michel Rauchs; Apolline Blandin and Keith Bear, (2020). "Legal And Regulatory Considerations for Digital Assets." CCAF Publications.

and are already regulated in securities laws in multiple jurisdictions.[259] However, the financial conduct authority (FCA) has expressed concerns about properly regulating all digital tokens because they are fluid and flexible. For instance, digital tokens may be utilized for raising funds one day, and the next day they may be used as an exchange mechanism.[260] Combined with their volume and speed, the value of these tokens poses risks as attractive mechanisms for illicit use, which will be elaborated on later in this chapter.

By way of example to the challenges of these tokens, since the Crypto assets Taskforce 2018 report, the UK government and relevant authorities have taken action as a means of addressing the risks of crypto assets, and at the same time, supporting the innovative value of such assets.[261] The first regulatory step can be described as uncertain and vague. The UK government clarified the regulatory authority of the FCA by setting out when tokens can be relegated to investment status under the Financial Services and Markets Act 2000 Regulated Activities Order 2001. Tokens capable of regulation may include tokens that are financial instruments under the Second Markets in Financial Instruments Directive or e-money. However, much depends on the type of activities, as in specific cases "FCA authorization or registration may be required."[262] The problem with these changes is that there are no fixed rules. Rather, the activity which is already free of centralization must first be examined to determine if it should fall under the FCA's regulatory framework. This leaves crypto asset service providers with the option of changing the activity to ensure that it does not fall under the perimeters of the FCA authority.

[259] Supra 257 and 258.
[260] Financial Conduct Authority. (2020) "Prohibiting the sale to retail clients of investment products that reference Cryptoassets."
[261] Supra 257 and 258.
[262]Financial Conduct Authority. (2020) "Prohibiting the sale to retail clients of investment products that reference Cryptoassets."

In the context of illicit use, as part of the anti-money laundering and countering the financing of terrorism legislative regime, a good example of legislative efforts can be found in the EU's Sixth Anti-Money Laundering Directive (6AMLD), where the proposal for a new AML Authority was a good option. The reason is that 6AMLD moved to harmonize the definition of money laundering across all EU member states, with an addition of 'aiding and abetting' to the list of activities that are categorized as money laundering. This was built on 6AMLD's predecessor, the Fifth Anti-Money Laundering Directive bringing virtual currency and asset custodians under the AML/CFT regulatory framework. 6AMLD prohibited the sale, marketing, and distribution of "derivatives and exchange-traded notes that reference certain types of crypto assets to retail consumers".[263] Ultimately, from a consumer protection standpoint, the legislation restricts the sale of contracts for difference, futures, options and exchange-traded notes referencing unregulated, transferable crypto-assets.[264] Therefore, the prohibition merely ensures that crypto assets are not formalized by allowing them to be passed off with formal and conventional notes which are regulated.

The shift – not only by the EU but also by individual nations requiring that authorities provide consumers with information about how to take proper safeguards against crypto asset scams – is a positive step to keep up with market trends, as seen by the extensive collapses and, quite literally, the disappearance of consumer tokens by multiple exchanges.[265] Given the fallout

[263] ibid.
[264] Supra n. 262.
[265] TerrsaUSD and LUNA, 3AC, FTX, Voyager Digital, Celsius Network, BlockFi

of multiple crypto monetary losses, brushed off as a "crypto winter," authorities now publicize,[266] warnings of crypto assets scams and identify entities that are known to be carrying on those scams. Still, given the emergence of innovative laundering techniques which complicate the interplay of multi-sector cooperation and regulation, further action is required if governments intend to protect the financial market's stability and integrity, protect consumers, promote competition and innovation and, ultimately, address sophistication of laundering capabilities through increased enhancement of crypto-enabled crimes on the dark web, which will be elaborated on later in this chapter and in chapter 6.

Legal Framework and Classification

At a basic level, crypto currencies are either centralized[267] or decentralized/distributed, and are either convertible or non-convertible.[268] The taxonomy of cryptocurrencies is summarized in **Figure 7**.

	Centralized	Decentralized
Convertible	Can be exchanged for Fiat currency – administrators, third-party ledgers, users and exchangers.	No administrators, no trusted third-party ledger, and can be exchanged for fiat currency
Non-convertible	Cannot be exchanged for Fiat currency – administrators, third-party ledgers, users and exchangers.	N/A

Figure 7: Cryptocurrency Taxonomy.

[266] Office of the Comptroller of the Currency (2023) "Joint Statement on Crypto-Asset Risks to Banking Organizations." Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation.
[267] Loyalty points from retail companies or air miles, confided to a particulate centralized structure of an entity.
[268] Used in transactions outside of a network using open-source software such as Litecoin, Dogecoin and Bitcoin.

There is currently no universally accepted regulatory regime for crypto assets; given the scale of research and development, both in the private industry and with over 100 countries exploring this technology.[269] The lack of a universally accepted regime, with an effect of a regulatory environment as the 'wild west' is due to a number of nuanced considerations, further discussed in this chapter. Achieving global harmonization on self-regulation by deputizing,[270] the private sector is difficult and unsustainable. This is partly due to a lack of uniformity of standard business practices for an industry continuously evolving and innovating, and, arguably, lack of a full comprehension of the unintended consequences of new functions of crypto. This leaves criminals to exploit jurisdictional inconsistencies. It has been expressed that businesses in EU member states can self-regulate, provided adequate regulatory oversight is present in this sphere, evidenced by recent developments attempting to harmonize a uniform legal framework for crypto assets across the EU.[271] Whether through Markets in Crypto Assets (MiCA), which seeks to establish a harmonized set of rules for crypto assets and related activities or services,[272] or 5AMLD/6AMLD which espouse cooperation and harmonization of money laundering offences and tougher rules on obliged entities, particularly in relation to crypto services and providers, the need for harmonization is not only apparent, but necessary. In the U.S. a Bit License is needed for any operations being conducted in the State of New York, where compliance obligations and

[269] Whether testing Central Bank Digital Currencies, researching and/or already distributing CBDC to the public. More on developing interest can be found at https://www.atlanticcouncil.org/cbdctracker/
[270] Imputing obligatory oversight by the private industry to self-regulate.
[271] (MiCA) Proposal for a Regulation of The European Parliament and of The Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 European Parliament (2022), press release 'Cryptocurrencies in the EU: new rules to boost benefits and curb threats.'
[272] Coming into force after a transitional period of 18 months, thus no earlier than Q3 of 2024, where rules around Stablecoins have a 12-month transitional period, thus potentially coming into force as early as spring of 2024.

examination protocols are required. In other states, money transmission laws apply, where the Financial Crimes Enforcement Network (FinCen), the Commodity Futures Trading Commission, and the Securities and Exchange Commission capture crypto assets under their regulatory reach.[273] While the regulations may differ in intensity and scrutiny, in Asia and some middle eastern countries, attitudes towards the technology are much more restrictive. Iraq, Egypt, Qatar, Oman, Morocco, Algeria, Tunisia, Bangladesh, and China have all taken a restrictive approach to Crypto assets.[274] By way of example, the "Chinese authorities have taken a tough stand on ICOs."[275] This was done through a notice on preventing financial risks relating to initial coin offerings on September 4, 2017.[276] As of November 2021, there were 9 jurisdictions with an absolute ban, 42 jurisdictions with an implicit ban and 103 jurisdictions with applicable regulatory frameworks to cryptocurrencies.[277]

The newness of this technology and its emerging capabilities across multiple sectors have sparked different approaches toward regulation. The UK,[278] Brazil,[279] Singapore[280] and

[273] There are on-going discussions related to the classification of Crypto assets as securities or commodities. However, on a general level, both are inevitably captured. As for exchanges and services which engage in the selling or buying of Crypto assets – they are subject to money transmission regulations by FinCen.
[274] Meaning that it does not support the ownership, mining and operations of exchanges within its jurisdictional borders when compared to the U.S.
[275] Lu, L. (2018). "Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response." Butterworths Journal Of International Banking And Financial Law, Vol. 33 Issue. 3, p. 180.
[276] See Lu, L. (2018) on discussions relating to China's regulatory response on Bitcoin risks.
[277] Library of Congress, Global Legal Research Directorate (2021) "Regulation of Cryptocurrency Around the World: November 2021 Update."
[278] Where in April 2022, the government announced its plan to make the UK a "global Crypto asset technology hub." See Codd, F. and Browning, S. (2022) Government's regulatory approach to Crypto-assets and currencies, House of Commons Library.
[279] Brazil's Law no. 14,478 of 2022 legalizes the use of Cryptocurrencies as a payment method within Brazil. This law was published on December 22, 2022, in the Official Gazette (Diário Oficial da União)
[280] It is friendly towards blockchain in finance, not speculative crypto trading and is critical of cryptocurrencies, where the Monetary Authority of Singapore (MAS) issues digital payment token licenses only to those who make it through an application process. See Monetary Authority of Singapore (2022) 'Consultation Paper on proposed regulatory approach for stablecoin-related activities' ; Monetary Authority of Singapore (2022) 'Proposed regulatory measures for digital payment token services.'

Switzerland,[281] have adopted a public private partnership model, where private actors adapt and leverage the new technology and in line with protecting the crypto ecosystem and its integrity, are active in adjusting to meet regulator demands. While this is not the sole approach to regulation of crypto, it does speak to the synergy between private expertise and public interest in regulation. Sandboxes and experimental exercises provide for proof-of-concepts and considerations of safeguards. At the other end of the spectrum, outright rejection of the technology represents a much more restrictive approach – one that does not provide capabilities for regulations to develop harmoniously with the market and its technology and, in effect, forces stakeholders and users to employ regulatory arbitrage or move underground. I would also argue that this restrictive approach has unintended consequences of alienating jurisdictions in leveraging the technology while further exacerbating the technology's risks.[282]

Apart from the crypto asset themselves and their regulations, there are further legal considerations associated with the parties subscribing to these technologies. Digital identities, biometric data, correspondent institutional relationships, asset forfeiture and seizure, taxation, interoperability, custodian obligations and consumer remedies are all examples which interfere with restrictive approaches[283] to regulation in this sphere.[284] Restrictive approaches to regulations presume that incumbent institutions are risk-free while anything new is highly risky and ignoring

[281] Contains favourable and attractive legal framework for Crypto assets, treated as property or gold, and regulated by the Switzerland Federal Tax Administration (SFTA) and Swiss Financial Market Supervisory Authority (FINMA). See: Federal Assembly of the Swiss Confederation (2021) 'Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology'; The Swiss Federal Council (2021) 'Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology.'

[282] For example, intelligence sharing, cooperation and pragmatic approaches to regulation are foundational to FATF recommendations, and, without them, jurisdictions are not always equipped to effectively address emerging markets with cross-border reach, exponentially growing in both traction and value.

[283] Whereby highly restrictive approaches will not solve these emerging legal issues.

[284] Each of these will be discussed further in this chapter and chapter 6.

that - at a fundamental level - these are assets which represent an underlying activity, whether a network or an application, with an espoused value that consumers are willing to buy and sell at the market rate. Whether a medium of exchange, unit of account, and/or in-store value, coupled with emerging usages for it,[285] the crypto market is not showing signs of slowing down. Thus, it was no surprise to see reform efforts gather pace in 2022 as a result of different occurrences. Notable amongst these was the Russian invasion of Ukraine in February 2022 and the 3 Arrows Capital, FTX bankruptcies and subsequent ripple effects. Thus, a series of international responses emerged, calling for countries to start designing frameworks for cryptocurrencies to prevent Russia's government and/or other parties from using the technology as a response to aggressive banking measures and sanctions while providing needed consumer and investor protections. This, however, is an apples-to-oranges comparison since every nation has different practices, degrees of risk-tolerance, and overall different requirements for either market sustainability or oversight of home-grown criminal operations.

Quite different approaches to cryptocurrency regulation are evident in how China and the US approached cryptocurrencies.[286] While China expressly banned, as in it does not support the exchange or financing "activities between fiat and coin substitution in 2017,"[287] the US has cryptocurrencies and exchanges increasing. The differences in the regulatory approaches taken by the US and China reveal only that the US is prepared to take calculated risks or to support the use of cryptocurrencies, subject to proper oversight available, in exchange for their potential and benefits. Contrast, China simply rejects the potential and benefits and does not feel comfortable

[285] Non-fungible tokens, royalties, metaverse, Web3, etc.
[286] Rain Xie (2019), 'Why China had to "Ban" Cryptocurrency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China.' Vol.18 Issue.2 Washington University Global Studies Law Review, p.457
[287] Ibid.

taking risks with traditional decentralized cryptocurrencies. That is why China flirted with the idea of CBDC in 2014 and launched the Digital Currency Research Institute in 2016.[288] Where in 2020, the People's Bank of China (PBOC) "launched the pilot experiment of CBDCs in Shenzhen which is the fully digital version of Chinese Yuan or Renminbi."[289] Lu examined that the "essence of issuing digital yuan is the digitalization process of cash with its intrinsic value being as stable as legal tender."[290] Furthermore, Lu outlined that the CBDC of China targets the retail sector in order to offer "flexibility, speediness, and wide acceptance… reduce customers' storage costs and the risk of carrying cash…cuts transfer costs between different commercial banks and mitigates the time lag…lower a country's public expense for maintaining banknotes and counts,"[291] and finally, "alleviates criminal activities relating to paper money transactions such as counterfeiting and money laundering."[292]

It is necessary to take China's political system into account, since in the context of CBDCs, "China is one of a few major economies starting this pioneering financial experiment."[293] Although China is an open market economy, it is a country where the government maintains significant control over its markets and economy. The nature of the decentralization of bitcoin and other cryptocurrencies would be an affront to the Chinese government's hegemony on all aspects of life within its borders. Lu reasoned that to "balance the AML compliance task with the protection of personal data and privacy will be a major concern for Chinese financial regulators when dealing

[288] Lu, L., & Chen, H. (2021). "Digital Yuan: The Practice and Regulation of China's Central Bank Digital Currency (CBDC)." Butterworths Journal of International Banking and Financial Law, Vol. *36* Issue.8, p.601.
[289] Ibid.
[290] Lu, L., & Chen, H. (2021). "Digital Yuan: The Practice and Regulation of China's Central Bank Digital Currency (CBDC)." Butterworths Journal of International Banking and Financial Law, Vol. *36* Issue.8, p.601.
[291] Ibid. p. 601-602.
[292] Lu, L., & Chen, H. (2021). "Digital Yuan: The Practice and Regulation of China's Central Bank Digital Currency (CBDC)." Butterworths Journal of International Banking and Financial Law, Vol. *36* Issue.8, p.602.
[293] Ibid. p.601.

with the cross-border use of CBDCs."[294] As one of the greatest aspects of cryptocurrencies is their pseudonymity, that is, the transaction can be carried out in relative secrecy to the user's identity but is open to the public on the blockchain,[295] the legality of many of these virtual currency transactions can be questioned as Buchwald states that "pre-coded agreements are riddled with a host of practical and governance-based complications."[296] Not lease due to conflict of laws grounds and also on the basis of common law contract principles of unequal bargaining power, meeting of the minds, misrepresentation and/or fraud. Because the state has an unarguable right to regulate and maintain a reasonable system of contract laws.[297] If they do not, contract disputes would be moot, and societal collapse would be imminent.

Approaches to Cryptocurrency

Legitimacy and reputation of legacy institutions and/or emerging markets are always a target for creative enterprises for misuse. Currently, the 21st century is described as a time when science and technology have skyrocketed rapidly and these developments have had a significant impact on the World Wide Web and its activities.[298] The potential for cryptocurrencies to reinvent financial transactions from a centralized system to non-intermediated capabilities has sparked a wave of innovations across multiple sectors.[299] As with conventional fiat currencies and centralized payment systems cryptocurrencies are vulnerable to being exploited by criminals for illicit purposes. The degree of quantifying opportunities and risks associated with cryptocurrencies

[294] Lu, L., & Zhang, A. L. (2021). "The Cross-Border Use of Central Bank Digital Currencies (CBDCs): China's Experiment and Regulatory Challenges." Oxford Business Law Blog.
[295] Cihan Cobanogly and Dr Valentina Della Corte (2021). 'Ozturk and Sulungur: the Regulation Problem of Cryptocurrencies.'
[296] Michael Buchwald (2020), 'Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration,' Vol.168 issue.5, University of Pennsylvania Law Review, p.1371.
[297] Mark Verstraete, (2019) 'the Stakes of Smart contracts,' Vol.50 Loyola University Chicago Law Journal, p.762.
[298] Valeriia Dyntu and Oleh Dyky, (2018) 'Cryptocurrency in the System of Money Laundering,' Vol.4 issue.5, Baltic Journal of Economic Studies, p.75.
[299] Online gaming, social media products, art, virtual ownership and profit, etc.

is important, as it allows interested parties to scan the environment while balancing regulation which fosters innovation and counters risks. However, given the newness of this industry and its rapid changes, coupled with dark figures of crime and the extreme value volatility of certain tokens in the market, their current and potential illicit uses and typologies must be addressed in the face of opportunities. Notwithstanding the private industry's bullish stance and optimism, law enforcement worldwide is always on the lookout for the illicit use of cryptocurrencies and has multiple concerns regarding it.[300]

As nations move forward with exploration and regulation, criminal enterprises will relocate to where there are more lax regulatory environments. The development and growth of cryptocurrencies have been met with mixed reactions from public, private and law enforcement as there are difficulties in striking a concrete balance in regulating this phenomenon among the legitimate market and criminal demands for them.[301] The attraction for both capital markets and criminals is linked to the pseudonymity of the currencies and their decentralization. Both features of cryptocurrencies account for their appeal to markets and criminals alike. At the same time, both features present legislators and regulating authorities with challenges for integrating and regulating cryptocurrencies.[302]

[300] Valeriia Dyntu and Oleh Dyky, (2018) 'Cryptocurrency in the System of Money Laundering,' Vol.4 issue.5, Baltic Journal of Economic Studies, p.75.
[301] Rain Xie, 'Why China had to "Ban" Cryptocurrency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China.' (2019) Vol.18 Issue.2 Washington University Global Studies Law Review
[302] Rain Xie (2019), 'Why China had to "Ban" Cryptocurrency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China.' Vol.18 Issue.2 Washington University Global Studies Law Review.

Although interest groups and stakeholders have expressed a need for the creation of a unified law regulating and limiting the use of virtual currency, such laws still need to be improved globally.[303] Corresponding with regulatory efforts, pragmatic efforts need to be satisfactorily made for states to cooperate in identifying and extraditing cyber criminals, as will be discussed in chapters 5 and 6. Until that happens, crypto currency can be seen as a largely unregulated online shopping and trading facility for legitimate and illegitimate uses.

[303] Daniel Holman and Barbara Stettner (2018). 'Anti-Money Laundering Regulation of Cryptocurrency: US and Global Approaches.' p. 26-39. in The International Comparative Legal Guide to: Anti-Money Laundering (2018), Global Legal Group, London.

Chapter 5 – Crypto Fieldwork, High-Level Officials' Perspectives

Introduction

There is wisdom in the multitude of counsel because experience is the mother of all teachers. In this vein, I have endeavoured to interview high-level officials from the public/regulator, private/reporting entity and law enforcement/intelligence fields. These critical stakeholders with skin in the game are at the forefront of interaction(s) with the emergent Crypto space. Thus, this chapter includes qualitative data from the interviews, which is analyzed to supplement critical literature analytics. Such data gave rise to themes[304] and subthemes[305] where the chapter is divided to analyze the legal definitions, gateways, frameworks and information sharing.

Respondent's views on the Virtual/Digital Ecosystem Vulnerabilities

The preliminary question I asked the respondents related to the increasing concerns by public stakeholders over this new techno financial Crypto phenomenon. This elicited a variety of diverse, yet occasionally similar, responses. The responses not only relate to the outlook of the private/reporting entity, public/regulator and LEA/Intelligence category groups towards the Crypto ecosystem but the general views on the future of the Crypto ecosystem commonly touted as the future of finance. Across the responses, it was recognized that Crypto could only be effectively addressed: healthy market utilization and minimization of illicit use, with participation from all three categories. As the public sector cannot regulate what they do not understand,[306] the

[304] i) Security, ii) privacy and iii) safeguards
[305] i) Sanction & law enforcement evasion, ii) obfuscation, iii) velocity, iv) information sharing, v) cross-border capabilities, vi) controls/frameworks and vii) responsibility allocation.
[306] Public sector interest and involvement in this new technology was slow until recent consultations and cross-collaborations with private enterprises to assist in framing productive regulation.

private sector cannot profit without certainty in regulation,[307] and law enforcement cannot enforce the law without authority,[308] a range of responses gathered does give an indication into the divergently similar views on the ecosystem. First, from the public/regulatory category group, the views posed is indicative of the cautious approach present:

> "What we're seeing at the moment, I think it's estimated that 1% of transactions for virtual assets are criminal. Whilst that's small, in the past two years, the Crypto space has exploded with popularity and adoption. And so, the more it explodes, in general, the higher the criminal aspect is going to be. The challenge with virtual assets is by nature, it's anonymous, or it can be anonymous, and it can bypass sanctions, it can bypass law enforcement. And so, I guess, regulators are somewhat concerned. And because we don't at the moment, have a lot of countries that have actually regulated the space. You know, obviously, where you regulate, people are just going to go where there is no regulation, or they will turn to p2p transactions, and other anonymous platforms. So, it is a bit of a challenge. But global regulators need to preserve the integrity of the financial system. And Crypto is here to say. So there needs to be some type of framework. And it's very early stages, as you've noticed. The technology isn't like there is the financial institutions yet to meet their obligations. So, it's been a bit of a challenge with implementation at this stage" (A1, Public/Regulator, Deputy Director)

Where the mandate of global regulators in the context of finance is to 'preserve the integrity of the financial system,' the FATF's objective at large is to ensure that the "Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security."[309] However, such preservation is challenged by the innovative operations of illicit actors. Notably, global regulators in the international legal framework against money laundering are a classification of soft laws instead of hard ones. In the context of international law,

[307] Given the nature of blockchain and Crypto technologies, where in the global market, the domestic regulations can assist or threaten the business competitiveness. As an example, there is a larger concentration in Crypto markets present in Singapore and Hong Kong: Langley, W. et al. (2022) Hong Kong takes on Singapore for Asia's Crypto Crown. Financial Times. Available at: https://www.ft.com/content/e90add6d-326e-4898-b8c1-78f98f2d6929.
[308] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime.
[309] FATF (2013), Methodolgy for Asessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, updated October 2021, FATF, Paris, France, p.15

hard laws are binding legal instruments which grant rights and impose obligations on the parties to which it is binding.[310] Soft laws are quasi-legal instruments that are not legally binding, compared to hard laws, and have weaker teeth than hard laws.[311] However, through the evolutionary process of the fight against money laundering, these soft laws have become recognizable standards to which domestic legislation adheres. Since FATF is not a binding legal body per se, its principles must adhere to the customs of international law to satisfy the principles of *jus cogens*, and state practice.[312] Thus, national-specific frameworks mandate private/reporting entity rules of engagement. In this vein, private/reporting entities summed the views on the Crypto ecosystem in the following terms:

> "In general, Fintech is, I guess I can just term it as non-bank, financial services providers that may be specializing in different niches. And yeah, the FATF is obviously right. When you think about money laundering, in general, fundamentally, you can launder money through anything that has value. Because it's all about just obfuscating the source of where the funds came from and making them seem legitimate and giving the person associated with those funds, a sheen of legitimacy and reputation that isn't criminally related. So, anything can be used to launder money, that has any sort of value. It's just a matter of how good is it for purposes of what you want to do with it. And it's kind of really depends on the means and the ends. So, for certain ends, Fintech is probably the best tool you can use to launder money or even for certain parts of the cycle of laundering money. Like a Fintech is great to move money fast. FinTechs are also great for obfuscating things by making them cross border. So, then the information sharing that would be needed across whether law enforcement or financial intelligence units is just that much harder and cumbersome. And then it just takes more time. And by the time that information would be gleaned, those funds are likely no longer at that FinTech where they've been moved, you know, x degrees further, where now you're so far behind, you'll never catch up to them. So, in that sense, they're really good. But they also have a big weakness on the placement side. Because you can't use a FinTech unless those funds are already settled electronically in the financial system. It's just really a matter of where are they coming from. Are they coming from a traditional bank? Are they coming from maybe a Cryptocurrency exchange? Because some of these FinTechs do both. They do traditional PSP kind of payments via a domestic payment rail or Swift international rail. But they also can

[310] Evans, M. D. (2010) International Law (3rd edition) Oxford: New York. Shaw, M. N. 2003. International law. Cambridge: Cambridge University Press. Cassese, A. (2005). International law. 2nd ed. Hampshire: Oxford University Press

[311] Ibid.

[312] The principles must be what the international community accepts as non-derogable rights, See Crawford, James (2008) Brownlie's Principles of Public International Law (8th edition) Oxford Press: Oxford. p.2.

allow blockchain transactions where you can bring in Crypto, convert it, and then send it throughout payment service providers." (B2, Private/Reporting Entity, Chief Compliance Officer.)

While this is not a one-size fits all approach to the Crypto ecosystem, it does portray the recognition by the industry in terms of the capabilities of crypto, whereby such capabilities have been outlined in chapter 3. Such capabilities will be further discussed in this chapter and chapter 6. For present purposes, it is important to note that such capabilities, i.e., risks, were contemplated by FATF, outlining that the regulatory and supervisory arm of nation-states based on the risk-assessment model is not a static one and calls for continuous assessment,[313] and will vary and develop based on how risks evolve.[314] In the context of addressing the risks, the law/enforcement intelligence category group expressed a healthy degree of prudence when dealing with the new Crypto ecosystem:

"I think, Fintech is absolutely needed in terms of progressing our economy, the collaboration between, the financial sector and where technology is going, and all things from blockchain to Crypto and everything. I think the sensitive part comes down to security, and privacy aspects. So, you're always have folks that want more privacy. And then you're always going to have the government that wants to have, more insight and visibility into those actions. But I think my comments on that is that there's got to be some type of control. And it doesn't always have to be from, the typical government standpoint, there has to be some controls in place. And this is where the FinTech companies have to kind of have ownership over having the visibility into who they're transacting with, and where's the money going… you have all great intentions. But criminals will find a way to find that loophole, to use the technology, use the methods that are in place to circumvent, you know, OFAC, sanctions, circumvent money laundering, violate anti money laundering aspects. And that's what concerns us. I'm a big proponent of the technology, big proponent of Crypto and the space and everything's being done. At the same time, I want to make sure that citizens, the financial sector, and the tax system, and everything else is secure and being controlled, and not taken advantage of from a criminal standpoint." (C1, Law Enforcement/Intelligence, Director.)

[313] FATF (2012). 'International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation', FATF, Paris, France.
[314] Hinterseer, K. (2002). 'Criminal finance: The political economy of money laundering in a comparative legal context.' The Hague: Kluwer Law International; and Hopton, D. (2009). 'Money laundering: A concise guide for all businesses.' 2nd ed. London: Gower Publications.

The misuse and abuse by illicit actors are a key consideration of risks for law enforcement/intelligence stakeholders, supplemented by FATF's recommendations which ensure that nations should have a series of essential measures and regulations in place to ensure the efficacy of six core intended purposes.[315] These purposes, fundamentally, are designed to encompass "all serious offences, with a view to including the widest range of predicate offences."[316] However, a challenge of law enforcement/intelligence runs a risk of a lack of uniform agreement on what constitutes a criminal activity corresponding to a select region. This is posed as the dual-criminality dilemma, whereby the very nature of laundering can and does cross the borders of jurisdictional reach. This brings with it questions of jurisdiction and legitimacy for a nation to interfere or impede on another's sovereignty; nationality principle, ubiquity theory, and or subjective territoriality principle.[317] However, Article 6.2(c) of the Palermo Convention outlines that nation X can request jurisdiction over a crime committed in nation Y, where the predicate offence is recognized in nation X but not in nation Y, often on the foundation that the victim(s) or offender(s) are nationals of nation X.

[315] FATF Recommendations (2012) p.6, outlined the purposes of these measures to 1) Identify the risks, and develop policies and domestic coordination; 2) pursue money laundering, terrorist financing and the financing of proliferation; 3) apply preventive measures for the financial sector and other designated sectors; 4) establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures; 5) enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; 6) and facilitate international cooperation.
[316] FATF (2012) Recommendation 3 Interpretive Note.
[317] Koh, J. (2006). 'Suppressing terrorist financing and money laundering.' New York: Springer; Stessens, G. (2000). 'Money laundering: A new international law enforcement model.' Cambridge: Cambridge University Press.

Security, Privacy and Safeguards

The consistent recognition by the respondents expressed the vulnerabilities of Fintech as an area while recognizing its potential utility. As discussed earlier, this new method of value transfer can have utility. Recognizing this, there were primary themes which the respondents addressed to safeguard the integrity of the financial system and, to stop illicit financial flows. With the growth of the Crypto market, the consistent themes and sub-themes that were expressed related to security,[318] privacy[319] and safeguards.[320] While this is not an exhaustive list, these are the primary issues identified in the interviews.[321] The degree of emphasis on the themes varies between respondents *across* and *within* categories. The central reoccurring factor put by the respondents concerned regulatory landscapes. A lack of uniform clarity in legislation and its regulatory infrastructure concerning this new technology stems from the lack of uniform definitions concerning the number of functions encompassing Crypto:

> "I think it's well-founded concern primarily because regulators have been slow to extend the reach of these emerging technologies and which meant as a means to transact, without any oversight by the regulators, I think the glossy on virtual currencies and so on. It's just that, we have a technology medium to facilitate payments and transactions. But regulators have always been concerned about the informal banking system, the hawala system, and I think Fintechs have just taken that to a different level. So, the fundamental concerns are the same. You have a system that's out of reach. And with regulations changing globally to try and reign in these sorts of solutions." (B3, Private/Reporting Entity, Head of AML & Sanctions)

> "So, for example, one of the things that has been mentioned in the variety of reports is the need for the public sector to catch up in terms of understanding technology. In terms of being able to respond to them, and in having experts in house that know what they're dealing with and know what it looks like, in practice, rather than, I can tell you the definition of Bitcoin, but if you show it to me on a computer, I probably don't know how to identify it or how it works. So, you need someone at the national level working with

[318] i) Sanction & Law Enforcement evasion, ii) obfuscation, and iii) velocity.
[319] i) Information sharing and ii) cross-border capabilities.
[320] i) Controls/Frameworks and ii) responsibility allocation.
[321] As of February 20, 2022, prior to the Russia-Ukraine war.

either the police or supervisors that understand this kind of thing" (A4, Public/Regulator, Policy Analyst)

The interplay between security, privacy and safeguards stems from the inconsistent *definitional infrastructure* which, if clarified, would assist all three category groups in better interacting not only with these technologies, but also, with each other in addressing illicit financial flows. The definitional aspect is present within the following themes and will be discussed accordingly.

Security

Fundamentally, Paul Ekblom defines security as " deliberate action to reduce the risk of and from criminal events, taken before, during or after those events."[322] Whereby with "with the advent of the internet, and the communication pathways provided through it, 21st century criminals are now even more equipped with sophisticated channels and the ability to coordinate more effectively and profoundly to not only maximize predicate offences but also to enhance laundering operations."[323] In this vein, proper security is "adapting to changes in the nature and patterns of crime and reducing the rate of growth of crime."[324] This is vital as Wakefield and Gips posit that for security stakeholders "the pace of change is such that the ability to continually adapt and develop their practice is vital."[325] In essence, Martin Gill explains that when security is based on good principles and when operationally competent, it is an "essential good."[326]

[322] Ekblom, P. (2022). Facing the Future: The Role of Horizon-Scanning in Helping Security Keep Up with the Changes to Come. In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.823
[323] Daoud, G – Ch.3 p.45
[324] Ekblom, P. (2022) p.824
[325] Wakefield, A and Gips, M (2022) 'Professional Security in the Fourth Industrial Revolution.' In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.731
[326] Gill, M (2022) 'Thinking About the Benefits of Security, and the Barriers to Recognising Them.' In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.997

As will be further discussed, this essential good is not universally harmonized across nations. Where different nations have different priorities with different resources and capabilities. The respondents identified the theme of security to be a perennial issue. The security theme was attributed to several factors, or sub-themes, including the explosion of '*popularity and adoption*',[327] velocity, and pseudonymous capabilities. There was a general recognition that cryptocurrencies' velocity and obfuscation capabilities allow them to 'bypass sanctions…bypass law enforcement' for certain laundering aspects.[328] As discussed, the fluidity of these tactics is diverse, but they are nonetheless possible by entities to effectively deploy:

> "Regulatory Arbitrage, which is, if you don't like the regulatory environment in one country, no problems go to the next country. If you don't like that country, just go to other countries, because at the moment, there's still at varying levels. And the FATF is trying to drive standardization. So, this is problematic." (B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.)

The risk tolerance and prioritization of security to individual nations vary, where "crime reduction priorities and aims of nations can change over time."[329] The lack of cohesiveness in a unified regulatory approach to Crypto compromises its security, which allows for regulatory arbitrage. The security of Crypto is not only obligatory for nations but also "those parts of 'the' private sector that seem unwilling to demonstrate 'sufficient' national and *transnational* social responsibility."[330] As the free movement and accessibility of the technology are expanding, '*the more it explodes, in general, the higher the criminal aspect is going to be.'*[331] For this new ecosystem to grow and stabilize sustainably with legacy financial institutions and the public, its

[327] A1, Public/Regulator, Deputy Director
[328] A1, Public/Regulator, Deputy Director .
[329] Levi, M. (2022) 'Combatting Money Laundering: Some Considerations for Security Professionals.' In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.286
[330] Ibid.
[331] A1, Public/Regulator, Deputy Director.

security dimensions must be addressed. From the data gathered, the dimensions, or sub-themes, which emerged were i) sanction & law enforcement evasion, ii) obfuscation, and iii) velocity.

Sanction & Law Enforcement Evasion

Eren Colleen expressed an extrinsic motivation of legitimate institutions, where immediate indicators were of "avoiding penalties."[332] The fear of legitimate institutions of enforcement(s) was suggested to cause "frivolous filing where staff does not sincerely believe a transaction to be suspicious, but files anyway to avoid regulatory enforcements."[333] This form of defensive filing, or defensive reporting, will be discussed further in this chapter. Still, for present purposes, "financial institutions rarely admit to filing defensively, as it would signal noncompliance and failure."[334] This complicates and increases excessive data, which hinder LEA/Intelligence efforts to triangulate illicit use. This triangulation is a complex and strenuous cycle of enforcement, outlined by John Madinger,[335] and becomes further strained by the cross-border pseudonymous capabilities of crypto. As respondents from all category groups suggested,[336] the issue of sanction & law enforcement evasion does pose a series of challenges given the rapid adoption of these technologies. In the virtual space, there is a school of thought where, if you don't possess the keys,

[332] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.15
[333] Ibid. p.8
[334] Teng Z. (2014). Defensive SAR filing: An unnecessarily heavy burden on the AML field. ACAMS. p.4
[335] Madinger, J. (2012). Money laundering: A guide for criminal investigators. 3rd ed. Boca Raton: CRC Press p. 303
[336] A1, Public/Regulator, Deputy Director: "The challenge with virtual assets is, you know, by nature, it's anonymous, or it can be anonymous, and it can bypass sanctions, it can bypass law enforcement. And so, I guess, regulators are somewhat concerned."
B2, Private/Reporting Entity, Chief Compliance Officer: "So, then the information sharing that would be needed across whether law enforcement or financial intelligence units is just that much harder and cumbersome. And then it just takes more time. And by the time that information would be gleaned, those funds are likely no longer at that FinTech where they've been moved, you know, x degrees further, where now you're so far behind, you'll never catch up to them."
C1, Law Enforcement/Intelligence, Director: "But criminals will find a way to find that loophole, to use the technology, use the methods that are in place to circumvent, you know, OFAC, sanctions, circumvent money laundering, violate anti money laundering aspects. And that's what concerns us."

you don't own the currency. As the espoused purpose of Satoshi Nakamoto and Martti Malmi,[337] as to allow virtual currency holders to have ownership and control of their respective coins, there will always be a segment of users who prefer the decentralized, unregulated functions of the network. As for private regulated exchanges and custodians, which serve as a medium between the user and the coins, the respondents in that category group expressed willingness to assist their colleagues in the other category groups during investigations.[338] However, the sub-theme of sanction & law enforcement is often a multi-variable exercise given the nature of the technology:

> "The challenge on market is, where you have one player involved or two players involved, you now have eight, you have the Crypto itself, the service provider you have the app that they're using, you have the social media that's interacting with the app, which is interacting with the back end. So, we have a challenge of we now have five or six different entities that we have to see who has the data. Everybody has different parcels of data that we need to get our access to prove a crime. So yeah, there's a lot of gaps being filled. But it's also that market becomes infinitely larger" (C1, Law Enforcement/Intelligence, Director)

Obfuscation

The capability of Crypto is not complete anonymity but pseudonymity. This has galvanized new industries, blockchain analytics & forensics, to innovate and offer solutions to the private/reporting entities, public/regulator and LEA/Intelligence category groups. As obfuscation techniques vary in degree and structure, the primary objective is to disassociate real-world identities from virtual transactions. While legitimate cryptocurrency users prefer its privacy aspect, as opposed to masking their real-world identity due to nefarious purposes, the emergence of sophisticated obfuscation techniques poses a security risk. The risks can arise through either the

[337] Martti Malmi also known as "Sirius", was one of the early developers of Bitcoin, as evidenced by his contributions on the Bitcoin forum (Bitcointalk.org) – see Summary - Sirius (no date) Bitcointalk.org. Available at: https://bitcointalk.org/index.php?action=profile%3Bu.

[338] B2, Private/Reporting Entity, Chief Compliance Officer: "And there's a reason why I'm here. And we're really committed to complying but doing it smartly and doing it for the right reasons and not having to do things we don't have to do or don't make sense to us."

enhanced obfuscation techniques deployed or the privacy-enhanced coins/unregulated exchanges used:

> "That's what we're seeing sort of in the Crypto space…For example, I mean, one thing that you've seen as typology of money laundering is chain hopping, where actors are moving very quickly from chain to chain to obfuscate transactions…Privacy coins - Everyone is working on a solution to Monero. There's nobody, no blockchain analytics company, don't believe that if they tell you they can trace Monero. There's one in particular that says, maybe they can, but I don't think so. No one can necessarily trace through a ring signature is the issue... So, I say all of that, because look, I think that the focus is rightfully on exactly what you just described. It is on these obfuscation techniques. It is on illicit actors." (B6, Private/Reporting Entity, Head of Legal and Government Affairs.)

> "Whether it's ring signatures or whatever the case may be, where it just makes it extremely harder for law enforcement to trace those I mean, they are instituting that technology for the method of obfuscating the trail, right, so ring signatures, Schnorr signatures, they're all kind of doing that to mask the sender recipient, throw in additional addresses to throw off that that one to one, transactional detail. So, it does become much harder, we do recognize that as a challenge to law enforcement" (C1, Law Enforcement/Intelligence, Director)

For Bitcoin, digital signatures allow coins to be transferred on the blockchain to prove ownership and authorize the transfer to a new owner by digitally signing a hash of the previous transaction and the public key of the next owner. Bitcoin uses the elliptic curve digital signature algorithm. Schnorr signatures offered better upgrades for Bitcoin, which are currently used, namely, key aggregation. For example, a typical digital signature has one public key, a message to be signed, and a signature proving that the public key's owner signed the signature. However, when multiple parties wish to sign the *same message,* they must each include their signature and public key. Schnorr allows the aggregation of multiple public keys to form a single public key and combines multiple signatures to form a single signature. In other words, it enables a transaction to be signed with a single signature, notwithstanding how many addresses the funds are being sent

from. All Schnorr spends will resemble each other, invalidating several heuristic methods discussed in this chapter.

As for Monero, it is a securable, untraceable, electronic 'cash' and freely accessible to all. Monero stealth addresses prevent outputs from being associated with a recipient's public address through the usage of a one-time destination public key. These one-time public keys are only spendable by the recipient, and only the recipient is able to detect their designated output on the blockchain. Since all outputs are unlinkable, the privacy of the recipient is insured. On the input side of a transaction, the sender's privacy is ensured with the use of a ring signature. Ring signatures is a "cryptographic technique of signing a message on behalf of a group, as a member of that group. The basic property of ring signature is anonymity."[339] It allows a single person, a signer, in a group of possible signers that are fused together to sign a transaction, whereby it is impossible to definitively know who signed the transaction, providing complete anonymity.[340] In effect, the digital signature is composed of the actual signer and the non-signers (compromised of past transaction outputs pulled from the blockchain, which act as decoys) to create a ring where all members in the group are equal and valid. These outputs, together, make the input of a transaction, whereas, to a third party, all the inputs appear equally likely to be the output spent in a transaction.

> "Z cash has the ability to do shielded or unshielded transactions, most people are doing unshielded transactions. And as an exchange, you can elect to only accept unshielded transactions. And so, there are options you can require if you're dealing with someone and you're dealing with Monero, that they share an audit key with you. So, I do think that there

[339] Purohit, Richa, Ring Signature (2019). 'Presenting New Design with Keyed Hash Function'. Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, p.1

[340] Gupta, P., & Kumar, S. (2014). 'A comparative analysis of SHA and MD5 algorithm.' International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 4492-4495.

> are controls that can be put in place around those. But they're an interesting dilemma" (B1, Private/Reporting Entity, Founder & Chief Compliance Officer.)

In privacy-enhanced coins, transactions can be either transparent or shielded. Z cash provides strong cryptographic anonymity guarantees, such as a shielded transaction, which uses a "cryptographic protocol that involves zero-knowledge proofs to provide enhanced anonymity and privacy for transactors."[341] Zero-knowledge proofs are further discussed in the gateways section of this chapter. Still, for present purposes, they are "proofs that convey no additional knowledge other than the correctness of the proposition in question"[342], wherein the context of Crypto illicit use shields beneficial ownership. These anonymity-enhancing protocols are a primary focus of LEA/Intelligence, as expressed:

> "But the other aspect I mention is that the blockchain is by and large transparent in terms of what transactions are occurring, at least in Bitcoin and some more established digital currencies. So that doesn't seem to be a significant challenge from our team for law enforcement to trace transactions through the blockchain. It's always about putting a name to a wallet which is a wallet address which is challenge and that's where regulation of exchanges can help. For me an area to have interest to look out for is privacy coins. Obviously, they exist now and there are privacy wallets and so on, and whether that starts having a significant impact on blockchain analytics capabilities and so on… But for now, we see that bitcoin is still preferred. I think even on darknet marketplaces and things like that, because it's established and known and perceived as a less of a risk. So yeah, it's an area that we're watching with interest." (C2, Law Enforcement/Intelligence, Principal Specialist.)

Velocity

The speed of cryptocurrency transactions is both a strength and a weakness, coupled with its obfuscation capabilities. Indeed, the enhanced obfuscation techniques mentioned above have forced significant entities like Mastercard, Visa and SWIFT to seek extensive improvements to

[341] Hull, Isaiah and Sattath, Or (2021), 'Revisiting the Properties of Money.' p.29
[342] Goldwasser, S., Micali, S., & Racko, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, Vol.18 issue.1, p.186

their operations to counteract new transaction modes coupled with enhanced risk awareness. At its root are the correspondent banking relationships commercial banks use for cross-border wire transfers. These relationships are declining,[343] due to idiosyncratic and complex factors since the global financial crisis of 2008 and 9/11 to de-risk[344], and legacy financial institutions (traditional financial institutions) are developing protocols that will interface with distributed ledger technology systems. The ability to access the financial system is now even more possible by anyone, anywhere, with an internet connection:

> "You can do transactions with another party without any financial intermediary. And it's more radical than cash because the velocity is huge. I can transfer an unlimited amount of money digitally, because there's no physical limitation, unlike cash, which is still based on Fiat and has at least some sort of government ties and CACHE serial numbers. And I think FATF recommendations have always been focused on financial intermediaries. And they themselves recognize the limitations of what they can do when it's literally a peer-to-peer transaction with no middlemen. And what are the rules for that? No one has figured them out. And that's part of the problem. And even the FATF guidance said initially, maybe centralized exchanges should prohibit off wallet transactions. And there was a big uproar. Because this is actually part of a financial revolution where I don't need a bank to be able to deal with you. We don't have to trust each other. There's a protocol that we can use where we know you can't screw me, and I can't screw you. And that's what the FATF is struggling with." (B2, Private/Reporting Entity, Chief Compliance Officer.)

> "When we're talking about Crypto in particular, the same qualities that make Crypto such a force for good and such a revolutionary moment in the history of our financial system, is the nature of permissionless programmable. So, the age of smart contracts, you can transfer funds cross border at the speed of the Internet, allowing for things like remittances to move more quickly and cheaper than ever before. You can provide banking to anyone with a cell phone and reach far corners of the world where people didn't have opportunities to engage with the banking system before. Those same qualities permissionless, decentralized programmable, cross-border, transfers at the speed of the Internet, also make it attractive to illicit actors who want to move money at the speed of the Internet cross-border. But what I think is missing sometimes from that conversation, is the fact that those financial flows

[343] Holden, H. (2019) 'New Correspondent Banking Data - the decline continues.' The Bank for International Settlements. Committee on Payments and Market Infrastructures.

[344] Chatain,Pierre-Laurent; Van Der Does De Willebois,Emile J. M.; Gonzalez Del Mazo,Ines; Valencia,Ricardo David; Aviles,Ana Maria; Karpinski,Karol; Goyal,Sameer; Corazza,Carlo; Malik,Priyani; Endo,Isaku; Eckert,Sue E.; Abel,Don. (2018). 'The decline in access to correspondent banking services in emerging markets : trends, impacts, and solutions - lessons learned from eight country case studies' (English). FCI Insight Washington, D.C.: World Bank Group.

are also more visible than they ever have been in human history" (B6, Private/Reporting Entity, Head of Legal and Government Affairs.)

For clarity, Bitcoin transactions do not validate in real-time, but rather, "are confirmed only when a new block is mined, and that takes place by design once every ten minutes."[345] However, there is a relationship between speed and fees, where "a transaction will be processed because economically rational miners choose to validate transactions with higher fees first."[346] For comparison, "Ethereum classic and Ethereum are the cryptocurrencies with the lowest latency, showing maximum confirmation times of no more than 31 seconds."[347] The velocity of Crypto capabilities provides incentives for legitimate users to engage with the blockchain network, which in turn, provides further incentives for illicit use to leverage '*transfers at the speed of the Internet.'*[348]

Privacy

Bennett and Raab comment that it "is an almost ritual feature of any analysis of privacy…to begin with a warning about the inherent difficulty, perhaps impossibility, of defining exactly what ''privacy'' is."[349] While prima facia, this may seem counterproductive, it undoubtedly speaks to the importance of approaching the notion of privacy, arguably, a main motivator of Crypto and its users. For present purposes, Westin defines privacy as "the claim of an individual to determine

[345] Hayes, Adam, (2016) "Decentralized Banking: Monetary Technocracy in the Digital Age". Tenth Mediterranean Conference on Information Systems (MCIS), Paphos, Cyprus, p.8.
[346] Shang, Guangzhi and Ilk, Noyan and Fan, Shaokun (2022). "Need for Speed, but How Much Does It Cost? Unpacking the Fee-Speed Relationship in Bitcoin Transactions". Journal of Operations Management, p.1
[347] Baur, Dirk G. and Dimpfl, Thomas, (2020). "Information Transmission across Cryptocurrency Markets and the Role of the Blockchain," p.10.
[348] B6, Private/Reporting Entity, Head of Legal and Government Affairs
[349] Bennett, C. and C. Raab. (2006). "The Governance of Privacy: Policy Instruments in Global Perspective." Cambridge, MA: MIT Press. p.6

what information about himself or herself should be known to others."[350] In the present context of financial privacy, "people's banking and other financial information comprise an intimate portrait of their lives,"[351] where it is "it is the capacity of an individual to control what personal financial information is known to the state that is at issue."[352] This right to privacy, if it were absolute, would "make any modern tax system unworkable,"[353] and thus, "the right to privacy is not absolute. Just as free speech does not extend to defamation, inciting crime or shouting 'fire' in a crowded theatre."[354] As will be further discussed in this chapter and chapter 6 in the context of illicit Crypto use, "people's financial data provide an important picture of who they are,"[355] and such a picture, is a piece of the puzzle when triangulating illicit use and criminals. As a number of respondents noted:

> "Digital currency exchanges can't operate without the bank accounts. It's still a needed thing. I think there's an issue with perhaps the two working together in terms of harm and harmony, and also privacy issues. I feel a tipping off and privacy issues if they even were to kind of to identify a customer that was perhaps a bit dodgy, and then they said they wanted to talk to the bank. They can't talk to the bank about it… our privacy laws and tipping off doesn't allow for the conversation to flow freely between the two, either" (*C3, Law Enforcement/Intelligence, Manager Regulatory Operations.)*

> "One excuse was that the information, they couldn't provide it under section [anonymized] of the [constitution anonymized]. Another excuse was the privacy legislation. We had an argument with [Intelligence Unit Anonymized] about whether section [anonymized] was actually an appropriate part of the [constitution anonymized], because that's the unreasonable search and seizure. They said, yes, you do have to understand how our system works. And I said, well, I actually do understand how the system works. I used to be a prosecutor in [anonymized]. But the [law enforcement anonymized] isn't conducting a search; they're asking for intelligence that you hold. And under your statute, you can share intelligence. They said well, we'll print off a professor of law from the University of

[350] Westin, A. (2003). 'Social and Political Dimensions of Privacy', Journal of Social Issues, Vol.59, Issue.2. p.431
[351] Sharman, J.C.. (2009). 'Privacy as roguery: Personal financial information in an age of transparency.' Public Administration. Vol. 87 Issue. 4. p.1
[352] Ibid. p.3
[353] Sharman, J.C.. (2009). 'Privacy as roguery: Personal financial information in an age of transparency.' Public Administration. Vol. 87 Issue. 4. p.3
[354] Ibid. p.3
[355] Sharman, J.C.. (2009). 'Privacy as roguery: Personal financial information in an age of transparency.' Public Administration. Vol. 87 Issue. 4. p.3

> [anonymized]. And he will confirm that. Well, that didn't work to their advantage because the professor that we spoke to agreed with us." *(A3, Public/Regulator, Executive Secretary)*

> "So, privacy coins really force us to have conversations about the privacy of money, and your ability to control your own funds. And you also have a lot of very opinionated people in this space who have strong opinions about privacy. Obviously, criminals would love it because they assume that their actions can't be traced online and whatnot. So, the thing that I would say, from a [anonymized] perspective, is that, and I think this is true for all analytics companies, is that our technology at the moment, can trace around a privacy coin, but it can't trace through a privacy coin" *(B9, Private/Reporting Entity, Advisor on Public and Private affairs.)*

The barriers of privacy, arguably, create a dilemma where "privacy laws and tipping off doesn't allow for the conversation to flow freely between the two"[356] and consequently spurred informal relationships with LEA/Intelligence where "there was ample evidence of informal relationship building that would expedite information flows and make SAR reporting more useful to intercepting crime."[357] The theme of privacy, the freedom to conduct financial transactions with limited insight from government and financial intermediaries, is one of the fundamental principled foundations of cryptocurrencies. Whether for legitimate or illicit purposes, the capability of cryptocurrencies to disassociate the virtual identity from the real-world identity is a vital feature of this technology. This is complicated not by traditional cryptocurrency use but by privacy-enhanced coins ("PEC"), unregulated exchanges, chain-hopping, peel chain and mixers/tumblers. **Appendix IV** visually demonstrates how these methods can operate. The practicality of the pseudonymous capabilities of cryptocurrencies is both a feature and a bug. Given the sophistication of blockchain forensics and analytics, two sub-themes were identified for privacy: i) Information sharing and ii) cross-border capabilities.

[356] C3, Law Enforcement/Intelligence, Manager Regulatory Operations
[357] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.1

Information Sharing

Information sharing is set out in recommendation 25 in the FATF Recommendations. Despite this, the respondents noted this to be a re-occurring dilemma. As an interviewee stated: "*The argument is that regulations and legislations is preventing those technologies from operating, because the technology can actually exchange information. But then the regulators say you cannot exchange information across borders in this way."*[358] The information sharing and infrastructure surrounding it to allow for effective flows is scarcely present in the context of actionable data, where even if useful and needed information is present, "*they can't even share that information with anyone else, which means it's not effective.*"[359] Actionable and effective data will be discussed further in this chapter and Chapter 6, where the challenges for "money laundering in particular; information is scattered, fragmented, or missing."[360]

For present purposes, the basic level information sharing present for illicit use minimization, frustrates stakeholder abilities for effective supervision and monitoring.[361] Where Verhage noted that "information sharing and transparency – in terms of providing feedback as well as non-reported atypical constructions – may not be entirely positive in its effect on the system's

[358] A4, Public/Regulator, Policy Analyst.
[359] A4, Public/Regulator, Policy Analyst.
[360] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 479.
[361] By way of example the PATRIOT Act in the United States has a framework for information sharing (section 314) Which can be contrasted with Canada, where "Canada is the only common law country that does not allow public-private tactical-level information sharing to support law enforcement investigations (i.e., outside public/private exchange of information in an STR, from RE to FINTRAC; and outside of a production order, from law enforcement to REs). At the FIU level, FINTRAC is unable to share tactical information related to their STR intelligence back to regulated entities or to request follow up information from regulated entities on the STRs filed." Retrieved from Maxwell, N.J. (2021) "Canadian Legislation, Supervision and Operational Processes for Information-Sharing to Detect Money Laundering and Underlying Crime, set in the Context of International Practices." Future of Financial Intelligence Sharing (FFIS).

functioning."[362] Not least due to that, complete privacy will hinder information sharing, and since illicit actors deploy enhanced obfuscation methods, the information-sharing regime becomes a problem:

> "In terms of effective investigate frameworks, one of the issues that always comes out in mutual evaluation reports is the lack of interagency cooperation. So, for instance, the law enforcement authorities are constantly complaining to us when we do mutual evaluations, but they don't have an appropriate framework, either by way of MOUs or by way of policy guidelines or whatever, to share information among law enforcement agencies. We got customs, Acts, police, maybe corporate regulators that have enforcement and prosecution power. That overarching framework, to share information is a constant complaint by law enforcement authorities… And I illustrate that, because that comes through in a lot of countries. Both that have high capacity, countries like Canada, and Australia, and low-capacity countries, in the Pacific or Nepal or, Pakistan, they have the same issue. That's a priority coming out of a lot of mutual evaluations, agency cooperation frameworks." (A3, Public/Regulator, Executive Secretary)

It is suggested that delegating authority to more than one agency is a more effective way to achieve the lawmaker's intended goals,[363] where "optimal interagency coordination can reduce policy fragmentation, mitigate wasteful competition among agencies, enhance efficiency and effectiveness, change organizational and administrative cultures."[364] Interagency cooperation precedes effective investigative frameworks, where in the Crypto space, it is increasingly apparent that inter-agency and intra-agency cooperation in information sharing is such that "*we have a challenge of we now have five or six different entities that we have to see who has the data."*[365] Indeed, regarding interagency law enforcement cooperation, "lack of cooperation might be very

[362] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 482
[363] Kaiser, F. (2011) cong. Rsch. Serv. "Interagency Collaborative Arrangements And Activities." p.14-20;
Jody Freeman & Jim Rossi (2012). "Agency Coordination in Shared Regulatory Space," 125 HARV. L. REV. p. 1139-1143
[364] Hafiz, Hiba, Interagency Coordination on Labor Regulation (2021). 6 Admin. L. Rev. Accord 199, Boston College Law School Legal Studies Research Paper No. 545. p.205
[365] C1, Law Enforcement/Intelligence, Director

damaging if it results in further crime being committed."[366] Not only is law enforcement cooperation an issue, which will be discussed further in chapter 6 intelligence frameworks, but also the role private enterprises have in a transactional lifecycle. Analogous to the multitude of actors present, and their required participation in effective investigative frameworks is the introduction of the term "AML complex" by Verhage,[367] where "new policing"[368] by compliance professionals is incorporated into the "transnationalisation of policing."[369] This new policy by compliance professionals is such that "Compliance officers knew each other (a small world) and are now also allowed to exchange information on investigations."[370] Such exchange of information in the Crypto space was interestingly expressed by the following respondent:

> "BCPIF (Bank Crime Prevention and Information Framework) and they share information within this forum, where they actually share like, personal information, right? Because you have that ability, even though there's no safe harbor provision, you can still do it if you feel like you're adhering to the standards of what that to be a section says. So within Crypto, there's been some initiatives around this as well, and I'm going to talk about it. But frankly, for me, it's concerning what's currently being done in the industry. There's this telegram group, where exchanges are sharing personal customer information to try to stop or detect fraud. We're not comfortable with that. To be honest, we don't feel like that framework is there to help guard one the personal information and to make sure that the people who are part of these groups and chats have been vetted" (B2, Private/Reporting Entity, Chief Compliance Officer.)

The previous discussion briefly outlined the importance of privacy and its centrality in the role in our society, but more so, as a motivator in the Crypto space, both as a function and as a principle. Ironically, the very objective of privacy protection resulted in unintended and unanticipated consequences of privacy breaches, where, remarkably, "the problem of the

[366] Tosza, Stanislaw, (2019). "Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations" p.18.
[367] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 480.
[368] Levi, M. (1997), "Evaluating the 'new policing': attacking the money trail of organized crime", The Australian and New Zealand Journal of Criminology, Vol. 30, p.1-25.
[369] Sheptycki, J. (Ed.) (2000), "Issues in Transnational Policing." Routledge, London.
[370] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 483.

unanticipated consequences of purposive action has been treated by virtually every substantial contributor to the long history of social thought."[371] Several academics and extensive literature have enunciated stark reminders of a lack of foresight.[372] In crypto, unintended consequences of heavy-handed regulation cause regulatory arbitrage, potentially driving users and markets underground, which will be further discussed in this chapter. Now, privacy-enhancing legislations have effectively forced Crypto exchanges to resort to the informal sharing of personal information, that, much like banks, are galvanized to "avoid regulatory enforcements."[373] This pressure on private/reporting entities is further exacerbated given the need for real-time investigations, where a respondent noted:

> "The international movement of money to terrorism financing to everything, we just need more connections, because of the time it takes to get records and to get information. To have better contacts in every country that's able to quickly provide intelligence on what's occurring. Because it could be something that's very sensitive and time sensitive, and we need to act quickly versus an M-lab that may take six to 10 months before a response comes back. You know, we just can't operate in that lag." (C1, Law Enforcement/Intelligence, Director)

Cross-border Capabilities

Cryptocurrencies allow users to transact across borders. These readily available borderless capabilities, offer significant opportunities, but they also present a challenge for nations and law enforcement. As FATF notes, based on "cases reported by jurisdictions, criminals have exploited

[371] Merton, R. K. (1936). "The Unanticipated Consequences of Purposive Social Action." American Sociological Review, 1(6), p.894

[372] Mises, L.von. [1977] (2011). "A critique of interventionism"; HansF.Sennholz(Trans). Auburn: Mises Institute. Redford, A., & Powell, B. (2016). "Dynamics of Intervention in the War on Drugs: The Buildup to the Harrison Act of 1914." The Independent Review, 20(4), 509–530. Safner. R, (2016) "The Perils of Copyright Regulation," Review of Austrian Economics, 29(2): 121-137. Miron, J. A. (2003). The Effect of Drug Prohibition on Drug Prices: Evidence from the Markets for Cocaine and Heroin. The Review of Economics and Statistics, 85(3), 522–530. Lambert, K.J., Coyne, C.J. Goodman, N.P. (The fatal conceit of foreign intervention: Evidence from the Afghanistan papers. Peace Economics, Peace Science, and Public Policy 27,285 310.

[373] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.15

the gaps in AML/CFT regimes on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs."[374] As a respondent noted, *"Regulatory Arbitrage, which is, if you don't like the regulatory environment in one country, no problems go to the next country. If you don't like that country, just go to other countries."*[375] These cross-border capabilities are not all illicit but do have potential financial and economic advantages, where "*With the money grams and the western unions, they charge, sometimes as high as 12%, for the privilege of being able to send assets cross border, whereas you could get a wallet and convert those funds into Bitcoin and send them to your family in Ecuador for pennies on the dollar."*[376] However, the same potential positive utility can also be exploited by illicit enterprises, for example:

> "When the Taliban took over recently, their Crypto use skyrocketed because they didn't trust the banks. The banks didn't have the cash to give them, all of a sudden, they resorted to crypto. So, there's market elements and user elements that the FATF looks at. That is not the performance of the market. It's more who's the customer base? What's it used for? Is the market use for cross border payments? Are companies and entities starting to use Crypto as a cheap and easy and quick way for cross border remittances or terrorist organizations using that to raise funds? They will look at it from that point of view." (A1, Public/Regulator, Deputy Director)

Notably, "cryptocurrencies, like Libra or Bitcoin are created, at least in part, to facilitate cross-border payment and exchange between different currencies."[377] As will be discussed, crypto, in and of itself, is yet to be a recognized currency,[378] and the ability to be traded for fiat currency,

[374] FATF (2020), "Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets." FATF, Paris, France, p.17
[375] B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs
[376] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[377] Li, Shuping, (2023). "Towards Digital Money Interoperability: Data Governance Coordination for Cross-border Payments." Houston Journal of International Law, Vol. 45, No. 2, University of Hong Kong Faculty of Law Research Paper No. 2023/10, p.2
[378] Subject to only two countries which took a step to recognize Bitcoin as legal tender: El Salvador and Central African Republic

goods and/or services is changing. This uncertainty in its legal tender status is not lost on illicit enterprises. Where illicit enterprises do not engage in costly illicit operations to have a cryptocurrency irredeemable for any recognized currency capable of purchasing goods or services. It would be remarkable if a terrorist organization or a laundering infrastructure instituted a policy for their operational workforce for compensation in the form of a cryptographic key on a public ledger marking ownership of any coin irredeemable for goods or services in national or international markets. In this vein, crypto, is able to offer the "transfer funds cross border at the speed of the Internet… allowing for things like, remittances to move more quickly and cheaper than ever before"[379] effectively allowing for cross-border flexibility. This flexibility stems from the structure of crypto, where "differently from traditional money remittance means, cryptocurrency (CC) users do not need any professional intermediary to intervene. As soon as the user is in possession of her private key, she can immediately transfer the CCs to the holder of a public key located anywhere in the planet."[380] Based on this capability, without the need for a traditional intermediary; indeed, Crypto has stepped out of the bounds of the global banking infrastructure, "where traditional AML policies and the blockchain technology that underlies CCs collide."[381]

Safeguards

For the Crypto ecosystem to cement societal trust into a trustless capability to transact, appropriate safeguards need to be clarified and adopted. The data gathered indicated that there needs to be transparent responsibility allocation and controls/frameworks for effective safeguards.

[379] B6, Private/Reporting Entity, Head of Legal and Government Affairs
[380] Silva de Freitas, Eduardo, (2020) "Cryptocurrency Regulation in the EU AML Regime: the path towards effective harmonization?" 2nd Crypto Asset Lab Conference - CAL2020 - Milan, p.10
[381] Ibid. p.10

> "There's this consideration of ensuring that the technology is adopted in a responsible manner, that it's fit for purpose, and that it's safe as then it ensures data quality, safety, etc. So that it doesn't lead to I think everyone's nightmare situation where the firm you're working with gets hacked, and everything is stolen, and you can't retrieve whatever, data, money, investments, you had in it." *(A4, Public/Regulator, Policy Analyst)*

In the AML context, the FATF emphasizes counter-party due diligence and notes that, unlike legacy financial institutions, correspondent banking is not necessarily required to move 'value' from VASP to VASP, and thus further clarified Recommendation 16 (Travel Rule), Recommendation 15 (New Technologies), and generally the overall obligations of natural or legal entities engaging with this industry.[382] However, given the reach of Crypto abuse,[383] "*FinTech companies underestimated the amount of time and resources*"[384] it would take to provide full safeguards. It should be noted that FATF explicitly intended, later discussed in this chapter, for the Recommendations to be 'broad' to capture appropriate safeguards with this new phenomenon, given that the "FATF has observed that VAs are becoming increasingly mainstream for criminal activity more broadly."[385]

Responsibility Allocation

Given the novelty of crypto, market players have yet to cement the responsibility allocation in given transactions. Where a respondent in the private/reporting entity category group expressed, "*I don't think we really have any standards. Just a matter of where do you stop? And where does the public sector take over?."*[386] In terms of the public sector, "*We always looked at it through the*

[382] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris.
[383] In particular – ransomwares, hacks, identity theft, previously discussed in chapter 3 and further discussed in this chapter.
[384] A2, Public/Regulator, Director of AML.
[385] FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France, p.5.
[386] B2, Private/Reporting Entity, Chief Compliance Officer

basis of who's compliance responsibility is it to put in all these measures?"[387] Fundamentally*, who* is responsible for *what* is the gatekeeper model described by Gadinis & Mangels,[388] which illustrates that firms are deputized as guardians of misconduct. While compliance frameworks assist, often, it is a general approach of 'tick-the-box' culture, as opposed to organizing compliance structures to assess and adjust according to risks continuously. This resulted in what Levi et al. examined as the growth of AML without an ability to evaluate effectiveness.[389] This is further examined in the 'Cultures of Compliance' section in Chapter 6. At this point it should be emphasised that the continuous innovative cycles for this phenomenon will increase, and as such, clear standards for business models must be proactive rather than simply compliant:

> "Fintechs are less bound by geography, it comes down to how well they're being regulated in the jurisdiction where they are based, if they are, in some cases. The question is often who has the obligation to report, that if anyone in these more complex arrangements? Do they even have the information about the customers if they're sort of one step removed, or three steps removed in a more complex arrangement? What do they know about the underlying customer?" (C2, Law Enforcement/Intelligence, Principal Specialist.)

The proactiveness in responsibility allocation for crypto, is a proposition applicable to other industries, through what Garland emphasized as a 'responsibilization strategy.'[390] Particularly, it is a government which acts upon crime "not in a direct fashion agencies (police, courts, prisons, social work, etc.) but instead by seeking to activate action on the part of non-state agencies and organizations."[391] Indeed, the information seeking efforts espoused of "*What do they know about the underlying customer,"*[392] starts with the identification of "people or organizations which have

[387] A2, Public/Regulator, Director of AML.
[388] Gadinis S., Mangels C. (2016). Collaborative gatekeepers. Washington & Lee Law Review, 73(2), p.797–914.
[389] Levi M., Reuter P., Halliday T. (2018). Can the AML system be evaluated without better data? Crime, Law and Social Change, 69, p.307–328.
[390] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, 445–471.
[391] Ibid. p. 452
[392] C2, Law Enforcement/Intelligence, Principal Specialist

the competence to reduce criminal opportunities effectively, and... to assess both whether those have a responsibility to do so and whether this responsibility can be enforced."[393] Much like the banking industry, in the Crypto space, new responsibilities are now on "compliance officers viewing themselves as police officers,"[394] since "banks have now been integrated into intelligence-led policing missions."[395] This deputization of the regulated places "a growing burden to fund the policing of criminal behavior,"[396] through the implementation of controls and frameworks, which are discussed in the following section.

Controls and Frameworks

In interviews, several respondents spoke of a 'check-the-box culture' regarding AML/CFT '*where it's passable from a regulatory perspective, but they're not really thinking through it on a deep risk level.*'[397] This will be further elaborated on in the 'Cultures of Compliance' section in Chapter 6. At a fundamental level, "*We're evaluating control systems. So that's what we did. Because we convinced [anonymized], that an understanding of those control systems was key to understanding whether they were doing fundamentally a good job or not.*"[398] However, for the present purpose of illustrating the importance of the controls/frameworks sub-theme, a respondent in the private industry category expressed:

> "Where I think the biggest vulnerability is, is that within the technology sector, there's often the idea that once something new exists, that it's somehow exempt or that existing regulations don't apply to it. And we have this awkward period of trying to figure out how

[393] Hough, M., Clarke, R. and Mayhew, P. (1980), 'Introduction' to R. Clarke and P. Mayhew, eds., Designing Out Crime. London: HMSO, p.16
[394] Eren, Colleen. (2020). 'Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia.' Journal of White Collar and Corporate Crime. p.4
[395] Ibid.
[396] Eren, Colleen. (2020). 'Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia.' Journal of White Collar and Corporate Crime. p.2
[397] B1, Private/Reporting Entity, Founder & Chief Compliance Officer.
[398] A2, Public/Regulator, Director of AML.

> regulations apply. And so, I do think that there's an interesting threat in that way, in that we have technologies and business models that get deployed, that don't necessarily meet the regulatory requirements or have the appropriate controls in place…But I think there's always this like, is this exempt? This thing is new, no one has ever done this thing before. The existing regulation doesn't apply. And there tends to be a lot of the time that way of thinking about it, as opposed to thinking about what is my risk? What controls should I be applying? Where do I have a vulnerability? And am I actually addressing the vulnerability? And I think that's, that's kind of interesting from a compliance perspective, in general, because there are those two pieces to it, there's am I meeting the regulatory requirement? And then am I actually managing the risk? And you can do one without doing the other. As a Venn diagram, those never overlap fully." (B1, Private/Reporting Entity, Founder & Chief Compliance Officer.)

A deputization[399] of compliance officers to be the new police officers,[400] causes increased emphasis on proper controls where "pressure on compliance has grown as a result of the greater importance of compliance departments in relation to controls and checks."[401] When *"we have this awkward period of trying to figure out how regulations apply."*[402] It is noteworthy that greater emphasis cannot be placed on "understanding the creation of the AML specialist role,"[403] to understand and implement coherent effective controls. Deputizing the regulated to interpret the rules and ensure implementation of corresponding controls is AML "creep" described by Turner and Bainbridge, and "meta regulation" described by Jordanoska where "significant amount of responsibility is placed on the regulated for interpreting the rules, devising compliance systems, and achieving outcomes."[404]

---

[399] B2, Private/Reporting Entity, Chief Compliance Officer: "Personally, I feel like the private sector has been deputized, probably too much"

[400] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.4

[401] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 485

[402] B1, Private/Reporting Entity, Founder & Chief Compliance Officer

[403] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.2

[404] Ibid. p.2 citing from Jordanoska A. (2018). "The dark side of finance." In Campbell L., Lord N. (Eds.), Corruption in commercial enterprise: Law, theory and practice, p.171

Contextualizing Discussions

The respondents' views assisted in identifying several factors which influence their opinions on illicit activity in the Crypto ecosystem. These factors are; i) definitions of Crypto – down-up (ground level approach), ii) gateways, interoperability between systems, iii) defining regulative frameworks – top-down (bird's eye view approach), iv) attributions, v) peer-to-peer and vi) digital identity. The main factor across all three category groups refers to the legal framework's challenges,[405] and its impact on the ecosystem. The second factor refers to information sharing,[406] and its importance in relation to technology-driven data. Not only do these factors influence the themes of privacy, security and safeguards, as discussed above, they also evidence some variances *across* and *within* category groups. Each of the factors will now be discussed in turn.

The Legal Definitions – A Vacuum of Wild West

There is no shortage of this industry being called the Wild West,[407] from the United States Securities and Exchange Commission,[408] to the European Central Bank[409] and even at the FATF level.[410] Specifically, given their rapidness and uncertainty in adoption, the vagueness of roles and responsibilities of stakeholders relating to "uncertainties of blockchain technology: issuers and purchasers,"[411] where "pigeonholing them into preexisting legal categories could be the greater

[405] 1) Definitions of the legal framework – down-up (ground level approach), 2) Gateways, Interoperability between systems, 3) Defining regulative frameworks – top-down (bird's eye view approach).
[406] 1) Attributions, 2) Peer-to-peer and 3) Digital identity.
[407] The Editorial Board, (2018), "Cryptocurrency Wild West is Crying Out for a Principled Sheriff," Fin. Times.; NBX Editorial, (2019) "Wild West No More: Regulation Comes to the Crypto Corral," MEDIUM; Mari Rogers, (2018) "The End of Blockchain's Wild West is on the Horizon—Why STOs are Poised to Take the Lead, Medium."; Kelvin Chan, (2018) "UK Lawmakers: 'Wild West' Cryptocurrencies Need Regulation," AP NEWS.
[408] Gensler, G. (2021), "Remarks Before the Aspen Security Forum," U.S. Securities and Exchange Commission.
[409] European Central Bank (2022), "For a few cryptos more: the Wild West of Crypto finance."
[410] FATF, "Virtual Assets: What, When, How?" p.3; FATF virtual assets homepage.
[411] Diamantis, Mihailis, (2020), "The Light Touch of Caveat Emptor in Crypto's Wild West." 104 Iowa L. Rev. Online 11. p.115

risk."[412] Indeed, "crypto-assets are bringing about instability and insecurity – the exact opposite of what they promised. They are creating a new Wild West."[413] These frameworks stem from disagreements over their nature of money, commodity and security, which has been discussed in chapters 3 and 4 and will be discussed further in the frameworks section. Still, for present purposes, in terms of the legal definitions, respondents called for clarity:

> "I think there's a few areas, specifically the regulation side of house, how do we regulate something that we don't fully understand? but you know, how do we define it as a product?" (C3, Law Enforcement/Intelligence, Manager Regulatory Operations.)

> "And there's always been these questions around, a lot of times, it's terminology right. How do we even explain what we're trying to regulate? When there's different definitions for digital assets, digital currency, virtual currency, Cryptocurrency, Crypto asset token. There's so many that it's a challenge". (C1, Law Enforcement/Intelligence, Director.)

Given the multifunctionality of this 'instrument,' there is no universal definition of cryptocurrency. The branded definitions for Crypto were set out earlier in the taxonomy of cryptocurrencies section in Chapter 4. Unsurprisingly, this lack of a universal definition causes difficulties.

However, given the volume of multiple Crypto innovations, a concrete definition must be examined at the foundational level. This is important because "If a problem cannot be defined, it cannot be solved—or, at least, it cannot be efficiently solved—because confusion over the nature of the problem can obscure attempts to provide solutions."[414]

[412] Ibid. p.116
[413] Gensler, G. (2021), "Remarks Before the Aspen Security Forum," U.S. Securities and Exchange Commission
[414] Schwarcz, Steven L (2008)., Systemic Risk. Duke Law School Legal Studies Paper No. 163, Georgetown Law Journal, Vol. 97, No. 1. p.197.

With respect to the nature of the definition(s), it should be noted that the phrase "Cryptocurrency" is misleading. A high degree of emphasis must be placed on the definition(s) as "for the specialist, it is of utmost importance to define his terms clearly and to distinguish them sharply from one another."[415] This is important since the corresponding definitions directly affect the legal classifications, and, therefore, the subsequent AML/CFT compliance obligations and effectiveness of safeguard measures.

An analysis of the fundamental meaning of Crypto is therefore in order. "*Crypto*" is derived from the Ancient Greek word *κρυπτός* (*kruptós*). This word in English has a number of different, yet overlapping definitions: conceal, private, hidden, inward, secret. The essential meaning of the word was exemplified in *Kyrptos*, an infamous sculpture by American artist Jim Sanborn located in Langley, Virginia at the Central Intelligence Agency. Dedicated on November 3, 1990, it contained four coded and hidden messages. Three have been solved and the fourth is infamous for being one of the unsolved codes in the world.[416] In the context of computer science, it is an accepted term for *Cryptography* to be the art and science of transforming (encrypting) information (plaintext) into an intermediate form (ciphertext) which secures information in storage or transit.[417] In essence, it is the use of *transformations of data* intended to make the data *useless* to one's opponents.[418]

[415] Stephen Ullmann, (1962). "Semantics: An Introduction to the Science of Meaning." Oxford: Basil Blackwell, p.126.
[416] Karl Wang, The Kryptos Scuplture, (n.d.) Available at: https://mathweb.ucsd.edu/~Crypto/Projects/KarlWang/index.html
[417] Matt Bishop, (2003) "Chapter 9: Basic Cryptography," in Computer Security: Art and Science, Boston, MA: AddisonWesley. p.217-240.
[418] Diffle and M. E. Hellman. (1979). "Privacy and authentication: An introduction to Cryptography." Proceedings of the IEEE, Vol.67, p.397-427

Cryptography, while central to blockchain technology, has been deployed in the context of military, intelligence and banking operations with regard to security and communications.[419] With records dating as early as 1900 BC in Egypt, to Sparta, and the Renaissance as earlier versions of *transformations of data.*[420] Regulators have sought to define the multiplicity of modern Cryptography *functions* within current legal infrastructures between the identified themes: security, privacy and safeguards. Scholars continuously attempt to fill this legal vacuum through diverse theoretical lenses. To govern the regional, national and cross-border relationships related to these new phenomena, it has been suggested that digital rights, contracts and money must become objects of civil rights.[421] It has also been recommended that "the legitimization of Cryptocurrency features will also improve the efficiency of financial intelligence, as it will be possible to adapt modern anti-laundering standards and recommendations to the peculiarities of virtual currency."[422] Tufano utilized a regulatory dialytic theory,[423] coined by Kane in 1977,[424] to this area, a quasi-realistic and pessimistic approach to illustrate that as nations attempt to decrease criminal activity in financial institutions, new technologies and methods for laundering will emerge.[425] Unsurprisingly, "not only is financial innovation a historical phenomena, it is also a widespread one."[426]

---

[419] Nick Ellsmore (1999). "Cryptology: Law Enforcement & National Security vs. Privacy, Security & The Future of Commerce" Thesis, University of New South Wales.
[420] Kahn, The Codebreakers, (Abridged version 1973 The New American Library Inc.) p.69.
[421] Timofeev S A (2018). "An attempt to legalize Cryptocurrencies: will the state dare?"
[422] Bolotaeva, O & Stepanova, A & Alekseeva, S. (2019). "The Legal Nature of Cryptocurrency." IOP Conference Series: Earth and Environmental Science. p.3 citing from Shaidullina V K (2018). "Cryptocurrency as a new economic and legal phenomenon." Journal of the State University of Management" Vol.2, p.137-142.
[423] Tufano, P. (2019) BOAO Forum for Asia, March 29, 2019, Hainan Province, China.
[424] Kane, Edward J. (1977). "Good Intentions and Unintended Evil: The Case against Selective Credit Allocation." Journal of Money, Credit and Banking Vol.9.1: 55–69.
[425] Lerner, Josh & Tufano, Peter. (2011). "The Consequences of Financial Innovation: A Counterfactual Research Agenda." Annual Review of Financial Economics.
[426] Ibid. p.3

In this current state, respondents often expressed the need for clarity on the legal nature. For conceptual clarity, it is suggested that cryptocurrency, digital currency, virtual asset, digital asset and so forth should be used under the term *Crypto*. While they differ in their functions, in a strict sense, the commonality amongst these Cryptos is their use of Cryptography and distributed ledger technology or similar, which are "technological solutions that enables a single, sequenced, standardized, and Cryptographically secured record of activity to be safely distributed to, and acted upon, by a network of diverse participants."[427] Fundamentally, the records include but are not limited to: puzzles, codes, chronicles, messages, transactions, records, asset holdings and identity data. As discussed in chapter 3, DLT's purpose is to verify, validate and *chain* the data to the following sequence of blocks, popularly referred to as Blockchain. For example, the original Bitcoin genesis block was 50 BTC, which has yet to be located. The genesis block had an embedded message within the raw data: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."* **Appendix V** portrays the raw hex version of the genesis block.

FATF Definition(s)

In grappling with the definitional application, in relation to the definitions, the FATF concluded in its updated VA/VASP guidance that:

> "The definition of VA is meant to be interpreted broadly, with jurisdictions relying on the fundamental concepts contained in it to take a functional approach that can accommodate technological advancements and innovative business models. In line with the overall ethos of the FATF Recommendations, these definitions aim for technology neutrality. That is, they should be applied based on the basic characteristics of the asset or the service, not the technology it employs."[428]

[427] Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasa Sugimoto. (2022). "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." IMF Fintech Note 2022/007, International Monetary Fund, Washington, DC.
[428] FATF (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.22

The report continues on to say:

> "The key question in this context is whether the VA has inherent value to be traded or transferred and used for payment or investment or, rather, is simply a means of recording or representing ownership of something else. It bears repeating, however, that assets that do not qualify as VAs should not be presumed to fall outside the scope of the FATF Standards. Instead, they may fall under other kinds of financial assets, such as securities, commodities, derivatives or fiat currency."[429]

It is worth noting that FATF's emphasis on '*the basic characteristics of the asset or the service, not the technology it employs*' has opened a floodgate of definitions relating to this phenomenon's ever-increasing innovative functions. The FATF itself revised, added and further listed extensive definitions of Crypto characteristics in updated guidance and reports.[430] The basic characteristics of the asset or service *is* the cryptographic technology it functions on. It is trite to say the basic characteristics of the asset or the service has intrinsic value,[431] but rather the excessive fluctuating potential of monetary returns of value assigned by society to it,[432] or non-fungibility of code 'marking' ownership of intangibles.[433] Subject to that, trustless communication systems have potential advantages and corresponding illicit activity opportunities. By evading the basic *functionality* of these cryptos and attributing their classifications to the multiplicity of innovative *functions*, the FATF has effectively confused stakeholders in this industry,[434] evidenced by the

---

[429] Ibid. p.23
[430] FATF (2015) "Guidance on VAs and updated guidance in 2021". FATF 12 Month review reports and 2020 VA red-flag indicators of ML/TF.
[431] Graham B. Buffett W. E. & Zweig J. (2013). The intelligent investor : a book of practical counsel (Revised). Harper Collins.
[432] Emikönel, Murat, Volatility and the Day of the Week Effect on Bitcoin Returns (2021). Journal of Emerging Economies and Policy; Zhang, Jiarui, Analyzing and Forecasting the Volatility of Ethereum based on Econometric Models (2021).
[433] Moringiello, Juliet M. and Odinet, Christopher K., Blockchain Real Estate and NFTs (2022). William & Mary Law Review, Forthcoming, U Iowa Legal Studies Research Paper No. 2022-16.
[434] C3, Law Enforcement/Intelligence, Manager Regulatory Operations: "I think there's a few areas, specifically the regulation side of house, how do we regulate something that we don't fully understand? but you know, how do we define it as a product?"
C1, Law Enforcement/Intelligence, Director: "And there's always been these questions around, a lot of times, it's terminology right. How do we even explain what we're trying to regulate? When there's different definitions for digital assets, digital currency, virtual currency, Cryptocurrency, Crypto asset token. There's so many that it's a challenge".

uneven applications of corresponding regulation(s) by nations, if at all. Given the unending innovative cycles by private parties in re-imagining new functions through cryptography and the increased innovative typologies that illicit actors deploy, such a '*functional'* approach is likely to decrease the needed harmonization of regulations relating to the borderless nature of this phenomenon. The objective of the FATF Recommendations of cooperation and coordination is frustrated, given the diverse definitions across jurisdictions. Where from a policy perspective, "unintended effects tend to become more important the longer a given control remains in force."[435] The ripple effect of this, is that the corresponding obligations of Crypto stakeholders are fluid: custodians, intermediaries, exchanges and owners. In the context of financial crime, the themes of privacy, security and safeguards are complicated, given the multiplicity of players and their corresponding obligations in the industry. Respondents noted the complications in obligations:

> "Now where you have one player involved or two players involved, you now have eight, right. You have the Crypto itself and then you have the service provider, you have the app that they're using, you have the whatever the case may be, the social media that's interacting with the app, which is interacting with the back end. So, we have a challenge of we now have five or six different entities that we have to see who has the data." (C1, Law Enforcement/Intelligence, Director.)

> "So, the question is, how far back do you go in your investigation to report a suspicious transaction on your customer? And where this law enforcement then has to take over if they feel like it's relevant, and they want to do an investigation on a certain subject, right? Because it gets a little more murky and gray in the blockchain industry. Because that transparency of the transaction goes back to zero. So that's kind of where it gets murky. And I don't think we really have any standards. Just a matter of where do you stop? And where does the public sector take over? And again, our standards are very low for reporting. So, I feel like we can stop at a pretty shallow threshold, whereas law enforcement obviously has to prove a conviction" (B2, Private/Reporting Entity, Chief Compliance Officer.)

[435] Kane, Edward J. (1977). "Good Intentions and Unintended Evil: The Case against Selective Credit Allocation." Journal of Money, Credit and Banking Vol.9.1, p.57

A Concrete Definition – The Essence of Crypto

Legal language stems from ordinary language, since "like any technical language, the language of the law overlays ordinary language; it uses English as a foundation on which to build rather than creating a wholly new language."[436] Conceptually, legal and ordinary language are different because legal language affixes phenomena beyond ordinary language. By way of example, "due process of law" may seem vague in ordinary language, meaning general principles of fairness, equality and justice, but at law, it means a series of specific and concrete legal processes which must be followed, lest a case be put into disrepute, bringing "due process of law" in a deterministic meaning.[437] Another example would be 'unreasonable', which portrays a vague meaning at law, but as Laura Donohue argued, 'unreasonable' should be read with the legal meaning of "against the reason of common law."[438]

For crypto, the form (functionality) must precede the matter (functions). As Aristotle described "by form I mean the essence of each thing and the primary substance… by the substance without matter I mean the essence".[439] Aristotle further elaborates, regarding definitions, "a definition is an account, and every account has parts, and as the account is to the thing, so the part of the account is to the part of the thing."[440] As such, "according to this principle, the definition of a thing will include the definitions of its parts."[441]

[436] McGinnis, John and Rappaport, Michael B. (2017), "The Constitution and the Language of the Law." San Diego Legal Studies Paper No. 17-262. p.1326
[437] Nathan S. Chapman & Michael W. McConnell (2012). "Due Process as Separation of Powers." 121 Yale L.J. 1672, 1677.
[438] Laura K. Donohue (2016), "The Original Fourth Amendment," 83 U. CHI. L. REV. p.1181, 1190, 1192.
[439] Yu, J. (2001), The Identity of Form and Essence in Aristotle. The Southern Journal of Philosophy, 39: 299-312.
[440] Ibid.
[441] Yu, J. (2001), The Identity of Form and Essence in Aristotle. The Southern Journal of Philosophy, 39: 299-312.

For the present purposes of crypto, the search for a definitive legal definition must come from ordinary language, which must then supplement a legal language. The legal definitions of the multiplicity of Crypto *functions* must be defined according to their basic *functionality,* in other words, their essence. The essence central to all these *functions* is cryptographic technology, the 'parts' which form Crypto *functions*. The basic characteristics of the asset or service *is* the Cryptographic technology it functions on. If cryptography is removed from these Cryptos, then all the innovative functions of Crypto, whether a 'token,' 'Cryptocurrency,' 'digital asset,' 'virtual asset,' and so forth, cannot exist. Therefore, the centrality of legal definition pertaining to Crypto must – contrary to FATF's emphasis on "*the basic characteristics of the asset or the service, not the technology it employs,*" include the fundamental essence of the technology or service, that is, the Crypto technology it employs, which form the 'parts' of Cryptos.[442] To put it another way, if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is not a dog. As such, entrusting legal definitions to the multiplicity of innovations in the private industry, which is akin to ordinary vs. legal language, will not only potentially cause confusion but rather, has caused the "wild west" regulatory landscape of crypto.

Gateways – Interoperability between Systems

Crypto gateways are the bridge between the real and virtual worlds. This is done through what is called on-ramps and off-ramps. Regarding visibility into transactions – respondents were optimistic about the capabilities of blockchain forensics. However, the most significant emphasis placed was by a respondent in the private/reporting entity category group who summarizes it as follows:

[442] Refer to Chapter 7 conclusions for the Liechtenstein approach of a new, abstract and neutral classification.

> "In terms of regulatory clarity, I think we have a lot of space to look at in the **on-ramps and off-ramps between Fiat and Crypto**. Because at the moment, I use my X bank account to load money into Coinbase. And then I withdraw money from my Coinbase account into my X account. And I go back and forth with funding, but banks will lose sight of the money once it hits Crypto. And Crypto will lose line of sight once that money hits traditional banks. So, where we used to go between banks, from Chase to RBC, to TD Bank to whatever. The banks could follow the money. And there was a chain of correspondent banking relationships where they could see where it was going, what the money was doing. There is a SWIFT system that supports that. And there are known checks and balances. **My biggest concern is that there's a huge amount of money that's going back and forth between Crypto and traditional banking, where we just simply are blocked in terms of visibility,** because you can't track money that I put in from Chase into Coinbase that I then move into Kraken that I then move into Binance and I cash out at JPMorgan, So the hybrid Fiat- Crypto is where I'm mostly concerned, because I think we're fine Crypto-Crypto, if all the practices are in place and AML controls. **But what worries me is that hybrid between Fiat and Crypto**" (B9, Private/Reporting Entity, Advisor on Public and Private affairs.) [Emphasis added by G. Daoud]

On-ramp is a means to exchange fiat for Crypto, and off-ramp is to cash out Crypto for fiat. This process is done by service providers internationally at any time. On-ramping is done through centralized exchanges, decentralized exchanges and/or NFT marketplaces. Off-ramp can be done through exchanges, Crypto debit cards, and/or buying goods or services.[443] In its 2015 guidance on Virtual Currencies,[444] the FATF called for regulation and oversight of the "nodes" which act as gateways. These nodes and their capabilities were discussed in chapter 3. Specifically, FATF stated:

> "The risk assessment also suggests that AML/CFT controls should target convertible VC nodes—i.e., points of intersection that provide gateways to the regulated financial system—and not seek to regulate users who obtain VC to purchase goods or services. These nodes include third-party convertible VC exchangers. Where that is the case, they should be regulated under the FATF Recommendations. Thus, countries should consider applying the relevant AML/CFT requirements specified by the international standards to convertible VC exchangers, and any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system."[445]

[443] Hartford Steam Boiler showed in a 2020 study that approximately 36% of small business accept Cryptocurrency. This is on the rise with major commercial entities and institutions are now accepting coins which have 'value.'
[444] FATF (2015), "Guidance for a Risk-Based Approach to Virtual currencies," FATF, Paris.
[445] Ibid. p.6

These convertible virtual currency (VC) nodes came to be known as Virtual Asset Service Providers (VASPs). While these nodes, are not illicit, they are highly useful in the context of regulatory arbitrage. In that, their emergence across multiple regions, with varying regulations, offers a high degree of selection for on-ramps and off-ramps. Where there is heavy regulation, as one interviewee illustrated, VASPs are forced to turn to anonymity-enhancing software or are pushed underground by heavy-handed regulations.[446] Conversely, minimal regulation leads to increases in illicit activity risks. The approach by different nations of partial or complete regulation of all or some of these VASPs is considered ineffective. Thus, FATF's 12-month review of revised FATF standards concluded that many nations have yet to implement VA standards, while even those who have are still in the early stages of supervisory regime developments.[447]

At a basic level, there are licensing and registration requirements for VASPs to go through where they were "created." That is the minimum legal requirement. Subject to that, nations are free to implement further requirements for VASPs offering services/products to their citizens even if the VASPs are situated overseas. However, given the cross-border and speed capabilities of Crypto, disintegrated regulation forces innovation from illicit actors to misuse Crypto capabilities through regulatory arbitrage. This further complicates the tracking, monitoring and reporting of suspected ML/TF activities and the subsequent intelligence required in real-time to intercept funds. As regulated exchanges and compliant entities regularly engage with their counterparts to detect, deter and prevent ML/TF, the fiat-Crypto gateways are still an issue. In addressing this issue,

[446] A1, Public/Regulator, Deputy Director
[447] FATF (2020), "12-month Review Virtual Assets and VASPs, FATF" Paris, France. p.12-13

compliant VASPs attempt to, or at least in theory, should abide by law enforcement requests. As two respondents noted:

> "Law enforcement still relies on production orders. Because say, they know an account from a bank funded to X, let's just say right, but they don't necessarily know what account it went to. And that's why they reach out to X, and they say, Hey, we've got this wire transfer from RBC. Can you tell us what account it went to? And then can you provide us with all information related to that account and the transactions for that account? Unless you know who the recipient of those funds is, you can't track the transaction further. And that's why a production order comes from law enforcement" (B2, Private/Reporting Entity, Chief Compliance Officer.)

> "Through [organization anonymized] stakeholder relationships with the financial institutions, we obtain financial information through coercive powers, such as search warrants, that can be later used in a prosecution… From a LEA perspective, despite being covered by [Country anonymized] Privacy legislation, Banks do not always recognize it when we need to make urgent requests for information." (C5, Law Enforcement/Intelligence, Commander - Counter-Terrorism Investigations)

When there is little to no visibility into the fiat-crypto gateways, the powers available to law enforcement will not be as effective, given the practical considerations,[448] of pursuing data from multiple national or cross-border entities. Blockchains by themselves do not provide connections to traditional legacy systems. *Oracles,* demonstrated in **Figure 8** are the links used to connect the blockchain with external legacy systems.

[448] Jurisdictional issues, conflict of laws, administrations, resources, legislative frameworks, etc.

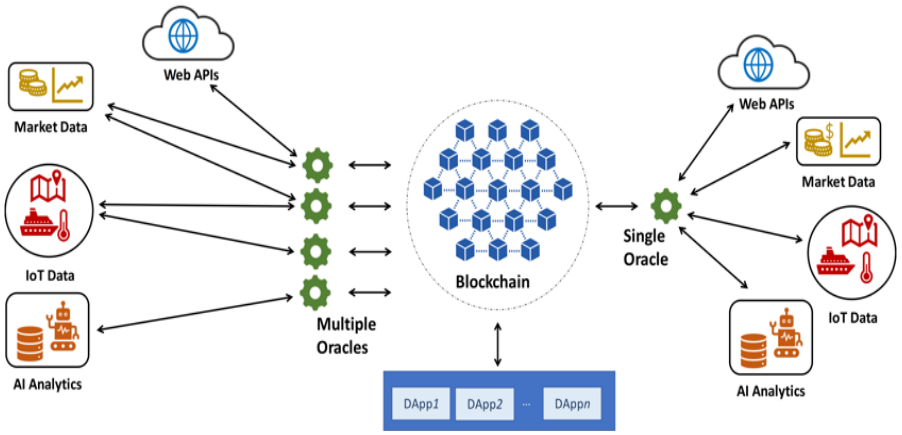


Figure 8: Basic Oracle Framework(s).

Source: Albreiki, Hamda & Habib ur Rehman, Muhammad & Salah, Khaled & Svetinovic, Davor. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. IEEE

Oracles are referenced as the invisible backbone of decentralized finance and applied blockchain applications.[449] Oracles serve as a middleware for data and transaction sharing between entities securely and authoritatively. Oracles can be tangible devices which measure real-world values (temperature, shipment delivery) or intangible such as a code (recording of external product prices on a blockchain). They are systems which operate partially on the blockchain (on-chain) and outside of it (off-chain) asynchronously.[450] Oracles' main purpose is to retrieve external data, validate it, and deliver it to the intended entity. Oracles provide the smart contracts in the blockchain with inputs, take the outputs, and then execute them as actions on external systems.

[449] Wintermeyer, L. (2021) Oracles: "The invisible backbone of defi and applied blockchain apps, Forbes." Forbes Magazine.

[450] In the context of computing and telecommunications asynchronously means requiring a form of computer control timing protocol in which a specific operation begins upon receipt of an indication (signal) that the preceding operation has been completed.

Since transactions on the blockchain are verified by nodes with high fault tolerance, then oracles become the entity which verifies the external systems to the nodes. In the context of Blockchain, Zero-Knowledge-Proofs ("ZKP") is used in terms of Cryptographic trustless interaction, where ZKP *proves possession of knowledge* regarding information without disclosing the underlying information.[451] ZKPs are used by diverse instruments, notably Cryptonote,[452] Zcash,[453] Monero,[454] and Zether,[455] to keep information private. ZKP is also used to *prove any fact* on an off-chain data point without disclosing the underlying data on-chain. Fundamentally, while this offers the pragmatic benefits of trustless verifications, it also allows for successfully obfuscating trails of funds, nationally and internationally, between on-chain and off-chain.

With greater *interoperability* from legacy financial institutions, the lack of visibility into fiat-Crypto bridges can be alleviated. Fundamentally, interoperability is concerned with the "technical, semantic and business compatibility that enables a system to be used in conjunction with other systems."[456] Research has demonstrated that "multiple reports analyzing the blockchain/DLT adoption by organizations have pointed out that blockchain integration with other systems (e.g. other blockchains or other non-DLT information systems) is one of the crucial

[451] Dor Bitan, Ran Canetti, Shafi Goldwasser, and Rebecca Wexler. (2022). "Using Zero-Knowledge to Reconcile Law Enforcement Secrecy and Fair Trial Rights in Criminal Cases." In Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22), November 1–2, 2022, Washington, DC, USA. ACM, New
[452] N. Van Saberhagen, Cryptonote v 2.0 (2013)
[453] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash (2014). "Decentralized anonymous payments from bitcoin," in IEEE Symposium on Security and Privacy. p. 459–474.
[454] S. Noether, (2015). "Ring signature confidential transactions for monero." IACR Cryptology ePrint Archive 1098
[455] B. Bunz, S. Agrawal, M. Zamani, D. Boneh, Zether (2020). "Towards privacy in a ¨ smart contract world." in: J. Bonneau, N. Heninger (Eds.), Financial Cryptography and Data Security - 24th International Conference, FC, Kota Kinabalu, Malaysia, February 10-14, 2020, Revised Selected Papers, Vol. 12059 of Lecture Notes in Computer Science, Springer, 2020, p.423–443.
[456] Bank for International Settlements (2022), "Options for access to and interoperability of CBDCs for cross-border payments", Report to the G20, p. 5.

challenges."[457] However, using standards to force interoperability may lock market participants into an inferior technology.[458] As a respondent stressed:

> "There's going to be the Crypto option and the legacy option. And those two will have to learn to play together in the sandbox. So, if these legacy anti financial crime software producers aren't open to a Crypto forensic option, and the Crypto or the blockchain forensic firms aren't open to a legacy option, they'll both die." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

The reality for regulators is starting to become more apparent. Indeed, as Chair of the Federal Deposit Insurance Corporation, Jelena McWilliams stated, "If we don't bring this activity inside the banks, it is going to develop outside of the banks. ... The federal regulators won't be able to regulate it."[459] Such a stance had been predicted by early enthusiasts and proponents of crypto; John Gilmore, one of the founders of Cyberpunks,[460] along with Eric Hughes and Tim May,[461] expressed, "We are literally in a race between our ability to build and deploy technology, and their ability to build and deploy laws and treaties. Neither side is likely to back down or wise up until it has definitively lost the race." [462] A respondent, an academic and an expert in the mechanics of cryptography, noted an interesting link:

> "In my opinion, my very firm opinion, Bitcoin, as the first one, grew out of a 1990s movement called cypherpunks. And in particular, a lot of the cypherpunks were libertarian, anarchists. They thought that a currency that was decentralized, there were no banks, or no governments involved, that was unregulated would make taxes impossible to collect, and that this would inherently cause the governments of the world to collapse. I never understood why they believe that or why they thought that would be a good thing. Nevertheless, having been on the cypherpunks mailing list in the 90s, this was a very strong belief among some subset of the cypherpunks. And Bitcoin they thought, they were wrong, they thought checked all the boxes they wanted to, for such a decentralized financial system

[457] World Economic Forum (2020). "Bridging the Governance Gap: Interoperability for blockchain and legacy systems." Technical Report.
[458] Jean Tirole (2006). "Standards and Intellectual Property: the view of an economist." Letter from the Regulatory Authority for Electronic Communications and Posts, No. 51, p. 14–16.
[459] Reuters (2021), "U.S. regulators exploring how banks could hold Crypto assets - FDIC chairman."
[460] Suggested by D1, Professor of Computer Science to be an anarchist wing of the Crypto movement.
[461] Founders of the Cyberpunks.
[462]"Cryptography Export Restrictions". www.freeswan.org. Archived from the original on 2018-09-11. See also Tim May's 1992 'Crypto Anarchist Manifesto,' replaced in **Appendix III**.

> that the governments of the world couldn't touch. One of the reasons I believe this, is that the original Bitcoin paper by Satoshi Nakamoto, whoever he, she, they, were would have been a surefire paper to be accepted in any Cryptography conference. Quite possibly would have won the best paper award. Because it solved a problem that had been unsolved for about 20 years. How do you have cash online without a trusted party like a bank, but Nakamoto chose to issue this as a white paper for enthusiasts rather than publish it academically. Which tells me that Nakamoto wanted this to be adopted, rather than have academic impact…I called Bitcoin, a lab experiment that escaped. It was not engineered. Nakamoto had the science, but not the engineering. There are variants of the blockchain that can support much higher transaction rates and have much better anonymity guarantees. But that's something that has been learned since then" (D1, Professor of Computer Science)

There is already willingness, albeit with some frustrations, by VASPs to go through the regulatory regimes required to operate and profit while alleviating ML/TF risks. This can be evidenced by the number of rising suspicious transaction reports (and their multi-national variations) recorded by the FATF. As 36 jurisdictions provided data on suspicious transaction reports (STRs) from VASPs from 2019-2020, nations reported a rise in suspicious transaction reports from 55,118 to 91,586.[463] This could be due to the volume of VASPs market growth, more knowledge of AML/CFT controls, and subsequent ability to refine their control systems with the help of blockchain forensic providers.[464] Another reason could be *defensive reporting*, as a respondent noted:

> "Defensive reporting was the realization that if we don't report anything at all, then that won't look good, because everybody knew that probably every firm was being abused by launderers, or crooks in one way, shape, or form. So, to report no transactions was not realistic. On the other hand, reporting lots of STRS draws a lot of attention. So where do you want to be? Somewhere in the middle. So, the parameters was set…we would focus solely on making sure that those fundamentals were in place, because trust me, there were plenty of gaps as early as fundamentals were in place, and that they had the abilities, the analytical abilities, were there to report. And, you know, there was all kinds of anecdotes and things that we saw flying out there. So, we were less focused on the STR reporting, and we were more focused on the underlying systems" (A2, Public/Regulator, – Director of AML).

[463] FATF (2021), "Second 12-month Review Virtual Assets and VASPs." FATF, Paris, France, p.12.
[464] Ibid

The legal frameworks around Crypto-fiat gateways present a unique dilemma and its subsequent consequences. AML/CFT regulations should focus on visibility into the interplay between on-chain and off-chain links as a collective - not different standards for VASPs and Financial Institutions. Crypto value is highly volatile and uncertain, as demonstrated by 10,000 Bitcoins exchanged for two pizzas on May 22, 2010,[465] and then valued later for tens of thousands of dollars. Currently, given the deep integration of traditional banking institutions and fiat currencies into society, Crypto must include utilization of any fiat currency to have 'value.' This exchange between the virtual and traditional financial realm provides a '*chokepoint.'*[466] As has been recognized "the biggest chokepoints and where we have our most success is when the on-ramping or the off-ramping of the virtual currency, so, for instance, getting it into the virtual currency realm. That is where we have our success in our undercover platforms and through our traditional money-laundering investigations."[467] A respondent expressed a similar sentiment:

> "The place where it has to touch the existing global financial system is the **plausible point** for regulation. There are Cryptocurrencies that are far less traceable than Bitcoin, some of these were designed by serious privacy enthusiasts, and adopted by people who wanted something less traceable. So, they could use it for ransomware or what have you. But ultimately, if I want to go live the good life in Crimea perhaps or what have you, I need to convert my Cryptocurrency to dollars, euros, yen rubles, what have you. Unless I find someone, who is willing to sell me these services for Cryptocurrency, which most places have not because the stock was too volatile, the value fluctuates too much. So, you generally have to convert at some point. And this becomes a **control point** for law enforcement and for the governments of the world. So be very interesting to see what happens in El Salvador, which is cited that Bitcoin is legal currency or something." (D1, Professor of Computer Science) [Emphasis added by G. Daoud.]

[465] Kamau, R. (2022). "What is Bitcoin Pizza Day, and why does the community celebrate on May 9, 22." Forbes Magazine.

[466] The time where criminals are most vulnerable, providing avenues for LEA/Intelligence to conduct effective identification and tracing.

[467] Subcommittee on Intelligence and Counterterrorism of the Committee on Homeland Security House of Representatives, one Hundred Seventeenth Congress First Session (2021). "Terrorism And Digital Financing: How Technology Is Changing The Threat." Serial No.117-25

The very objective of illicit actors is not to invest in costly sophisticated laundering typologies, computerized integrations and data operations to ultimately collect any Cryptographic codes (NFTs, Cryptocurrencies, tokens, etc.) irredeemable for any fiat currency accepted anywhere as serving the essential three functions of money in society.[468] That would be a foolish and non-revenue-generating utilization of resources for illicit enterprises. However, there is a distinction between illicit actors favoring this technology and Crypto maximalists who push for a new hegemony based Crypto world to completely displace traditional financial institutions. Crypto maximalists' view that the 'new' Crypto innovations will displace legacy financial institutions is simply unattainable. As a respondent noted:

> "I'm not a Bitcoin maximalist, I'm not one of these people who say Cryptocurrencies are going to usurp the central bank business model. That'll never happen. The central bank business model is way too entrenched. But what's going to happen is that they're going to be rails and the two rails are going to have to learn to work with each other, legacy is going to have to work with Crypto and Crypto is going to have to work with legacy." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

Addressing this, Cryptocurrency's security and safeguard themes can be stabilized. Allowing nations to choose partial or no regulation for borderless Crypto capabilities without synergy or an international rail is impractical. Practically, the capabilities exist to integrate these systems. From a national standpoint, 'commercial bank deposits' and 'cash' are interoperable, where under normal market conditions, they both function as 'money', that is, they are interchangeable. Any given resident can use the form of 'money' they wish to use for a payment transaction, with little friction if such a transaction cross systems. From an international standpoint, there are engagements in place for cross-border payments: continuous linked settlement (CLS),

[468] Means Of Exchange, Unit of Account and/or In-Store Value.

the Trans-European Automated Real-time Gross Settlement Express Transfer system (Target2) securities and the TARGET Instant Payment Settlement (TIPS) systems.

An analogous example is useful at this point, concerning an Indian project in the context of agriculture, utilizing interoperability between blockchain, oracles and legacy systems. The Pradhan Mantri Fasal Bima Yojana (translated as Prime Minister's Crop Insurance Scheme) was launched in 2016. This framework required several stakeholders and entities, who operate several technical systems, to collect and process data relating to crop yield and weather, conduct crop-cutting experiments to verify actual yield, remote sensing to collect large-scale data on crop impact, insurance companies to underwrite risk, and banks/governments to provide farmers with credit and welfare transfers. The scale of the operation involved $28 million hectares of crop area insured, $2 billion total insured and over 12 insurance companies involved.[469] Such capabilities exist to integrate new and legacy systems. Another example of integration can be seen with the U.S non-profit news agency Associated Press, who announced that they "will make its trusted economic, sports and race call datasets available to leading blockchains via Chainlink, the world's largest decentralized network of oracles, enabling smart contracts on any blockchain to securely interact with the [news agency's] real-world data".[470] Oracles, which are never discussed or mentioned in FATF guidelines, need to be considered and explored further for AML/CFT industry standards. The standards for these private enterprises and data processors *must* provide successful visibility between inevitable on-chain and off-chain activities.

[469]Department of Agriculture, Cooperation and Farmers Welfare Ministry of Agriculture & Farmers Welfare (no date) Pradhan Mantri Fasal Bima yojana - crop insurance: PMFBY - crop insurance, PMFBY.
[470]Associated Press (2021). "Chainlink to bring trusted data onto leading blockchains."

Big data governance considerations are key to adequate safeguards.[471] Big data, from a technical standpoint, is defined as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[472] The is known as the "3-Vs" definition of volume, velocity and variety. From a non-technical standpoint, big data refers "to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more."[473] In the Crypto ecosystem, big data analysis by Mittal illustrated a 5V approach of: volume, variety, velocity, veracity and value.[474] The usage of big data analytics was illustrated by Mittal to have led to breakthroughs of "crime, forecasting and banking."[475] Central to these breakthroughs, is blockchain forensics entities, discussed further in chapter 6, who use advanced analytics, heuristics and clustering methods,[476] to track and monitor Crypto movements.

Defining Frameworks – Systemic or Sectoral Oversight?

From a bird's eye view regulatory standpoint, attempts have been made to categorize Crypto into several areas' existing frameworks. While Crypto innovations utilize the same Cryptographic technology, their instruments' are treated as different across national legislations,

[471] A4, Public/Regulator, Policy Analyst "I think everyone's nightmare situation where the firm you're working with gets hacked, and everything is stolen, and you can't retrieve whatever, data, money, investments, you had in it."
[472] Doug Laney (2001). "3D Data Management: Controlling Data Volume, Velocity, and Variety." Gartner.
[473] Mayer-Schönberger, Viktor, and Kenneth Cukier, (2013). "Big Data: A Revolution That Will Transform How We Live, Work, and Think." Boston: Houghton Mifflin Harcour.
[474] Mittal, P. (2020). "A multi-criterion decision analysis based on PCA for analyzing the digital technology skills in the effectiveness of government services. In (2020) International Conference on Decision Aid Sciences and Application." DASA p. 490–494. IEEE; Mittal, P. (2020). "Impact of Digital Capabilities and Technology Skills on Effectiveness of Government in Public Services." In 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy, ICDABI 2020 (p. 1–5). IEEE.
[475] Mehta, Kamakshi and Jain, Renu and Mittal, Prabhat and Sharma, Shikha (2022). "Cryptocurrency: A Critical Analysis of Embedded Big Data Analytics."
[476] See 'Attributions' section later in this chapter.

FATF glossary, and interpretive notes.[477] This has caused the 'wild west' regulatory landscape and the need for a definitive legal nature, as discussed earlier in the 'Legal definitions – A Vacuum of Wild West' section. The approach to defining this instrument varies and has been attributed to "their function, the perceptions of market participants and regulatory attitudes towards them."[478] The discussions over the legal categorizations of Cryptocurrencies is nuanced and continuing, whether as a means of exchange, money, property, money surrogates, a calculation and even commodities. [479] The different definitions directly affect the legal classifications and corresponding AML/CFT obligations. The non-harmonized definitions are due to the fact that "authorities have chosen different criteria for categorizing Crypto assets across various jurisdictions and differed in definitions of related activities that would fall into the regulatory scope."[480]

In this vein, respondents often opined that the multiplicity of definitions, present and emerging, for Crypto causes confusion, inconsistent interpretations and uneven national implementations.[481] A respondent noted the frustrating categorization or 'fitting' of Crypto into existing frameworks:

[477] See FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p. 21
[478] Lee, J. (2022). Crypto-Finance, Law and Regulation: Governing an Emerging Ecosystem (1st ed.). Routledge. p.53
[479] David Yermack (2015). "Is Bitcoin a Real Currency? An Economic Appraisal" in handbook of digital currency 31 David Lee Kuo Chen ed., (2015); Söderberg, Gabriel (2018): "Are Bitcoin and other Crypto-assets money?" Economic Commentaries. No. 5/2018. Sveriges Riksbank, Stockholm.; Dong He & Karl F Habermeier & Ross B Leckow & Vikram Haksar& Yasmin Almeida & Mikari Kashima & Nadim Kyriakos-Saad & Hiroko Oura & Tahsin Saadi Sedik & Natalia Stetsenko & Concha Verdugo Yepes, (2016). "Virtual Currencies and Beyond; Initial Considerations," IMF Staff Discussion Notes 16/3, International Monetary Fund.
[480] Rodrigo Coelho, Johathan Fishman and Denise Garcia Ocampo (2021). "Supervising Crypto assets for Anti-Money Laundering." Financial Stability Institute Insights on Policy Implementation No. 31.
[481] C3, Law Enforcement/Intelligence, Manager Regulatory Operations: "I think there's a few areas, specifically the regulation side of house, how do we regulate something that we don't fully understand? but you know, how do we define it as a product?"
C1, Law Enforcement/Intelligence, Director: "And there's always been these questions around, a lot of times, it's terminology right. How do we even explain what we're trying to regulate? When there's different definitions for digital assets, digital currency, virtual currency, Cryptocurrency, Crypto asset token. There's so many that it's a challenge".

> "Even just defining what a financial product is, understanding the products that they even provide, even trying to understand who's in the landscape to bring them into the fold of legislation and regulations is a whole another thing like De-Fi, we're still trying to work out if they even fall into our legislation at the moment." C3, Law Enforcement/Intelligence, Manager Regulatory Operations

FATF purposefully left VA/VASPs definitions broad so as to "...broaden the applicability of the FATF Standards to encompass new types of digital assets and providers of certain services in those assets. It was not intended to subtract from the existing definitions."[482] However, FATF's approach of casting a wide net of potential meanings to capture the maximum types of new technologies leads to confusion rather than certainty across multiple entities using the same underlying Cryptography. This leads to "words with blurred edges"[483] with the effect that the legal nature of the assets on the blockchain technology is unclear.[484]

In considering the multitude of definitions, respondents consistently opined that the current approach is unclear, whether from a regulatory or reporting entity perspective. This is particularly so in the AML/CFT context, which we turn to now.

The regulative approach to Crypto has remained sectoral, not systematic. It is worth noting at the outset that AML laws were the first to recognize the legal status of *Cryptocurrencies* as 'money'.[485] This was influenced by the reality that payment tokens, or rather "Cryptocurrency",

[482] FATF (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" FATF, Paris, p. 22
[483] Stephen Ullmann (1962). "Semantics: An Introduction to the Science of Meaning." Oxford: Basil Blackwell, p.126.
[484] Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird (2016). "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.
[485] Peter Chapman and Laura Douglas (2018). "The Virtual Currency Regulation in the United Kingdom" in Michael Sackheim and Nathan Howell (eds), The Virtual Currency Regulation Review (The Law Reviews 2018) p.310, 329.

were fundamental to the establishment and growth of the largest online market platform for illegal activities, the Silk Road,[486] with subsequent darknet copycat platforms operating and competing daily.[487] Given the geographical capabilities of this phenomenon and its infancy in market maturity,[488] it is unlikely that one single national regulator will be able to determine the legal status of Crypto and claim exclusive oversight. Instead, an international approach is needed. Coordination from an international perspective largely relies on memorandums of understanding to avoid operational, legal and/or organizational conflict.[489] The international cooperation necessary to supervise or 'reign in' Crypto will largely depend on their legal classifications.[490] Currently, in the AML context, the FATF reports on the regulation regarding this space as "the wild west".[491] The breadth of regulatory reach is complicated by the contextualization of the quantitative nature of the problem, the data of illicit use. Given the diverging ranges of data available regarding visibility into illicit use by Crypto, the FATF itself concluded:

> "There does not yet appear to be a fully established method or widely accepted literature on how to undertake such research into P2P transactions, due to the evolving nature of blockchain and the virtual asset sector. Blockchain analytics is probabilistic, and data produced has an inherent level of uncertainty associated with it. Accordingly, the data included in this report and the conclusions drawn should be treated as a first attempt."[492]

[486] David Adler (2018). "Silk Road: The Dark Side of Cryptocurrency." Fordham Journal of Corporate and Financial Law, 21.
[487] Project Hydra recently shut down by the German authorities, Welcome2Video shut down by IRS criminal investigations as well as a copycat website "DarkScandals" – both specializing in child sexual abuse. AlphaBay and Hansa marketplaces, shut down in July 2017. DeepDotWeb shut down in 2019. Operation SaboTor and Operation Disarray shutdown over 50 darknet marketplaces.
[488] It is important to note that market maturity is not meant as only dollar value of market capitalization but rather the overall stability and segmentation of the instrument into the market, as legacy financial institutions have done as per my discussions in chapter 3.
[489] David Adler, (2018). "Silk Road: The Dark Side of Cryptocurrency." Fordham Journal of Corporate and Financial Law.
[490] Apolline Blandin and others (2019). "Global Cryptoasset Regulatory Landscape Study." University of Cambridge Faculty of Law Research Paper No. 23/2019.
[491] FATF (undated) Virtual assets homepage.
[492] FATF (2021), "Second 12-month Review Virtual Assets and VASPs, FATF." Paris, France, p. 30

As the data on illicit transactions is unsettled,[493] there have been other attempts, conceptually, to define Crypto in a legal classification(s). The legal nature of the assets built on the blockchain technology, is still unclear.[494] For useful insight, it should be noted that there is work by technical experts dedicated to the technical aspects of blockchain technology,[495] while others have addressed the comparative approach of blockchain technology and its interaction with the banking systems.[496] Whilst the classifications, the determinative legal nature, are yet to be established, the essence of the functionality of this phenomena was expressed by Nobel Prize winner Professor Milton Friedman as far back as 1999:

> "The only thing that is missing, but what will soon be - is a reliable electronic money - a method by which you can buy something on the Internet or transfer funds from user A to user B, and these users may not know each other at all". [497]

[493] Ibid. p.30. Consensus has yet to be reached on data with an "inherent level of uncertainty."

[494] Gryshova, I.I., Mityay, O.V., Kuzhel, V.V. (2015). "Evaluation of financial potential development factors in agricultural production. Actual Problems of Economics." No. 10(172). - C.169-172.7; Dong He & Karl F Habermeier, Ross B Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad & Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, Concha Verdugo Yepes, (2016). "Virtual Currencies and Beyond; Initial Considerations," IMF Staff Discussion Notes 16/3, International Monetary Fund.; Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird (2016). "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.

[495]C.E. Shannon (1949). "Communication theory of secrecy systems." Bell Systems Technical Journal, 28(4):656–715; D. Kahn (1967). "The Codebreakers." Macmillian, New York; W. Diffle and M. E. Hellman. (1979). "Privacy and authentication: An introduction to Cryptography." Proceedings of the IEEE, 67:397-427; Ronald L. Rivest. (1990) "Cryptography." In Jan van Leeuwen, editor, Handbook of Theoretical Computer Science Volume A: Algorithms and Complexity, chapter 13, p. 717- 755. Elsevier and MIT Press.; Kshemkalyani A (2008) "Distributed Computing. Principles, Algorithms And Systems." Cambridge: University Press.

[496] Barrdear J. and Kumhof M (2016). "The macroeconomics of central bank issued digital currencies"; MacDonald T.J., Allen D.W.E., Potts J. (2016) "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking." In: Tasca P., Aste T., Pelizzon L., Perony N. (eds) Banking Beyond Banks and Money. New Economic Windows. Springer, Cham.

[497] Milton Friedman predicts bitcoin in 1999 (2013) YouTube. Taxpayer's Union. Available at: https://www.youtube.com/watch?v=leqjwiQidlk&t=60s.

The idea of private money itself is not new; in 1976, for example, an Austrian-British economist described a "currency independent from banking and governmental".[498] As the legal definition(s) of Crypto is currently the subject of discussions amongst stakeholders, basic considerations are attributing it to national existing legal frameworks of 'money', hence the loosely used term, *Cryptocurrency*. Research into Crypto is developing continuously, given the newness of this industry and the increasing interest(s) in it. As such, nations approach Crypto differently and the diverse approaches nations have used can be found in various national-specific legislation(s).

Attempts to date have either taken the approach of squeezing functions of this phenomenon into existing legal frameworks (commodity, non-documentary securities, MSBs, foreign currency, etc.), or recognizing it as a fundamentally new phenomenon and creating the corresponding legislative frameworks as brand new. Undoubtedly, a body of established Crypto jurisprudence has yet to crystalize fully since the "new Crypto-asset market structure cannot be created without introducing new laws and rules, and this requires the establishment of a new social contract for governance based on new legal doctrines that transcend 'contract' and "property.'"[499]

Jurisprudence is still in the early stages of conceptualizing this Crypto phenomenon into a definitive legal category. Several early cases have engaged with the intangible nature, its rights for ownership and the authority to transfer such ownership. Similarly, there is a school of thought,

[498] Hayek, F. (1976). "The Denationalization of money." The institute of economic affairs. London
[499] Lee, J. (2022) "Crypto-assets law and regulation." In Crypto-Finance, Law and Regulation: Governing an Emerging Ecosystem (1st ed.). Routledge. p.53

where there is no engagement with Crypto, to emphasize transaction blacklisting.[500] However, this approach can be quite counter-productive:

> "It could happen that FATF puts in a regulation and acknowledges that it can credibly have these platforms too to meet those obligations. And so, at that point, do they then get shut down? If they're operating in Japan, and Japan can't regulate them, and they can't meet their obligations, then should they be operating? So that's what's happening with the VASPs that have been banking with or then transferring on un-hosted wallets or privacy coins or enabling those anonymizing software and transactions or are hopping due to shut down there. But then they go underground. And I think there's a real acknowledgement that you don't want to push them under either. It's better to have some type of oversight than none." (A1, Public/Regulator, Deputy Director)

The '*real acknowledgement that you don't want to push them under either*'[501] echoes Grabosky's anticipatory diagnosis where "regulators would be wise to consider those elements of a target system that might subvert their regulatory objectives."[502] A regulatory objective for intervening to introduce Crypto regulations, by its sheer act, is to establish order and minimize illicit use in order to "minimize the negative externalities in question."[503] Where the "choice of regulatory instruments should serve to neutralise or otherwise counteract those negative tendencies which cannot be 'designed out.'"[504] This should not only be a careful consideration on what needs to go right by the introduction of regulatory intervention, but also "the ability to think about what could possibly go wrong and who has an incentive to make it go wrong."[505] In other words, counterproductive regulation should primarily be considered to "enable decision makers to

[500] Moeser M, Boehme R, Breuker D (2013). "An inquiry into money laundering tools in the Bitcoin ecosystem." In: Proceedings of the APWG E-Crime Researchers Summit. Anti-Phishing Working Group, Inc. p.1–14; Boehme R, Grzywotz J, Pesch P, et al (2017). "Bitcoin and Alt-Coin Crime Prevention." Erlangen: BITCRIME Project.
[501] A1, Public/Regulator, Deputy Director.
[502] Grabosky, P. N. (1995). Counterproductive regulation. International Journal of the Sociology of Law, Vol. 23 Issue.4, p.25.
[503] Ibid. p.24-25.
[504] Grabosky, P. N. (1995). Counterproductive regulation. International Journal of the Sociology of Law, Vol. 23 Issue.4, p.25
[505] Weimer, David and Aidan Vining (1992). "Policy Analysis: Concepts and Practice." Englewood Cliffs, NJ, Prentice Hall. p.331.

anticipate negative consequences, to prevent them if possible, and where not, to minimise their impact."[506]

Furthermore, A1, Public/Regulator, Deputy Director's analysis is consistent with FATF's underlying theme where "countries that have such frameworks may clarify to their private sector that such FIs might not be on the designated VASPs lists, or even not under the supervision of the same regulator, to *avoid unnecessary de-risking*."[507] Pushing any industry out of the scope of regulation will inevitably contribute to illicit market development, where risks are enhanced given the features of Crypto.

Respondents in the law enforcement/intelligence and public/regulator category groups contended that their focus is on the underlying systems, the governance frameworks, and the continuous risk assessments to measure and enhance effectiveness, and not only simple compliance with the increasing functions of this Crypto phenomena.[508] This is because proactive and continuous risk assessments, later discussed in the cultures of compliance section in Chapter

[506] Grabosky, P. N. (1995). "Counterproductive regulation." International Journal of the Sociology of Law, Vol. 23 Issue.4, p.26

[507] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris. p.64 [Emphasis added by G.Daoud]

[508] A2, Public/Regulator, – Director of AML: "If you've got a client at zero risk for money laundering, and then you see unusual activity, your systems should flag that up, and have a way of investigating it. And either eliminating it, because it's not suspicious at all, or it requires further investigation. So, at some point, you got to ask yourself, we've got to get all these red flags. What are we doing? There was no "what are we doing?" So, somebody put in a system to red flag these on your transactions. And all we saw in the records was a set of initials and "not suspicious," but no rationale for why it wasn't suspicious. And no collation of these reasons into a set of analyses of the underlying reasons why something was unusual, but not suspicious."
C1, Law Enforcement/Intelligence, Director: "So, to the private sector and ecosystem, why should I comply? Is there efficiencies on their end that will assist or make it better for them? What can we do that might be able to make it easier for us to identify criminals, but not provide too much of a burden to the ecosystem? Or take away what made the Crypto space enticing?"

6, are more effective than compliance projections, i.e., *defensive reporting*, when addressing illicit activities.

With respect to legal interpretation(s), courts themselves have reached varying conclusions when approaching crypto-related matters. For example, the European Court of Justice (ECJ) in *Skatteverket v. David Hedqvist* held that "it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators."[509] In the Japanese court case *MtGox*, the court approached Bitcoin as property with trepidation.[510] In *AA v. Persons unknown and Bitfinex*[511] (English law) and *Bitspread v. Paymium*[512] (French law) the courts expressed willingness to treat Crypto assets as transferrable intangible property. In November 2019, LawTech Delivery Panel presented a 'Legal statement on Crypto assets and smart contracts' whereby members of academia, judiciary and other professionals explored whether Crypto is personal property in English law. Specifically, the panel's findings emphasized that, at least in English Law, the treatment of Crypto assets as property will ultimately depend on the "***nature*** of the asset, the ***rules*** of the system in which it exists, and the ***purpose*** for which the question is asked"[513] (emphasis added). As such, the panel found that (i) Crypto-assets have all of the indicia of property, (ii) their novel or distinctive features do not disqualify them from being property, (iii) nor are Crypto-assets disqualified from being property as pure information, or because they might not be classifiable either as things in possession or things in action, (iv) Crypto-assets are therefore to be treated in principle as property,

[509] Judgement of the European Court of Justice of 22 October 2015 in Case C-264/14, Skatteverket v. David Hedqvist
[510] Judgment of the Tokyo District Court, Civil Division 28, of 5 August 2015, MtGox; An unofficial English translation of the judgment is available at https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf
[511] AA v Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019)
[512] Judgment of the Commercial Court of Nanterre, France of 26 February 2020, Bitspread v. Paymium
[513]UK Jurisdiction Taskforce (2019). "Legal statement on Cryptoassets and smart contracts."

but (v) a private key is not in itself to be treated as property because it is information.[514] The panel focused not on the *functions* of Crypto, as the FATF has, but rather focused on the *fundamental characteristic functionality* of Crypto which is (a) intangibility; (b) Cryptographic authentication; (c) use of a distributed transaction ledger; (d) decentralisation; and (e) rule by consensus.[515] In line with this, the regulatory focus of this Crypto phenomenon must be on the digital property and data governance frameworks but must also go further, as Lee alluded to transcend 'contract' and 'property.'[516]

Information Sharing

According to FATF, "effective information sharing is one of the cornerstones of a well-functioning anti-money laundering/counter-terrorist financing (AML/CFT) framework."[517] For Crypto products, "cross-border information sharing by authorities and the private sector with their international counterparts is critical in the VASP sector."[518] Indeed, Amicelle and Chaudieu emphasized that, in the context of information-sharing tensions, "tensions in transnational financial intelligence are due either to a lack of capacity to respond to a request, to the low level of spontaneous dissemination, or to 'abusive' restrictions on the use of information."[519] An analogues example is evident in the context of beneficial ownership information and the transparency

[514] Ibid.
[515] UK Jurisdiction Taskforce (2019). "Legal statement on Cryptoassets and smart contracts."
[516] Lee, J. (2022). Crypto-Finance, Law and Regulation: Governing an Emerging Ecosystem (1st ed.). Routledge. p.53
[517] FATF (2016-2017), "Consolidated FATF Standards on Information Sharing," FATF, Paris , updated November 2017. p.6
[518] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" FATF, Paris. p.77
[519] Anthony Amicelle and Killian Chaudieu (2018). "In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units." in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.665

required, where "without access to information on beneficial owners and control of legal persons, it is not possible to match financial traces to an identity."[520]

The continues efforts to create national beneficial ownership registries are not limited "to existing national databases but also focus on the systematic creation of new databases."[521] The rationale of this triangulating is "any kind of natural and legal persons linked to money that is 'dirty' because of either its origin or its use."[522] Complicating matters is Amicelle and Chaudieu's analysis of FIUs, where "response time is still a concern for all the FIUs we examined, which sometimes receive the requested information but several months too late to be relevant."[523] This is particularly important, as discussed by a respondent, emphasizing the inability to operate with extensive lag.[524] In the context of Crypto, while movements of transactions are 'visible' on an open-ledger, it does not necessarily mean that the information is 'shared.' The pseudonymity of Crypto is both a feature and a bug, where unlike banks which contain an identity relating to "information on the account's opening, modification, and closing."[525] Often, Crypto user identities are segmented and spread across multiple parties,[526] complicating matters for law enforcement/intelligence. Furthermore, on the private/reporting entity front, the information is

[520] Ibid. p.667
[521] Ibid.
[522] Anthony Amicelle and Killian Chaudieu (2018). "In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units." in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.668
[523] Ibid. p.669
[524] C1, Law Enforcement/Intelligence, Director: "Because it could be something that's very sensitive and time sensitive, and we need to act quickly versus an M-lab that may take six to 10 months before a response comes back. You know, we just can't operate in that lag."
[525] Anthony Amicelle and Killian Chaudieu (2018). "In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units." in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.667
[526] C1, Law Enforcement/Intelligence, Director: "So, we have a challenge of we now have five or six different entities that we have to see who has the data. Everybody has different parcels of data that we need to get access to prove a crime."

further complicated where *"unless you know who the recipient of those funds is, you can't track the transaction further. And that's why a production order comes from law enforcement."*[527] Indeed, not only the internet but the capabilities of Crypto, discussed in Chapter 3, provide "good news for those who are trying to launder their money is that, in the modern globalized world, money flows across borders with the touch of a button."[528]

Respondents highlighted pressure points relating to this industry regarding the information *and* data which is shared, but more so, information and data unavailable for sharing.[529] With regards to the FATF Recommendations, and the totality of this Crypto phenomena, if all the Crypto movement information were to be readily available for law enforcement, in the context of visibility between on-chain and off-chain and successful attributions, notwithstanding privacy-enhancing software/coins and self-hosted wallets, that would strike a major blow to illicit infrastructures and professional launderers operating on the dark web. Given that international regulatory consensus in this space will never be matched with Cryptographic consensus technologies and their increasing utilities, the regulative frameworks should therefore focus on harmonizing systemic standards for data collection and information sharing between the real-virtual worlds.

---

[527] B2, Private/Reporting Entity, Chief Compliance Officer.

[528] Mouzakiti, F. (2020). "Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive." New Journal of European Criminal Law, Vol.11 Issue.3. p.352

[529] B9, Private/Reporting Entity, Advisor on Public and Private affairs: "My biggest concern is that there's a huge amount of money that's going back and forth between Crypto and traditional banking, where we just simply are blocked in terms of visibility."
C1, Law Enforcement/Intelligence, Director: "And then when these blockchain analytic companies are still in the infancy of building out capabilities to trace multiple coins and trace across smart contracts and trace NFT's, there's not a lot of data that goes along with those."
B2, Private/Reporting Entity, Chief Compliance Officer: "A Fintech is great to move money fast. FinTechs are also great for obfuscating things by making them cross border. So, then the information sharing that would be needed across whether law enforcement or financial intelligence units is just that much harder and cumbersome. And then it just takes more time. And by the time that information would be gleaned, those funds are likely no longer at that FinTech where they've been moved, you know, x degrees further, where now you're so far behind, you'll never catch up to them"

Attributions

The fundamentals and techniques of attributions must first be outlined in order to contextualize the data gathered. Attribution, in a basic sense, focuses on gathering evidence to prosecute an individual. In the Crypto world, technical attribution is relevant to "the ability to associate an attack with a responsible party through technical means based on information made available by the cyber operation itself—that is, technical attribution is based on clues available at the scene (or scenes) of the operation."[530] Blockchain forensics are conducting around-the-clock heuristics and monitoring to successfully attribute illicit funds to actors. The techniques and degree vary, whether from time clustering, multiple input addresses, and/or one-time change address.[531] Notable blockchain forensic providers have successfully assisted all three category groups in getting closer to de-mystifying some illicit transactions based on data clustering.[532]

There is work related to Ethereum based clustering whereby exchange deposit address reuse and deposit address reuse, self-authorization, and airdrop multi-participation have been

[530] Lin, Herbert. (2012). "Escalation Dynamics and Conflict Termination in Cyberspace." Strategic Studies Quarterly 6 no. 3 p. 46–70.

[531] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, (2013). "A fistful of bitcoins: Characterizing payments among men with no names," in Proc. Conf. Internet Meas. Conf. (IMC),p.127-140; F. Reid and M. Harrigan, (2011). "An analysis of anonymity in the bitcoin system," in Proc. IEEE 3rd Int. Conf. Privacy Secur., Amsterdam, The Netherlands, Oct. 2012, p.16-20; E. Androulaki, O. G. Karame, M. Roeschlin, T. Scherer, and S. Capkun, (2013). "Evaluating user privacy in bitcoin," in Financial Cryptography and Data Security, A.-R. Sadeghi, Ed. Berlin, Germany: Springer, 2013,p.34-51.

[532]B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs: "For example, if you'll use our tool and you put in a wallet address, or you'll put in a specific transaction address, the data that pings goes back earlier, in terms of potential illicit activities that wallet might have been associated with. If you use a tool that's only been collecting illicit activity and kind of clustering them since 2018, or 2021, or 2020, you're missing out. Because it doesn't have that duration, that history of the blockchain to check against…So those three, law enforcement and regulators, to financial institutions, sort of large financial institutions that are thinking about how to engage with Crypto. I think it's really what you're doing. So, we have a tool that we use across those three verticals. And that one tool includes a forensics tool, which is used as a tracing tool, essentially, to follow the flow of funds. And investigators use and compliance officers use that. And we also have a transaction monitoring solution, which is used primarily by financial institutions and Crypto businesses as part of their Crypto compliance stack. So, it is essentially, it's the same data set, the same tool being used across those three verticals."

demonstrated to be effective heuristic techniques.[533] The actual and potential 'anonymity' through firmer definitions of one-time change address and multiple input addresses for address clustering is utilized.[534] While other work focuses on supervised machine learning to predict unidentified entities for attributions.[535] Linking of IP addresses where transactions have originated to de-anonymize Bitcoin users has also been examined, whereby applicability to users behind firewalls or NATs of their ISPs has been suggested.[536] Network observations relating to correlating IP addresses with transactions likewise have been undertaken.[537] BitIodine was designed and implemented to parse the blockchain, and cluster addresses which are likely to belong to a group of users or one user to classify them and label them.[538] Heuristic-based address clustering typologies have also been linked to de-anonymizing The Onion Router ("**TOR**") users through the exploitation of onion websites, the blockchain, and social networks.[539] The multiplicity of these investigative techniques and scholarly research, along with blockchain forensic providers, has contributed to and assisted LEA and reporting entities to have insight into the massive volume of transactions conducted.

---

[533] F. Victor, (2020). "Address clustering heuristics for Ethereum," in Financial Cryptography and Data Security, J. Bonneau and N. Heninger, Eds. Cham, Switzerland: Springer, p.617-633.
[534] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy,G. M. Voelker, and S. Savage, (2013). "A fistful of bitcoins: Characterizing payments among men with no names," in Proc. Conf. Internet Meas. Conf. (IMC), p.127-140.
[535] M. A. Harlev, H. S. Yin, K. C. Langenheldt, R. Mukkamala, and R. Vatrapu, (2018). "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," in Proc. 51st Hawaii Int. Conf. Syst. Sci., p.1-10.
[536] A. Biryukov, D. Khovratovich, and I. Pustogarov, (2014). "Deanonymisation of clients in bitcoin P2P network," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS). New York, NY, USA: Association for Computing Machinery, p.15-29.
[537] T. Neudecker and H. Hartenstein, (2017). "Could network information facilitate address clustering in bitcoin?" in Financial Cryptography and Data Security, M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, Eds. Cham, Switzerland: Springer, p.155-169.
[538] M. Spagnuolo, F. Maggi, and S. Zanero, (2014). "Bitiodine: Extracting intelligence from the bitcoin network," in Financial Cryptography and Data Security, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, p.457-468.
[539] H. A. Jawaheri, M. A. Sabah, Y. Boshmaf, and A. Erbad, (2020). "Deanonymizing tor hidden service users through bitcoin transactions analysis," Comput. Secur., vol. 89, Art. no. 101684.

Open-source intelligence on a surface level is readily available. For example, with regard to public Bitcoin addresses, they always start with the characters 3 or 1, are formatted to Base58,[540] and are 34 characters long. Search engines like google can be used if the address is known. However, search engines do not allow searches that use pattern-based searches or that use regular expressions, so a search engine cannot be asked to "look for any and all addresses in its index for the whole web or for a specific site".[541] Compensating for this, there are tools such as Httrack and Agent Ransack which allow searches for the entire structure of downloaded web pages in coordination to match with specified regular expressions to locate any Bitcoin address, and the regular expression can be adjusted to look for other Cryptocurrency addresses.[542] With regards to private keys, they can come in a number of different formats.[543] They can also be in the form of mnemonic code words called a "seed". Software tools like online recovery engines can be used to reverse the seed back into the private key. With regards to physical seizures of private keys from technological tools (phones, computers, tablets), there are commercial data-carving tools like Guidance Software's EnCase, AXIOM, Forensic Toolkit (FTX) and more. Recently, there has been a shift from imaging RAMs (random access memory) controversy due to running an executable on a suspect's computer to an accepted attitude of imaging RAMs as a priority, evidenced by the increase in RAM imager tools like Belkasoft Live RAM capture and MAGNET RAM capture to counter RAM dumps.

However, the information sharing required in the context of attribution of wallet addresses to illicit activity and associating that with multiple addresses and/or multiple identities becomes

[540] Encoding methodology which converts a Cryptocurrency address into a shorter and more-user-friendly format.
[541] Furneaux, N. (2018). "Investigating Cryptocurrencies" (1st ed.). Wiley.
[542] Ibid.
[543] Standard 256-bit hex (64 characters long, Wallet Import Format (51 characters long)

complex for law enforcement and favorable to illicit actors. With regard to deeper dives into attributions and the corresponding results, whether false positives or negatives, respondents in the LEA/Intelligence and Public category group expressed a healthy degree of awareness when dealing with this emerging phenomenon:

> "It's the devil we don't know. And I always used to say that when we were dealing with other cases. That information that we're just not aware of, I mean, in these all these blockchain analytical platforms, they try to identify darknet markets or, these mixers, tumblers, or things like that, that are nefarious, and being able to identify the volume that's going through these type of accounts just on a surface level, and then compared to the larger total volume of transaction. So that's where they come up with that, that amount of 1%. But to your point, we don't know all the attributions to all of these markets, and all of these illegal services and things going on. So there certainly is a variance of Delta there" (C1, Law Enforcement/Intelligence, Director.)

As rightly expressed by the respondent in that blockchain forensics works "*identify the volume that's going through these type of accounts just on a surface level, and then compared to the larger total volume of transaction,"*[544] where *"we don't know all the attributions to all of these markets, and all of these illegal services and things going on. So there certainly is a variance of Delta there."*[545] In essence the attributions are highly important since *"*even though investigators can follow the funds by analyzing the blockchain, they may not be able to connect those funds to a culprit in the real world. We have received 'Mickey Mouse' who resides at '123 Main Street' in subpoena returns."[546] The routinely touted figure that estimated Crypto crime accounts for 1% of Crypto,[547] must be taken with a grain of salt since "the estimator is not a simple sum of

[544] C1, Law Enforcement/Intelligence, Director
[545] C1, Law Enforcement/Intelligence, Director
[546] Forgang, George, (2019). "Money Laundering Through Cryptocurrencies." Economic Crime Forensics Capstones. p.13
[547] Chainalysis (2023) - 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking."; Schickler, J. (2022) "How big is Crypto crime, really?" Yahoo Finance.

observations."[548] Where the 1% crime figure risks a classic observational (measurement) error of the difference between a measured value of a quantity and its true value.[549] In other words, it should be known that "these errors are 'known unknowns."[550] Where previous research has expressed, relating to dark figures of crime geographically, that "areas with more citizens without qualifications have a larger dark figure of crime."[551] Where the dark figure crime estimations were merely on a small sample size of a particular georgical region. In the context of Crypto, a global internet-operative pseudonymous high-velocity phenomenon, it is important to recap the estimations.

The estimates relating to illicit use were at least $4 Billion in 2017, to $14 Billion in 2021.[552] Reports suggest the extent of illicit use increased to over $20 Billion in 2022,[553] where "this is a lower bound estimate — our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that this figure doesn't capture proceeds from non-Crypto native crime (e.g. conventional drug trafficking involving Cryptocurrency as a mode of payment)."[554]

[548] David W. Hosmer, Stanley Lemeshow and Susanne May (2008), "The Delta Method," in Applied Survival Analysis: Regression Modeling of Time-to-Event Data. p.355
[549] Dodge, Y. (2003) The Oxford Dictionary of Statistical Terms, OUP.
[550] Brown AW, Kaiser KA, Allison DB. (2018). "Issues with data and analyses: Errors, underlying themes, and potential solutions." Proc Natl Acad Sci U S A. Vol.115 Issue.11, p.2563-2570.
[551] David Buil-Gil, Juanjo Medina, Natalie Shlomo, (2021). "Measuring the dark figure of crime in geographic areas: Small area estimation from the Crime Survey for England and Wales." The British Journal of Criminology, Volume 61, Issue 2. p.380
[552] Chainalysis (2022). "2022 Crypto Crime Report."
[553] Chainalysis (2023). "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking."
[554] Ibid.

Attributions and de-anonymizations are extensive exercises, apart from the "*the devil we don't know"*[555]*,* which is, the dark figure of crime. De-anonymizing a user through transaction historical analysis of a given account to attribute to transaction history is available.[556] Whether public keys are posted as they are through online forums (Bitcoin forum)[557], or voluntarily as a mechanism of trust bargaining,[558] a de-anonymization inquiry was already conducted to link IP addresses to public key users.[559] This presented the capability to map IP addresses, with the assumption that the real-world identity is in-fact the identity of the sender/receiver.[560] Further studies conducted identified 40% of Bitcoin users despite implanting privacy measures recommended by Bitcoin,[561] and further behaviour-based clustering methods allowed linking of geographical users and corresponding transactions and registered businesses with an 80% accuracy.[562] Increased privacy attacks have been demonstrated to be linked to the so-called anonymity behind these systems,[563] given the inferences of user social ties from geographical data along with transaction history.[564] The Blockchain forensic intelligence varies in reliability,[565] and service providers do not always have the historical clustering required for successful attributions:

---

[555] C1, Law Enforcement/Intelligence, Director

[556] Taylor, M.B. (2013). "Bitcoin and the age of bespoke silicon", International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), Montreal, p.1-10.

[557] Reid, F. and Harrigan, M. (2013). "An analysis of the anonymity in the Bitcoin system", in Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N. and Pentland, A. (Eds), Security and Privacy in Social Networks, Springer, New York, NY.

[558] Taylor, M.B. (2013), "Bitcoin and the age of bespoke silicon", International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), Montreal, p.1-10

[559] Kaminsky, D. (2011), "Black Ops of TCP/IP Presentation." Black Hat, Chaos Communication Camp, Las Vegas.

[560] Shentu, Q. and JianPing Y (2015). "A blind-mixing scheme for Bitcoin based on an elliptic curve Cryptography blind digital signature algorithm."

[561] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013). "Evaluating user privacy in bitcoin." In Sadeghi, A.R. (Ed.), Financial Cryptography and Data Security. Lecture Notes in Computer Science, Springer, Berlin, Vol. 7859.

[562] Ibid.

[563]Narayanan, A. and Shmatikov, V. (2009). "De-anonymizing social networks", Proceedings of the 30th Symposium on Security and Privacy, Oakland, CA, p.173-187.

[564] Crandall, D., Backstrom, L., Cosley, D., Suri, D., Huttenlocher, D. and Kleinberg, J. (2010). "Inferring social ties from geographic coincidences." Proceedings of the National Academy of Sciences, Vol. 107 No. 52, p.22436-22441.

[565] Since "Blockchain analytics is probabilistic, and data produced has an inherent level of uncertainty associated with it." Source: FATF (2021), "Second 12-month Review Virtual Assets and VASPs." FATF, Paris, France. p.30

> "We've got the sort of early advantage because we're able to already associate addresses and wallets and bad actors that were already operating on the blockchain at that time, with potential illicit activities. And for example, with being that kind of information from 2018, or from 2020, they don't have that historical clustering or labeling of wallet to, for example, if you'll use our tool and you put in a wallet address, or you'll put in a specific transaction address, the data that pings goes back earlier, in terms of potential illicit activities that wallet might have been associated with. If you use a tool that's only been collecting illicit activity and kind of clustering them since 2018, or 2021, or 2020, you're missing out. Because it doesn't have that duration, that history of the blockchain to check against" (B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.)

The primary limitation of clustering heuristics is the lack of quality assessment, either false negatives or false positives due to the lack of large-scale datasets. As there is currently no process or mechanism to reverse a transaction processed and completed throughout the system,[566] LEA/Intelligence is left with confirming identity through verification checks and triangulation associated with transactions from multiple entities, "*now where you have one player involved or two players involved, you now have eight, right…All that stuff just creates additional struggles for law enforcement to keep on that trail. And then when these blockchain analytic companies are still in the infancy of building out capabilities to trace multiple coins and trace across smart contracts and trace NFT's, there's not a lot of data that goes along with those."*[567]

Peering into peer-to-peer

Peer-to-peer was designed to bypass the regulatory reach of the traditional financial sector.[568] Successfully, illicit peer-to-peer exchanges have positioned themselves as the money launderers of the virtual realm. Most P2P exchanges charge a premium for users to remain

[566] Pflaum, I. and Hateley, E. (2014), "A bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation", Georgetown Journal of International Law, Vol. 45 No. 4, p.1169-1215.
[567] C1, Law Enforcement/Intelligence, Director
[568] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Unpublished manuscript.

anonymous.[569] Notably, they also operate as vendors on darknet marketplaces for illicit activities. By way of example, Fentanyl can be purchased on open-source and dark web marketplaces and then subsequently shipment into different countries where demand is high, such as the United States. **Figure 9** demonstrates a visual screenshot of a typical darknet marketplace,[570] Wall Street Market, using Bitcoin and Monero, which was seized and shutdown (prior to the seizure, approximately $11 million of virtual currency was held in escrow by the website administrators), demonstrating the amazon-style narcotics available for purchase online.

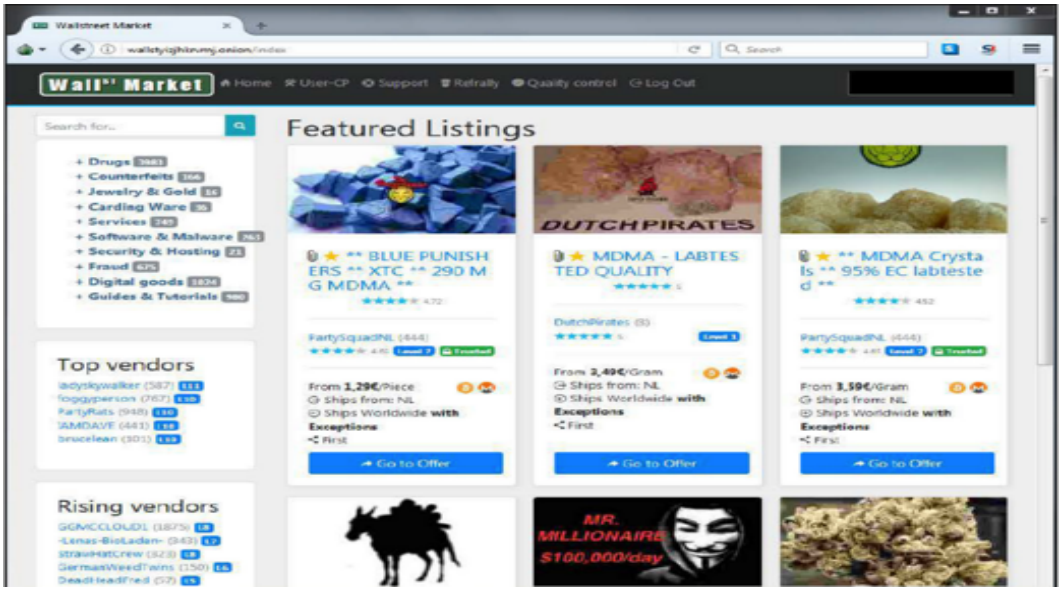


Figure 9: Wall Street Market.

In the context of identification, LEA/Intelligence's investigate techniques will be discussed further and highlighted in Chapter 6, however, the 'anonymity' afforded by such technologies have created, quite literally, new frontiers of dark payments in dark markets. The checks and resources required in the life cycle of an investigation become more cumbersome.[571] In the context of Crypto

[569] By selling VCs above market-value and buying below market value from users who wish to remain anonymous.
[570] Affidavit of Leroy Shelton, United States District Court for the Central District of Colombia (May 1, 2019) Criminal Complaint, Case No. 19MJ1843.
[571] In the context of TOR relay networks, in the United States District Court for the district of Columbia, Case 1:18-cr-00243, Indictment, August 9, 2018, it has been stated in the context of darknet operations, there was "no practical method to trace a user's actual IP address back through those Tor relay computers."

usage, from an intelligence standpoint, "information compiled, analyzed, and/or disseminated in a effort to anticipate, prevent, or monitor criminal activity",[572] must be enhanced.[573] This enhancement assists LEA/Intelligence in "systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature."[574] However, in the context of 'anonymity', an interviewee theorized the main obstacle regarding the wild west nature of peer-to-peer in the following terms:

> "There's a reason that there's not an identity behind the unhosted wallet. And that's not always, you know, because they're dodgy, it's just that's how they're banking. FATF doesn't care about p2p transactions, because they're not trying to regulate users, right? They see peer-to-peer transactions like me handing you cash. There's no one regulating that. There's no entity over that. It's just me handing you cash. And peer-to-peer is the same thing, except obviously a higher risk because I can send $5 million over to Syria in two seconds. No problem. But that's why FATF doesn't regulate peer-to-peer. And then when you have a VASP involved, but you have a VASP involved in half the transaction, and the other half of the transaction is just a person behind the wallet. Then that gets difficult. (A1, Public/Regulator, Deputy Director)

In this vein, P2P transactions have the capability to facilitate and validate transactions, where a user can enter and leave the network at any given time.[575] The 'anonymity' afforded with such technology was identified by FATF to be a "red flag indicator."[576] Pragmatically, while 'anonymity' in and of itself is not conclusive of illicit means or motives, nonetheless, they are still cautioned against by FATF. Similarly, Europol categorized anonymity enhancing technologies as a top threat.[577] The new age of technological advancements is not without risks, and such

[572] Jimeno-Bulnes, Mar, (2017). "The Use of Intelligence Information in Criminal Procedure: A Challenge to Defence Rights in the European and the Spanish Panorama." New Journal of European Criminal Law 2017, vol. 8 issue. 2 p.171-191.
[573] Enhanced in terms of advanced heuristics and attributions, but also, reassortment to traditional investigate methods, i.e., undercover operations, stakeouts, and traditional financial analysis.
[574] Department of Justice (2003), "National Criminal Intelligence Sharing Plan." p. 28.
[575] LAM, Pak Nian and LEE, David K. C. (2015). "Introduction to Bitcoin." Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Research Collection Lee Kong Chian School Of Business. p.5-30.
[576] FATF, (2020). "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing."
[577] De Bolle, C. (2020). Europol, "Internet Organised Crime Threat Assessment 2020."

advancements have effectively been able to by-pass AML checks.[578] In the context of market use and by-passing of AML checks through 'anonymity' enhancing P2P, a respondent in the private/reporting entities category group exemplified the extent of it as follows:

> "There's something called Local Bitcoin, which would enable you to basically meet up with somebody in downtown Toronto, they'd send you a QR code to prove that it's you, you would meet up with them anywhere, and then you'd show them your QR code that would match. Before meeting you, they would have gone to their bank or ATM, withdrawn, the amount of money you're looking for, and give it to you there. That's actually the model that Abra uses. They really changed the game. It's basically an Uber for financial services. So, say, for example, my aunt lives in Mexico City, she wants me to send her the equivalent of 3000 pesos. So, she can use it for whatever. So, I'm here in the United States. So, I tell her to download the Abra app. So, she downloads the Abra app to her smartphone. I activate the Abra app, I convert my bitcoin into Bitcoin that sent through Abra. That's very key, they don't custody any of the assets. Abra acts as a facilitator. So, because they don't custody, any of the assets, they don't have to register as a money service business. So Abra is just a facilitator. These are the options you have in Mexico City, to be able to convert or to be able to receive the money your nephew sent you. So, it'll be about six or seven individuals, and they're in different locations around Mexico City. They're all competing with each other for her business. So that's going to drive the rates that she has to pay for the transaction way down. So, she decides on one and she gets a message saying, you know, John will be at the Starbucks off the central plaza at 1pm. John had gone to the ATM in Mexico City, withdrawn 3000 pesos, so he has it with her. And then he just gives her the 3000 pesos. There's a cross-border transaction. Completely seamless. Completely off the radar of any regulators or law enforcement. Although, I think to show goodwill Abra did agree to put in some controls related to that. Like Hawala, I have to trust you as a Hawala broker, because I'm giving you cash. And you have to trust the network in X country because they're giving cash on your behalf. So, the money hasn't crossed the border, the money is just being sourced from other related sources on the other side of the border. The physical money never transfers. **So, I call the Abra business model Hawala on steroids because you have to have zero trust in anybody you're dealing with**" (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.) [Emphasis added by G. Daoud]

As P2P grow in size, structure and sophistication, so too have the options of illicit usage, and the growing profit-maximization capabilities. As P2P services compete for market dominance,

[578] Y. J. Fanusie, (2020). "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them." The Digital Social Contract: A Lawfare Paper Series, p.1–23.

the capabilities to offer "c*ross-border transaction. Completely seamless. Completely off the radar of any regulators or law enforcement"*[579] will therefore increase the risks of illicit use. Given the nature of innovation of P2P transactions, what we have learned, is that LEA/Intelligence are forced to resort to traditional methods of investigation, in order to combat this phenomenon. The central consideration then becomes, how can LEA/Intelligence effectively investigate this 'higher risk' phenomenon. A respondent noted how this is done:

> "Peer-to-peer, a lot of times, we end up deploying other investigative techniques, like undercover transactions and undercover involvement. Trying to identify if we do have any identifiers. Can we make other law enforcement techniques plausible outside of the digital realm? Because, you're almost running into a lack of information. This is where Crypto takes more of the form of cash. Because if I want to, I can peer-to-peer transact all day long, and there's not much collected, while it's just like cash, if I wanted to go give $100,000 in currency to an individual, there's no record of that it's not like that's recorded somewhere in some third parties, overseeing it, criminal or not. So, we have the ability that if you are peer to peer transacting with somebody else, in large amounts, for whatever reason, depending on the reason behind it, if you're doing it for financial motive and just making money and whatever you're doing your activity, you then have to off-ramp that into Fiat or you're looking to use it for personal expenditures. So, one thing we do, and what we're good at, is the whole financial picture of an individual's wealth. So, a lot of times, we go back to traditional financial analysis, we also go back to some of these undercover components, we go back to sitting on stakeouts and surveillance, physical surveillance to identify individuals and their activities. Because, like I said, it does operate like cash" (C1, Law Enforcement/Intelligence, Director.)

As virtual currency is becoming a more commonly used methodology for transnational organized crime of sophisticated enterprises to transfer proceeds across borders,[580] the opportunities available now for laundering such proceeds increases. The impracticality of regulating peer-to-peer is as difficult as regulating person X giving cash to person Y. The turning to traditional investigative exercises, sting /undercover operations, for LEA/Intelligence stems from the unavailability of data to share with regard to P2P and usage of specialized nodes (TOR

[579] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[580] Drug Enforcement Administration, (20221). "2020 National Drug Threat Assessment."

relays), later discussed in Crypto-funded pedophilia cases in Chapter 6, which complicate investigation techniques. Discerning discrepancies, motives and overall linkage of a crime's life cycle becomes much more cumbersome on LEA/Intelligence, whereby the *modus operandi* of laundering operations change as innovative business models evolve. [581]

Digitizing Identity

Digital identity has been expressed in data to be a new driver in relation to AML/CFT safeguards.[582] Digital identity is defined as "a set of claims made by one digital subject about itself or another digital subject."[583] Allen[584] segments online digital identity and identity management into Centralized identities,[585] Federated identities,[586] User-centric identities[587] and Self-sovereign identities.[588] FATF Recommendation 10 stressed the use of "reliable, independent source

[581] Yaya J Fanusie and Tom Robinson (2018). "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services."

[582] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer: "Digital identity will allow these institutions to focus on individuals, not nations, by-passing risk classifications"
C1, Law Enforcement/Intelligence, Director: "Digital identity is important, I think it needs to be a factor."
B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs: "And I think digital identification platforms and kind of solving for digital identities, the number one thing that will help us move forward from a security and integrity perspective"

[583] Cameron, K., (2005). "The Laws of Identity." Microsoft Corp p.8–11.

[584] Allen, C., (2016). "The Path to Self-Sovereign Identity."

[585] Central authority administers control. For example: IP addresses are administered through Internet Assigned Numbers Authority (IANA), Domain names are administered through The Internet Corporation for Assigned Names and Numbers (ICANN), and/or Certificate authorities (CA). It is important to note that amongst these centralized systems, refer to chapter 3 for discussion on single-point failures which highlight issues with such systems.

[586] Using the same identity for multiple systems and/or organizations through a single sign-on (SSO). I.e., twitter, google, Facebook, and other social media.

[587] "Allows users to control their own digital identities. Users are allowed to select their credentials when responding to an authentication or attribute requester and it gives users more rights and responsibility over their identity information." G -J. Ahn, M. Ko and M. Shehab (2009). "Privacy-Enhanced User-Centric Identity Management," IEEE International Conference on Communications, Dresden, Germany, p.1.

[588] Self-sovereign identity (SSI) is where a person has complete autonomy over their identities by deciding when, if and how their data is disclosed. For further discussion, see Giannopoulou, Alexandra, (2020). "Data Protection Compliance Challenges for Self-Sovereign Identity." J. Prieto et al. (Eds.): Blockchain 2020, AISC 1238, p.1–10.

documents, data or information" for customer identification and verification.[589] The FATF, in its March 2020 Digital Identity report, stated that:

> "An identity assurance framework sets requirements for different 'assurance levels' or 'levels of assurance'. Assurance levels measure the level of confidence in the reliability and independence of a digital ID system and its components." [590]

The Basel Committee's core principles agrees with this, where all banks *must* "have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities."[591] It is estimated that approximately one billion people in developing countries do not have access to an officially recognizable identity.[592] The enlargement of concrete identity programs has been an explicit objective of the UN to "provide legal identity for all, including birth registration" by approximately 2030.[593] While the characteristics of a standard physical document identification[594] are document-based,[595] siloed,[596] and inflexible,[597] such inherent characteristics prove a limitation in the context of the digital realm. In the context of assurance and de-anonymization, respondents expressed a trend regarding market movement of digital identity.

[589] FATF (2012-2022). "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." FATF, Paris, France. p.14.
[590] FATF (2020). "Guidance on Digital Identity." FATF, Paris. p.6
[591] BCBS 29 in Core Principles for Effective Banking Supervision, September 2012.
[592] Vyjayanti Desai. Anna Diofasi, Jing Lu, (2018). "The global identification challenge: Who are the 1 billion people without proof of identity?" World Bank, World Bank Group's Identification for Development (ID4D) initiative, "The Global ID4D Dataset" last updated June 25, 2018.
[593] United Nations (2015). "Transforming our world: the 2030 Agenda for Sustainable Development."
[594] World Economic Forum, (2016). "A Blueprint for Digital Identity: The role of financial institutions in building Digital Identity."
[595] This depends on possession or access, which can enable usage of an entity's credentials by a different user.
[596] Data for identity is stored in places which are not interconnected and cannot be aggregated or connected to other applications.
[597] Information is not easily adapted and is collected upon standardized set of information for a specific purpose.

> "There are global north financial institutions that have risk assessments that prohibit them from doing business with sanctioned countries. Digital identity will allow these institutions to focus on individuals, not nations, by-passing risk classifications. I think data pools are going to change this significantly because it's not as rare to have a global citizen. I've made this argument from the beginning that I personally believe that as great as virtual assets are, the bigger impact will be on blockchain digital identity, which will fundamentally change everything. So, for example, Nigeria is considered a high-risk jurisdiction. There are a significant number of financial institutions that cannot do business there based on their risk assessment. So that entire country is coded red. But what blockchain digital identity will do, it will allow Global North financial institutions to focus on the individual. So, you could be an upstanding citizen in Nigeria. And today, you would never be serviced by a chase bank or a TD Bank, because of the high-risk designation for the entire country. But on the blockchain, digital identity will be so foolproof and so revolutionary. Based on biometric information, and a lot of other data points." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

In the context of financial inclusion,[598] the shift from assessing financial acceptance and/or financial services available from nation-based to user-based can allow "*institutions to focus on individuals, not nations, by-passing risk classifications.*"[599] Where in context of financial access "rural communities are often more affected than urban communities as geographical distance to urban centers tend to reduce financial access."[600] In the new age of internet-based banking, "Mobile banking models leverage off the enormous success of mobile phone uptake in developing countries by using the phone as a key channel to reach new and underserved customers."[601] While positive from a financial inclusion standpoint, it is suggested that from an illicit finance standpoint, "financial exclusion works against effective AML/CFT policies."[602] The effects of individual-

[598] Refer to chapter 3 and 6 for financial inclusion discussions.
[599] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[600] de Koker, L., & Jentzsch, N. (2013). "Financial Inclusion and Financial Integrity: Aligned Incentives?" World Development, 44. p.4
[601] Ibid.
[602] FATF (2011). "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion." FATF, Paris. p.15-16

based focus can, potentially, avoid unnecessary de-risking,[603] where such blacklisting can have the unintended consequence of "*that you don't want to push them under either. It's better to have some type of oversight than none."*[604] The lack of oversight through unnecessary de-risking will, in effect, "inevitably make due diligence work more difficult."[605] As Ramachandran, Collin and Juden's work outlined, where de-risking, that is, de-banking occurs, "MTOs may even disguise the true nature of their operations from banks in order to remain banked, further reducing transparency." Conclusively, "the possibility that industry de-risking might be driving more money into less transparent channels should be of immediate concern."[606] However, there are also risk parameters of digital identity,[607] where it has been suggested that in the digital realm, identity theft, fraud, and synthetic identity come at play:

> "Digital identity is important, I think it needs to be a factor. It's one of those things where you have a huge spectrum of what's collected on individuals. And if you can identify certain components of multiple areas, then that's helpful, versus putting all of your eggs in one basket and saying we're going to create a complete digital identity. That scares me, because digital, anything can be hacked and somehow changed and synthesized where it's synthetic identities are being created. And now we don't know the real person from the false person, or if this person is even a real individual. So, I think it has to be a combination" (C1, Law Enforcement/Intelligence, Director.)

---

[603] "Countries that have such frameworks may clarify to their private sector that such FIs might not be on the designated VASPs lists, or even not under the supervision of the same regulator, to avoid unnecessary de-risking." [Emphasis added by G.Daoud].FATF (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.64.

[604] A1, Public/Regulator, Deputy Director.

[605] Ramachandran, V, Collin, M, and Juden, M. (2018). "De-risking: An Unintended Negative Consequence of AML/CFT Regulation." in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.251

[606] Ibid. p.252

[607] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer :"There were hundreds of attempts every month, either through identity theft, elder abuse, synthetic identity, that would be shut down. And that would force us to file a suspicious activity report… So, I would say identity theft, synthetic identity, elder abuse, I wouldn't put in that same category because that's completely different. But they're there. I can tell you from experience and I, I left [Anonymized], I think in [Anonymized], there were hundreds of attempts every month, at some way to bypass, to compromise a legitimate account based upon these hacks."

Academic research expressed the ability for agencies to chain multiple identity data sources to secure user information, even if such information did not originate from a direct source of an alleged offence.[608] Given that there is no published user directory for the Blockchain system, it is possible to combine blockchain data with off-network information for a partial system of identification.[609] While nations should "facilitate access to digital financial services by developing, or encouraging the development of, customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence",[610] international organizations along with data from respondents expressed the need for Digital ID systems to prove "official identity."[611] Fundamentally, there are four basic identity forms, segmented into static or dynamic forms to be: physical, electronic, legal and/or behavioral.[612] A physical or behavioral identity is interactive and internal, defining who someone is, while a legal identity is external and summarizes who someone is. Electronic has been surfaced with the advent of increased interaction of users with social media, albeit external and not fully descriptive of someone's identity. As careful attention should be put to the unintended consequences of digitizing identities, in line-with data sovereignty,[613] as the digital realm is that much more prone to higher risks:

> "Talks on this kind of technology aren't always the most exciting. So, to get people more engaged, I would fire up TOR and take them on the dark web. And then that

[608] Gross, R. and Acquisti, A. (2005), "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, p.71-80.
[609] Reid, F. and Harrigan, M. (2013), "An analysis of the anonymity in the Bitcoin system." In Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N. and Pentland, A. (Eds), Security and Privacy in Social Networks, Springer, New York, NY.
[610] Global Partnership for Financial Inclusion, (2016). "G20 High-Level Principles for Digital Financial Inclusion." p.1
[611] FATF (2019). "Public consultation on FATF draft guidance on digital identity." p.6. This consultation outlines that "official identity" is defined as the specification of a unique natural person that: (a) is based on characteristics (identifiers or attributes) of the person that establish a person's uniqueness in the population or particular context(s), and (b) is recognized by the state for regulatory and other official purposes.
[612] Litan A (2016). "The global identity dilemma – static biometrics are not the answer." Gartner Blog Network, 16
[613] Weigend A (2017). "Data for the people." Ingram Publisher Services, Pennsylvania.

> would be cool because I go to these sites that sell cocaine and heroin. And that'd be WOW. You're not going to get arrested for going there. And they don't know I'm there because I'm going through the onion router. They have no idea who's doing this. But if you go to those sites, they wheel and deal in the identities that were stolen through these hacks. Experian and Target had a big hack that released a lot of PII, personally identifiable information. So, these names and entities are out there with dates of birth, with social security numbers, National ID numbers, addresses, all of that information is there, and it's a big business because you can go and buy it. I can buy your identity, George and see if there's corresponding information from one of the hacks on the dark web. Purchase that, go to X, if I think you got an account at X. You compile all that information, and basically hijack your accounts. What Estonia is doing would be the biometric factor. The fact that when I got my card, it was fingerprinted, and a DNA swab, that's going to evolve. You're going to have fingerprinting, DNA swabs, and retinal scans. Eventually, it'll be all off of our eyes. So that's becoming more and more complex with time. And that's the one thing that the entities that offer synthetic identity, it would be really difficult to kind of create your own biometric database. Because I mean, that's the one thing short of me cutting off the finger of someone I want to take their identity. So, I think as long as the identity is backed by biometric information, synthetic identity isn't necessarily a factor, or identity theft." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

The 'true' identity of a person thus requires the level of assurance (LOA)[614] dependent on the degree of security assurance and the level of confidence in the context of which information is captured.[615] If higher LOA is present, then there is lower risk that a service provider will be susceptible to compromised/fraudulent identifications in transactions. The World Bank outlined global fully functioning and interoperable identity systems for individuals to have both a unique and secure identity.[616] In the context of KYC and CDD obligations, not all organizations have sufficient mechanisms to comply with KYC and CDD obligations.[617] The minimum requirement for identity confirmation is the user's full legal name, age and residential address. However, often,

[614]World Bank, (2019). "ID4D Practitioners Guide Version 1.0." Report N. 137292
[615] World Bank, (2022). "Catalog of Technical Standards for Digital Identification Systems."
[616] Vyjayanti Desai, Alan Gelb, Julia Clark, Anna Diofasi, (2017). "Ten Principles on Identification for Sustainable Development." World Bank.
[617] Irwin, A., Slay, J., Choo, R. and Liu, L. (2013), "Are the financial transactions conducted inside virtual environments truly anonymous?: experimental research from an Australian perspective." Journal of Money Laundering and Control, Vol. 16 No. 1, p.6-40.

these were inadequately documented and verified, hindering their application.[618] This is complicated in the context of '*peeling chain*,' whereby large sums of a Bitcoin, are segmented into smaller transactions to many change accounts to obfuscate who is truly receiving the majority of the payments.[619] Due to rapid technological innovations, standard developments become challenging. The EU sought to establish such standards relating to justice and home affairs,[620] judicial and police cooperation migration and asylum.[621] They coined[622] a European search portal,[623] a share biometric matching service,[624] a common identity repository[625] and a multiple identity detector.[626] Another example would be Bangladesh's digital IDs of members of a board of directors recorded to validate beneficial ownership.[627] As the area of digital identity is growing, more sophisticated algorithms are becoming readily available, and continue to be tested and deployed.[628] Ultimately, a trusted digital ID must encompass the ability to verify and authenticate with a high LOA across digital canals, must be unique, and must have the individual's informed consent, and must safeguard user privacy while ensuring control over personal data.[629]

[618] Ibid.
[619] Meiklejohn, S. (2013), "A fistful of Bitcoins: characterizing payments among men with no names", IMC.
[620] Regulation (EU) 2019/817 – interoperability of Borders and Visa in EU information systems.
[621] Regulation (EU) 2019/818 amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
[622] Council of European Union, (2019). "Interoperability between EU information systems: Council Presidency and European Parliament reach provisional agreement."
[623] Allows authorities to utilize multiple information systems simultaneously utilizing both biometric and biographical data.
[624] Comparing and searching biometric data such as facial images, fingerprints across multiple systems.
[625] Biometric data and biographical data from third-country nations in EU information systems.
[626] Allows the usage of the previous systems to detect multiple identities linked to the same set of biometric data.
[627]World Bank Group, (2018). "G20 Digital Identity Onboarding."
[628] The analysis of rapidly growing literature in this space was exemplified by L. Ante, C. Fischer and E. Strehle (2022), "A bibliometric review of research on digital identity: Research streams, influential works and future research paths." Journal of Manufacturing Systems, 62: p.523-538.
[629] Olivia White et al, (2019). "Digital identification A key to inclusive growth." McKinsey.

Conclusions

The *ethos* of the FATF standards relating to Crypto is to not hinder the practical benefits of these assets and their underlying systems but to clarify to nations that the regulatory focus is linking illicit transactions with their corresponding entities. In other words, "when banks and fintech firms vie for the same customers with similar services and by taking similar risks, they should be similarly regulated: same risk, same regulation."[630] Notwithstanding this, respondents in the public/regulator and law enforcement/intelligence category groups continuously expressed admiration for these Crypto assets' potential benefits and innovations. And as illicit transactions between the real-virtual worlds continue to pose challenges with visibility, tracking, attribution and collection, blockchain forensics and private/reporting entities have a *key* (quite often literally) part to contribute as gatekeepers in this new era. Literature is developing regarding the legal mechanics of compelled decryption to secure convictions.[631] The debate around this has yet to be settled and it is currently unknown whether jurisprudence in the area of ML/TF will fully be able to set an established body of precedents, which can be referenced internationally by the three category groups. The legal consensus simply does not exist yet. The debate on how to categorize Crypto assets is far from being concluded. It is currently the subject of discussions amongst regulators internationally,[632] with different definitions attributed to how Crypto assets *should* be classified.[633] Sykes and Vanatko identify why this phenomenon is so attractive to criminals,

[630] Carstens, Agustín (2018). "A Institute of International Finance Board of Directors dinner: A level playing field in banking." Bank for International Settlements.
[631] Sarah Ann Scheffler, (2021). "Decrypting Legal Dilemmas." Ph.D. Dissertation. Boston University ; Aloni Cohen and Sunoo Park. Compelled decryption and the Fifth Amendment: Exploring the technical boundaries. Harvard Journal of Law & Technology, 32: p.169–234.
[632] Morton, D. T. (2020). "The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy." Loyola University Chicago International Law Review, Vol.16 Issue.1, p.129-143.
[633] McDonald, D. C. (2021). "Coining New Tax Guidance: How the IRS is Falling Behind in Crypto." University of Miami International and Comparative Law Review, Vol.28 Issue.1, p.151-180.

through the lens of previous prosecutorial and regulatory actions.[634] Irwin offered insights on how this phenomenon is a *perfect* instrument for illicit actors to deploy.[635] Given the uncertainty in this space, it allows illicit actors to effectively by-pass verification checks due to their un-easy to follow multi-chain audit trail.[636] Quite literally, in this space, regulation speed is overwhelmingly mismatched by the rate of innovations of Crypto functions and their diverse uses and techniques.[637] By focusing on selectively defining different *functions* of Crypto, the need for definitive and cohesive regulations will never cease to exist. The focus of regulations, and therefore the standards of the FATF, should be on the pressure points within this space. Namely, the link between on-chain and off-chain and the successful attribution of transactions to their beneficial sender and receiver. This requires uniformity of standards applicable to the interactions between VASPs, nodes, and legacy global north financial institutions. In other words, a systemic standard as opposed to a sectoral approach. This will force both FIs and VASPs to coordinate during relationships, ensuring transactions are '*not blocked, in terms of visibility'*[638] when travelling between the virtual and real worlds and the need for urgent insight in real-time to address what is essentially a more '*radical than cash'*[639] phenomenon.

[634] Skyes, J. B. & Vanatko, N. (2019). "Virtual Currencies and Money Laundering Legal Background, Enforcement Actions, and Legislative Proposals." Congressional Research
[635] Irwin, A. S. M. & Turner, A. B. (2018). "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where." Journal of Money Laundering Control, Vol.21 Issue.3, p.297-313.
[636] Sharma, A. M. (2020). "Cryptocurrency and Financial Risks." Doctoral dissertation, Liberty University.
[637] Nesbitt, E. (2020). "The Scope of Cryptocurrency in the Information Age." In Maniszewska, K. & Piasecka, P. (Eds.), Security and Society in the Information Age, Collegium Civitas Press. Vol. 2, p.179-193.
[638] B9, Private/Reporting Entity, Advisor on Public and Private affairs
[639] B2, Private/Reporting Entity, Chief Compliance Officer

Chapter 6 – Law Enforcement/Intelligence, Public/Regulator and Private/Reporting Entity Considerations

Introduction

The crypto phenomenon has attracted interest from private enterprises, public bodies, and law enforcement agencies due to its rapid expansion in the recent years, with the United States taking a serious and proactive approach at the start of the Russia-Ukraine War.[640] In the Crypto ecosystem, multi-national non-harmonized regulatory frameworks contributed to the current "wild west" regulatory landscape. As such, in approaching this crypto phenomenon, a series of considerations were identified in the interviews. While the previous chapter considered interviewees' insights into crypto themes of security, privacy and safeguards, this chapter will explore the considerations of law enforcement/intelligence, public/regulator and private/reporting entities when approaching this crypto phenomenon. Due to the slow pace of legislative enactment and bureaucratic frameworks in which they operate, technology changes and criminal adaption of such changes are outpacing aggressive strategies of investigations, enforcement and prosecutions. Moreover, existing laws and procedures, including digital evidence, hinder criminal justice authorities' capabilities in investigating, enforcing and prosecuting evolving laundering techniques.[641] Thus, this chapter will explore practical challenges, including capabilities identification, current regulatory framework tensions & gaps present. The first part of the chapter will discuss all three category groups' considerations. The second part of the chapter will discuss

[640] President Biden's Executive Order, (March 9, 2022). White House, Press release.

[641] Mason, S., and B. Schafer. (2010). "The characteristics of digital evidence." In Electronic evidence: Disclosure, discovery and admissibility. 2nd ed., ed. S. Mason. London: Lexis Nexis; Nelson, B., A. Philips, and C. Stuart. (2010). "Guide to computer forensics and investigations." 3rd ed. Boston: Course Technology, Cengage Learning; Casey, E. (2011). "Digital evidence and computer crime: Forensic science, computers and the internet." 2nd ed. London: Academic.

the current risk-based approach applicable to illicit financing in the context of FATF mandates. The third part will examine cultures of compliance, including barriers to cooperation and means to incentivize cooperation. The last part of the chapter will discuss blockchain forensics, who are an essential block in crypto-related AML/CFT.

Law Enforcement/Intelligence Considerations

Comparative analysis regarding national enforcement methodologies is complex whereby "the means by which regulators enforce legal requirements may well differ materially around the world."[642] In the context of illicit transactions and the unintended consequences of an industry described as a 'wild west' regulatory environment, it is essential first to highlight the focus of the type of illicit transactions. In the context of prioritization, LEA/Intelligence priorities were summed up by the following LEA/Intelligence respondents:

> "So, a good example would be two spectrums, not that they're related. But Welcome to Video case, something that's high priority Child Exploitation case where we knew of. We didn't know who or where, but we knew that there were children involved in current situations that needed to be saved from those situations. So, I know the agents personally, that worked on that case, and I'm talking working around the clock through holidays and that's something that in a matter of a few months, you have prosecutions, you have indictments rolling down and you have hitting doors taking down bad guys in a matter of months, over Christmas or just working non-stop. Those are the things that you make a priority. You make it no matter what. You have the other side of the spectrum, where you could have a large darknet market or a large exchange, illicit exchange or something BTC, that's doing tons of volume, tons of data, that then when we collect it, it's going to take a while to go through because there are challenges in the storage of the data, there are challenges in reviewing the data from a legal standpoint, understanding the nuances of what crime we're trying to prove. Now, I mean, when we start working on a case, we've seen an exponential increase in digital evidence collected in the last five to ten years, to really large degrees. I think just in the last couple of years, we've seen a decrease in actual computers, and more in mobile devices, and tablets and things of that. Whereas computers were really a large collection of our information for a long time." (C1, Law Enforcement/Intelligence, Director.)

[642] Howell E. Jackson, (2008). "The Impact of Enforcement: A Reflection." Vol. 156 U. PA. L.REV. PENNUMBRA p.407.

> "Financial intelligence/analysis: support to identify assets and resources of the targets. Target development: undertaking target identification and development, with triaging of broader financial data, to identify related matters and targets (including assets), involved in terrorism and foreign interference activities. – With both a domestic and international focus. Strategic advisory: working collaboratively with public and private sector stakeholders, providing advice to decision-makers at both the national and international level, and conducting project-based work to proactively identify trends and methodologies to inform strategic advice to stakeholders…In CT, urgent/imminent threats to life take priority, for example, if the money is being used to fund a terrorist act. We work closely with financial institutions on education to assist them in identifying suspicious transactions and therefore submitting suspicious reports to [Intelligence Unit Anonymized] which are of greater value to LEA. Increased reliance on online banking and transactions may have been impacted as a result of COVID. More sophisticated use of smaller platforms such as 'buy me a coffee' to transfer funds." (C5, Law Enforcement/Intelligence, Commander - Counter-Terrorism Investigations)

Welcome to video contained over one million downloads of child exploitation videos by users, funded by Bitcoin. This website followed a trend of 'Hurt Core,' a branch of pornography dealing with excessive abuse and depravity of children by evil minds with "a fetish for people who get aroused by the infliction of pain, or even torture, on another person who is not a willing participant."[643] Welcome to video resembled previous sites such as Hurt2theCore, a forum dealing with the sexual abuse of babies. In total, welcome to video had over 250,000 cases of sexual abuse and exploitation of sexually explicit children's material across 38 countries with more than one million Bitcoin addresses, with over 45% of videos containing new images that have not been known to exist for children aged as young as two and four years old.[644] As acting executive associate director Alysa Erichs stated that "Sadly, advances in technology have enabled child predators to hide behind the dark web and cryptocurrency to further their criminal activity."[645]

[643] Daly, Max (2018). "Inside the Repulsive World of 'Hurtcore', the Worst Crimes Imaginable."
[644] Department of Justice, Office of Public Affairs (2019). "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin."
[645] Ibid.

While the market sensationalization of crypto products is undoubtedly attractive to individuals not involved in criminal activity, it is important to recognize the utility of such technology in the dark web. As undercover agents accessed the website, law enforcement/intelligence was able to cluster thousands of unique BTC addresses since the free downloadable Tor network made it possible to have "no practical method to trace a user's actual IP address back through those Tor relay computers."[646]

The priority of LEA/Intelligence should be on crime at all stages of money laundering. Suppose the emphasis is on only the money laundering, as opposed to the predicate offences which preceded it. In that case, the focus is blurred – where such predicate offences are particularly serious, "such as corruption, trafficking in human beings, trafficking of narcotic substances, and organized crime more generally."[647] As a respondent in the LEA/Intelligence category group noted:

> "I think the government's missing the point. The FATF is missing the point. The point is organized crime. If there's no organized crime, and people are making millions and billions of dollars, then there wouldn't be that much money laundering. But to emphasize the last step in the process as your priority. And ignore the first two. There has to be a crime, then there has to be the proceeds of the crime. And then, if they do anything with the proceeds of the crime. It goes into money laundering" (C4, Law Enforcement/Intelligence, Director and Founder of Financial Intelligence Agency of [Country Anonymized]

The priority of LEA/Intelligence is to protect society from criminals. Likewise, it is understood that operatives on the darknet markets are no less different than traditional criminals in any other marketplace, where they are motivated by evading detection and decreasing the risks

[646] United States of America v. Jong Woo Son (August 9, 2018). United States District Court for the District of Columbia, Case 1:18-cr-00243, Indictment. p.2
[647] Hufnagel, S. (2018). "A comparative legal history of international policing." In Comparative Policing from a Legal Perspective. Cheltenham, UK: Edward Elgar Publishing. p.19

of answering for their crimes.[648] As the market value of crypto products have increased, the functions of such products have enabled the 'value' of crypto to provide either a haven or a successful modus operandi for criminal activity, including large-scale financing of and profiting off the sexual abuse of children. In essence, Tim May's prophetic words in **Appendix III** have crystalized: "*An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of Crypto anarchy.*"

The heinous crimes perpetrated on the dark web are now all the more 'profitable' due to societal attributions of 'value' to what is fundamentally a hex version of a string of numbers and letters on a computer screen portrayed as 'money,' but is, fundamentally, a communication system. This portrayal of 'money' is likewise fueled in 'value' by a select few, where there was recent research which noted that a single "whale,"[649] manipulated the market and shot up the value of Bitcoin in 2017 from USD 1,000 (In January) to USD 19,000 (In December).[650] Thus, "unlike global capital markets, the price of the digital coins largely depends on the valuation of their issuers and a small community of investors."[651] Where the period between March 2017 to March 2018 was "associated with 58.8% of Bitcoin's compounded return and 64.5% of the returns on six other large cryptocurrencies (Dash, Ethereum Classic, Ethereum, Litecoin, Monero, and Zcash)."[652]

---

[648] Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E. and Hoorens, S. (2016), "Internet-facilitated drugs trade: an analysis of the size, scope and the role of the Netherlands." RAND Europe, Cambridge; Murray, K. (2016), "The value of understanding organized crime business structures and processes: background paper commissioned by the EMCDDA for the 2016 EU Drug Markets Report." European Monitoring Centre for Drugs and Drug Addiction, Lisbon.
[649] Whales are investors who control more than 1,000 Bitcoins: See: Kharif, O. (2019) Bitcoin whales get ever bigger, threatening increased volatility, Los Angeles Times.
[650] Griffin, John M. and Shams, Amin, (2019). "Is Bitcoin Really Un-Tethered?"
[651] Lu, L. (2018). "Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response." Butterworths Journal Of International Banking And Financial Law, Vol. 33 Issue.3, p.178.
[652] Supra N.650, p.6.

Given the exponential increase of 'value' attributed by society, a given user on welcome to video, where a screenshot is attached in **Appendix VI**, would be "paying 0.03 BTC (approximately $352.59 as of March 5, 2018) for a "VIP" account,"[653] with unlimited download privileges. Welcome to video began to operate on or about June 2015, where from "June 2015 to on or about March 8, 2018, Welcome To Video received at least 420 BTC through at least 7,300 transactions worth over $370,000.00 at the time of the respective transactions."[654] On February 8, 2018, welcome to video indicated on their download page that files downloaded were "more than a million times,"[655] and by March 5, 2018, the server had over "200,000 unique video files,"[656] with the top keywords searched to be: "PTHC,"[657] "PEDO,"[658] "%2yo,"[659] "%4yo,"[660] and "incest." In contrast, as of "March 5, 2018, one BTC was worth approximately $11,573.00."[661]

A Bitcoin in and of itself, irredeemable for any fiat currency, would not offer an incentive for any welcome to video publishers to sell their product. As chapter 3 outlined the principles of fiat currency, that is, serving the three basic functions of money, Ludwig von Mises outlined the regression theorem to emphasize why anyone would accept any fiat currency in the first place. In principle, the demand for any money, is contingent on it having positive value, that is, non-monetary uses, *prior* to its acceptance as a medium of exchange.[662] Mises emphasized that "It is

[653] United States v. Twenty-Four Cryptocurrency Accounts (October 16, 2019). United States District Court for the Central District of Colombia, Civil Action No. 19-cv-3098. p.5
[654] Ibid. p.4
[655] United States v. Twenty-Four Cryptocurrency Accounts (October 16, 2019). United States District Court for the Central District of Colombia, Civil Action No. 19-cv-3098. p.4
[656] Ibid.
[657] "PTHC" is an abbreviation for "preteen hardcore."
[658] "Pedo" is an abbreviation for "pedophile."
[659] "%2yo" is an abbreviation for "2-year-old."
[660] "%4yo" is an abbreviation for "4-year-old."
[661] United States v. Twenty-Four Cryptocurrency Accounts (October 16, 2019). United States District Court for the Central District of Colombia, Civil Action No. 19-cv-3098. p.3
[662] Mises, L. von. [1913] 1934. "The Theory of Money and Credit." London: Jonathan Cape.

therefore illegitimate to adopt the point of view of the community as a whole when dealing with the value of money. All consideration of the value of money must obviously presuppose a state of society in which exchange takes place and must take as its starting point individuals acting as independent economic agents within such a society, that is to say, individuals engaged in valuing things."[663] Conclusively, "all that it is important to know about the objective use-value of money may be summed up in the one statement - it depends on the objective exchange value of money."[664]

To reiterate the 'worth' of one Bitcoin – the first 10,000 Bitcoins were 'exchanged' for two pizzas on May 22, 2010,[665] whereas on March 5, 2018 valuation,[666] the two pizzas would have been exchanged for, or in other words, 'worth,' $115,730,000.00, which is an absurdity. It would be a farcical "objective exchange value of money"[667] for welcome to video to operate in 38 countries, with over a million downloads with 45% of videos containing new images that have not been known to exist in exchange for any fraction of the 'value' of any 2 pizzas, but with societal attribution of 'value' in the timespan of 5-8 years from 2010's first Bitcoin transaction, indeed, has allowed this website and its potential to not only become a possibility but, in fact, a dark reality. While the Crypto characteristics of settling 'transactions' is on a consensus model, there is no consensus on its value by "independent economic agents,"[668] but instead, "a small community of

[663] Ibid. p. 144.
[664] Mises, L. von. [1913] 1934. "The Theory of Money and Credit." London: Jonathan Cape. p.128
[665] Kamau, R. (2022) "What is Bitcoin Pizza Day, and why does the community celebrate on May 9, 22." Forbes Magazine; for the valuation journey of Bitcoin, see 'Diagram 1' in Lu, L. (2018). "Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response." Butterworths Journal Of International Banking And Financial Law, Vol. 33 Issue.3, p.179.
[666] $11,573.00 (March 5, 2018, single bitcoin value) x 10,000 (total bitcoins exchanged for two pizzas May 22, 2010).
[667] Mises, L. von. [1913] 1934. "The Theory of Money and Credit." London: Jonathan Cape. p.128
[668] Ibid.p.144

investors."[669] As such, for the purposes of this thesis, the outline of crypto-related aspects of such criminality poses challenges for law enforcement.

Currently, the reactionary regulations of crypto products is arguably created via enforcement actions,[670] because "cryptocurrencies are not issued by financial institutions and are therefore not subject to the same regulations."[671] Where "through enforcement actions, agency interpretations, no-action letters, and staff guidelines, the SEC has forced cryptoasset developers and crypto-gatekeepers, such as online trading platforms, to comply with the federal securities law."[672] The approach for criminal enforcement varies from nation to nation and is dependent on several factors, which are not exhaustive, such as: selection of cases,[673] policy and programmatic value,[674] bureaucratic procedures to bring actions,[675] and/or resource availability. Notably, the United States "with its very different emphasis on litigation, deterrence, and high penalties, appears to stand apart"[676] as a high-intensity enforcement jurisdiction that "distinguishes the United States from other international market centers."[677] Contrast the U.S. with China, which has a different approach to Crypto related activities,[678] employs active money laundering enforcement

[669] Lu, L. (2018). "Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response." Butterworths Journal Of International Banking And Financial Law, Vol. 33 Issue.3, p.178.
[670] Yuliya Guseva, (2020). "The Leviathan of Securities Law in Cryptoasset Markets: A Cost-Benefit Analysis."
[671] Forgang, George, (2019). "Money Laundering Through Cryptocurrencies." Economic Crime Forensics Capstones. p.7
[672] Yuliya Guseva, (2020). "The Leviathan of Securities Law in Cryptoasset Markets: A Cost-Benefit Analysis." p.5
[673] Commodity Futures Trading Comm'n, Div. Of Enf't., Enforcement Manual (2020); Harvey L. Pitt & Karen L. Shapiro (1990). "Securities Regulation by Enforcement: A Look Ahead at the Next Decade," 7 YALE J. ON REG. Vol.7 Issue.149.
[674] Stephen J. Choi & A.C. Pritchard (2017). "The SEC's Shift to Administrative Proceedings: An Empirical Assessment," Vol. 34 YALE J. ON REG. 1; James J. Park & Howard H. Park (2020). "Regulation by Selective Enforcement: The SEC and Initial Coin Offerings." Vol. 61 WASH. U. J.L. & POL'Y 99.
[675] James J. Park, Rules (2012). "Principles, and the Competition to Enforce the Securities Laws." 100 CALIF. L. REV. 115.
[676] John C. Coffee Jr. (2007). "Law and the Market: The Impact of Enforcement." Vol. 156 U. PA. L. REV. p.281.
[677] Ibid.
[678] See chapter 4 for discussions.

actions in relation to crypto products.[679] Given the cross-border nature of this phenomenon, for LEA/Intelligence, criminal law intervention might involve specialized joint operations with security companies, Big Tech, and blockchain forensics. These joint operations create "*collaborative environments, where a lot of data can go through them, and they collect a lot of it so that we can do what we call deconfliction*."[680] Deconfliction is the "military term for a process aiming at creating mutual awareness among the various missions of each other's activities, with the aim of avoiding duplication of effort."[681] In the context of law enforcement/intelligence "*event deconfliction* is the process of determining when law enforcement personnel are conducting an event in close proximity to one another at the same time. Events include law enforcement actions, such as undercover operations, surveillance, and executing search warrants."[682] A brief outline of deconfliction-based information-sharing systems is thus in order, which we now turn to.

From a global perspective, INTERPOL provides a technical network, 'I-24/7,' which allows LEA access to all of INTERPOL's 19 databases which contain information relating to names and fingerprints; stolen property such as passports and vehicles; and weapons and threats, such as firearms.[683] There is I-Checkit, a border management screening program that gives private actors, like airlines, which will be discussed further, access to crime information. I-Checkit is the "only system that allows direct access by a private sector to crime information possessed by

[679] Wolfie Zhao, (2020). "How a Money Laundering Crackdown in China is Ensnaring Crypto OTC Trading." The block.
[680] C1, Law Enforcement/Intelligence, Director
[681] Guilfoyle, Douglas, (2012). "Somali Pirates as Agents of Change in International Law-Making and Organisation." Cambridge Journal of International and Comparative Law, Volume 1, Issue 3, p.94
[682] Department of Justice, Office of Justice Programs, (2020). "Event deconfliction." National Criminal Intelligence Resource Center.
[683] INTERPOL (2019) Databases, Fact Sheet.

domestic and foreign governments."[684] In the U.S., the primary information-sharing systems used are: Case Explorer, which was developed and is maintained by the High Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISSafe) by the Bureau of Justice Administration (BJA) focused on sharing information amongst local law enforcement for multi-state organized crime and Secure Automated Fast Event Tracking Network (SAFETNet) maintained by HIDTA but does not provide case management functions.[685] Likewise, the El Paso Intelligence Center (EPIC) , a 24-hour watch centre, which provides intelligence analysis on threats which emerge in the western hemisphere, led by the DEA "with twenty-seven partner law enforcement agencies that focus on narcotics, drugs, human trafficking, and weapons trafficking."[686] Similarly, there is the Deconfliction Internet Connectivity Endeavour (DICE), where federal, state, local and tribal law enforcement "are mandated to use DICE to deconflict any case-related information, telephone numbers, email addresses, license plates, and IP addresses."[687] The DEA created the Special Operations Division (SOD) to "identify overlapping investigations into transnational drug trafficking organizations and enhance deconfliction and communications among the agencies."[688] Because the multiple systems posed a "information gaps that can lead to safety issues for investigators,"[689] the Criminal Intelligence Coordinating Council (CICC) determined that "keep officers safe, all law

[684] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.81
[685] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.16-18
[686] Ibid. p.18
[687] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.19
[688] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.20
[689] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.73

enforcement agencies must conduct event deconfliction using one of the three universally recognized deconfliction systems: Case Explorer, SAFETnet, or RISSafe."[690]

The deconfliction efforts pose a challenge as multiple systems are being used; similarly, not all agencies use such systems, where "the use of multiple systems breeds inefficiency,"[691] and "use of multiple deconfliction systems complicated the investigation and increased the dangers to law enforcement."[692] As immediate preservation of electronic records and internet service providers records can be obtained through informal networks of LEA/Intelligence and treaty-based agreements, such as the "24-7 Network", often, they do not include preservation requests for VASPs.[693] Likewise, such records may not be available due to the uneven standards nations have with respect to data privacy, record retention, and different AML/CFT standards, which limit the scope of evidence required and/or available for collection.[694] Deconfliction and deep information sharing are at the heart of strategic coordination, for without it, LEA/Intelligence would continue to face dead ends in investigative operations. In this vein, it is pertinent that "law enforcement and other government agencies are modifying and enhancing their methods of identifying and combating money laundering activity through cryptocurrencies."[695]

[690] Carr, Tom, Kent Shaw, and Jack Killorin, (2017). "Event Deconfliction Avoids Operational Conflicts, Saves Lives, and Solves Cases." Police Chief, p.6
[691] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.22
[692] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.79
[693]Department of Justice (2022). "The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets." p.7
[694] Ibid.
[695] Forgang, George, (2019). "Money Laundering Through Cryptocurrencies." Economic Crime Forensics Capstones. p.26

Public/Regulator Considerations

The idea that *code is law*[696] "seems likely to hasten the obsolescence of legal concepts upon which federal securities regulation has pivoted for the last sixty-odd years, but which were clearly premised on a paper-based information."[697] And there is extensive literature that suggests that these new forms of design systems have effectively confused regulators.[698] Although it is true that "while competition is socially desirable, the understandable concern of regulators is that these new entrants may escape the oversight and accountability that the traditional exchanges have long accepted."[699] However, it would not be correct to say that all regulators are confused by this technology or its application. Indeed, some and many demonstrated strong awareness of practical and pertinent challenges. In the words of one interviewee:

> "The majority of virtual assets will at some point go through a VASP, Peer-to-peer or not; eventually, it will come through a VASP, or a bank at some point, whether they want to withdraw the money in Bitcoin that has to go through a bank or a Bitcoin ATM, which is then considered a VASP, under the first standards. So, the point is, is that you've got those gatekeepers there, that the individual can do what they want. But if they're doing something dodgy, that's going to be picked up by the company that's facilitating it, which is why lawyers and accountants should be regulated, because people use them. That's a different story. So that's why it's the onus is not on the individuals from that point, but criminally it is. FATF is all about tailoring resources to the risk. Tailoring resources to where it's most productive. I mean, it's a government decision. I think China tries to regulate people and ban crypto in general, because they see it as a threat to their financial system. So that's a different agenda than banning crypto because you think that that it can be used for criminal purposes, because so can Hawala. So can remittance services. So can casinos. You don't want to push it underground. Because crypto is one of those things that you can ban all you like, it is going to happen. China can ban it, people can continue to use peer-to-peer. It is

[696] Lessig, L. (2000). "Code is law." Harvard Magazine, 1, 2000.
[697] Coffee, J. C. (1997). "Brave New World?: The Impact(s) of the Internet on Modern Securities Regulation." The Business Lawyer, Vol.52 Issue.4, p.1198.
[698] Karim, S., Lucey, B. M., Naeem, M. A., & Uddin, G. S. (2022). "Examining the interrelatedness of NFTs, Defi tokens and cryptocurrencies." Finance Research Letters, 102696; Ross, D., Cretu, E., & Lemieux, V. (2021). "NFTs: Tulip Mania or Digital Renaissance?" IEEE International Conference on Big Data (Big Data), 2262–2272; Assis, C. V. S. R. de. (2021). de Assis, C. V. S. R., Costa, P. P. S., Filho, H. M. G., de Almeida, G. A. Q., de Almeida, A. L., Guarienti, G. S. S., & da Silva Teixeira, R. F. (2022) Análise E Detecção De Ponzi Schemes Em Contratos Inteligentes Na Rede Ethereum. Tecnologia Da Informação E Comunicação: Pesquisas Em Inovações Tecnológicas - Volume 2, 72–84.
[699] Coffee, J. C. (1997). "Brave New World?: The Impact(s) of the Internet on Modern Securities Regulation." The Business Lawyer, Vol.52 Issue.4, p.1199.

> going to happen. And it facilitates that. So how about we work together? How about let's just regulate the comings, let's provide some consumer protection. Let's provide some certainty for investors in their business operations. Let's make this work instead of banning, but that's the country's decision to make" (A1, Public/Regulator, Deputy Director)

This interviewee's analysis is consistent with themes in chapter 5, namely, the controls/frameworks oversight, where governments are in the business of regulation. In relation to gatekeepers, these have been a focus of recent enforcement actions.[700] The unintended consequences of pushing this crypto phenomenon underground will further fuel the innovative dark payments, which finance criminal activity, along with "leading to an exodus of start-ups and talent to other jurisdictions that offer a "friendlier" regulatory environment."[701] From the standpoint of regulation theory and the rationale for regulation of the financial system as a whole, "once the losses fall on the private sector rather than the taxpayers, the rationale for government regulation— that it is intended to protect the Fed, the FDIC, or taxpayers— wholly disappears."[702] Indeed, the rise of the internet where "technology is faster than the law,"[703] generates emerging "business opportunities, but it also creates tremendous challenges that require some form of state regulatory intervention."[704] This form of regulatory intervention, is what Teubner famously classified as a "regulatory trilemma."[705] Where regulatory interventions face three main risks, "the risk of the regulatory action not working, (i.e., the regulation misses the target or is otherwise ineffective); the risk of breaking the thing it seeks to regulate, (i.e., the regulation removes any incentive to engage in the activity that is being regulated); and the risk of undermining the law,

[700] Yuliya, Guseva, (2021). "The SEC, Digital Assets, and Game Theory." J. CORP. L.
[701] Fenwick, Mark and Vermeulen, Erik P.M. (2020). "The Future of Finance: Why Regulation Matters." Tilburg Law School Research Paper Forthcoming, p.4.
[702] Wallison, Peter J., (2005) "Why Do We Regulate Banks?" Regulation, Vol. 28, No. 4, p.17.
[703] Fenwick, M., Kaal, W.A., and Vermeulen E.P.M. (2017). "Regulation Tomorrow: What Happens When Technology is Faster than the Law." American University Business Law Review 6: 561-94.
[704] Fenwick, Mark and Vermeulen, Erik P.M. (2020). "The Future of Finance: Why Regulation Matters." Tilburg Law School Research Paper Forthcoming,, p.3
[705] Teubner, G. (1986). "Dilemmas of Law in the Welfare State." London: De Gruyter.

(i.e., the regulation undermines the doctrinal integrity of the law and legal system, more generally)."[706]

As expressed, in the context of emerging technologies, '*It's better to have some type of oversight than none.'*[707] It is important to note that when nations pursue an outright ban on this crypto phenomenon, it will further drive regulatory arbitrage and increase black market demand, whereby nefarious actors exploit already legitimate uses of crypto mining.[708] The intricate balance required for oversight of this cross-border crypto phenomenon cannot be said to be implemented with major economies pursuing a black listing approach. Therefore, the risks of either harsh or complete lack of regulatory intervention emphasized in Teubner's regulatory trilemma increase. Whereby professional enablers allow such misuse of this crypto phenomenon, former IRS chief Don Fort expressed, "We cannot continue to operate in the same ways we have in the past, soiling our information from the rest of the world while organized criminals and tax cheats manipulate the system and exploit vulnerabilities for their personal gain. The J5 aims to break down those walls, build upon individual best practices, and become an operational group that is forward-thinking and can pressurize the global criminal community in ways we could not achieve on our own."[709] Pragmatically, there will always be a segment of bad actors who misuse any phenomenon, where a respondent expressed a quasi-realistic/pessimistic certainty of life:

> "Let me draw a picture, the way that I think that those are. So, imagine that you're on a fishing trawler, and it's out there in the ocean, and it wants to catch certain size of fish. So, it uses nets that are designed specifically, so a very, very small fish, that is not really all that interested can pass through the gaps in the net. But any fish or creature over a certain

[706] Fenwick, Mark and Vermeulen, Erik P.M., (2020). "The Future of Finance: Why Regulation Matters." Tilburg Law School Research Paper Forthcoming, p.4 citing from Teubner, G. (1986). "Dilemmas of Law in the Welfare State." London: De Gruyter.
[707] A1, Public/Regulator, Deputy Director
[708]Bauer, Sharon, and Imran Ahmad. (2017). "Cryptocurrency and cybersecurity: A primer." The Lawyers Daily.
[709] Joint Chiefs of Global Tax Enforcement (2018). "Tax enforcement authorities unite to combat international tax crime and money laundering." p.2

> size will be caught in the net, it will be very difficult for some to escape being caught by the net. So, the proceeds of crime is like cromac and the regulations is like that net. Every person who deals with a financial institution has to provide certain information to the financial institution. The vast majority of those people are honest, law-abiding citizens. But some of them are not. The penetrating questions and the degree of detail required under the proceeds of crime acts against a particular customer is designed to deter crooks from using the financial system to move money. That was the original purpose of that thing is to be a deterrent. That's what the risk-based approach is really in a nutshell. The risk is that you in deterring you will inevitably let some crooks in, that might happen. But you will also deter a lot, we hope that will happen. That's the theory of it. So, the quid pro quo for keeping most of them out is that one or two of them might go in. But on the other hand, we've got police forces, and we've got financial intelligence unit. And let's hope we catch the others that way. And, of course, what has happened is that it hasn't, the deterrence factor has been partially successful. But if you look at the amount of money that has just been awarded every year around the world has hardly changed. So somewhere, somehow this money is still being haunted. And if it's not being laundered through federally regulated banks in [Country Anonymized] it is being laundered someplace" (A2, Public/Regulator, – Director of AML).

The established principle of deterrence rests on the assumption of fear imputation into the hearts and minds of a criminal.[710] Conceptually, this approach has been enunciated to be "One of the greatest checks on Crime is not the cruelty of punishments, but their inevitability…. The certainty of a chastisement, even if it be moderate, will always make a greater impression than the fear of a more terrible punishment that is united with hope of impunity."[711] Jeremy Bentham's (1971) *Panopticon* theory is consistent with any government's approach in relation to crime, whereby governments cannot possibly oversee *all* actions, but the mere fact that criminals cannot tell with certainty if/when they are being watched, will, in theory, motivate them to act as if they are being watched.[712] The existence of deterrence effects was analyzed by Blumstein, Cohen and Nagin where the "evidence certainly favors a proposition supporting deterrence more than it favors

[710] Cesare Beccaria, (1764). "On Crimes and Punishments." In David Young Trans., Hacket Publishing Co. (1986). p.46.
[711] Ibid.
[712] Jeremy Bentham (1791). "Panopticon Or the Inspection House." Volume 2. London.

one asserting that deterrence is absent."[713] While Nagin portrayed that "the certainty of punishment is far more consistent than that for the severity of punishment."[714] In the Crypto illicit finance world, the certainty of punishment for illicit actions, when compared to, for example, murder, cannot be said to be as strong since concrete regulatory infrastructures have yet to crystalize, along with adequate policing mechanisms. Where even for banks, with established regulatory infrastructures and policing mechanisms in the form of regulatory oversight, "bankers have been tolerating the laundering of proceeds of crime without obvious harm,"[715] has been illustrated where "even extreme fines had no impact on the banks' financial prowess."[716] In the Crypto illicit world, in line with principles of deterrence, "the certainty of punishment is conceptually and mathematically the product of a series of conditional probabilities: the probability of apprehension given commission of a crime, the probability of prosecution given apprehension, the probability of conviction given prosecution, and the probability of sanction given conviction."[717]

Jeremy Bentham's *Panopticon* theory is at the heart of the crypto revolution, whereby crypto proponents distrust the guard (government) watching over their transactions, and thus galvanized the original Bitcoin whitepaper to attempt to blind the guard, for anyone to operate at any time. This has further spurred non-illicit and illicit innovative crypto functions of mixers, tumblers, privacy-enhanced coins and anonymity-enhancing systems. To be able to disassociate the attempted watchful eyes of the government into their actions. This might be a legitimate aim,

[713] Blumstein, Alfred, Jacqueline Cohen, and Daniel Nagin, eds. (1978). "Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates." Washington, D.C.: National Academy of Sciences. p.7.
[714] Nagin, D. S. (2013). "Deterrence in the Twenty-First Century. Crime and Justice" Vol. 42 Issue.1, p.199.
[715] Verena Zoppei, (2015) "Money Laundering: A New Perspective in Assessing the Effectiveness of the AML Regime." European Review of Organised Crime, p.140.
[716] Erin Lawlor-Forsyth and Michelle Gallant, (2018) "Financial Institutions and Money Laundering: A Threatening Relationship" Vol.19 Issue.2, Journal of Banking Regulation, p.147.
[717] Nagin, D. S. (2013). "Deterrence in the Twenty-First Century." Crime and Justice, Vol.42 Issue.1, p.201.

for privacy and freedom-based individual liberty principles where "people use it legitimately--they just don't want others to know whether they're buying a coffee or a car."[718] The unintended side-effect of this is that criminals can also exploit the privacy & anonymity-enhancing benefits, where "monero provides massive advantages for criminals over bitcoin, so they would use monero."[719] As acting assistant Attorney General Mythili Raman expressed that "criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception…because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services."[720] In comparison with traditional crime, specific crypto-based crime has increased exponentially, where over $3 Billion in crypto-asset equivalent was stolen via hacking in 2021 and until July 31, 2022, that number grew by 58%.[721] Similarly, the damage done by websites like Welcome to Video and Hurt2thecore is irreversible, where the 21st century has not seen such rapid evil capabilities brought forth with the ease of a number of keyboard buttons pressed.[722] Since when an individual uses an Internet Service provider (ISP) "to upload an image located on a server in a foreign state, there is no frontline law enforcement officer monitoring whether the image is, for example, child pornography."[723] This complicates matters for regulators where "to detect and deter crime in the global-digital era, states have no choice but to increasingly rely on private sector actors who are

[718] Kharif, O. (2018). "Bitcoin is being dropped by criminals in favour of privacy coins like monero." para.18.
[719] Ibid.
[720] Press Release, Department of Justice (2013). "Acting Assistant Attorney General Mythili Raman Testifies Before the Senate Committee on Homeland Security and Governmental Affairs."
[721] Jardine, E. (2022) "Mid-year crypto crime update: Illicit activity falls with rest of market, with some notable exceptions." Chainalysis.
[722] "Good news for those who are trying to launder their money is that, in the modern globalized world, money flows across borders with the touch of a button." Mouzakiti, F. (2020). "Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive." New Journal of European Criminal Law, Vol.11 Issue.3. p.352.
[723] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.80.

often crime victims or facilitators, instead of frontline law enforcement officers."[724] This interconnected duty for regulators to provide oversight, and private enterprises' duty to report crime, is all the more important in light of emergent crypto crimes. In other words, the responsibilisation of the private/reporting entities is fundamental, which we now turn to.

Private/Reporting Entities Considerations

Reuter and Truman emphasized that "the fight against money laundering typically involves a dual approach, combining preventive and repressive measures and including both public and private partners."[725] At a basic level, Sungyong illustrated that private enterprises have a "duty to report crime."[726] Through that private/reporting entity information-sharing efforts, it is thus "regarded by many scholars as a crucial factor in deterring crime, sometimes even more than a stronger punishment."[727] As discussed earlier, the "greatest checks on Crime is not the cruelty of punishments, but their inevitability."[728] Thus, private/reporting entity administrative regulatory reporting "accomplishes crime deterrence by raising the probability of punishment."[729] Appropriately, as Garland outlined, concerning the responsibilisation of crime governance to create "active citizens,"[730] in the crypto crime realm, crime prevention extends to "agencies, organizations and individuals which are outside the state and to persuade them to act

[724] Ibid.
[725] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 479.
[726] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1
[727] Ibid. p.88.
[728] Cesare Beccaria, (1764). "On Crimes And Punishments." In David Young Trans., Hacket Publishing Co. (1986). p.46.
[729] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1 p.88.
[730] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.452.

appropriately."[731] This has been demonstrated in the traditional financial banking sector, where compliance functions spending is soaring, which will be discussed further. But for present purposes, in essence, traditional financial banking "have had to expand and transform their practices in order to keep pace with their new workload"[732] in the context of increased compliance duties and obligations. As O'Malley emphasized, in the world of financial crime, as traditional banking and emergent crypto finance contain compliance duties, so too does "the public and private sectors had been added a strong theme of responsibilisation."[733] In effect, the private/reporting entities have been deputized to "fund the policing of criminal behavior."[734]

In the context of crypto crime compliance, a 'black hole and confusion'[735] has taken root in relation to private/reporting entity-specific obligations. Several respondents in this category group expressed this to be a major issue:

> "Personally, I feel like the private sector has been deputized, probably too much. You just read the reports, and you see it. Ultimately, you look at disclosures, you look at law enforcement prosecutions, versus how many suspicious transactions we report, how many investigations we do, and how many resources we have committed to complying with proceeds of crime legislation. I think it's very clear to see that there's a huge asymmetry there. And while I get it to a certain degree, it's probably tilted way too much in the private sector. I'll give you a great example of this, George. Especially in the blockchain industry. It's unique because with a blockchain explorer, you could even go 4,5,6,7,20,30, or 50 hops out from the transaction. Because that transaction history is there on the blockchain, right? There's nothing stopping you from getting the information. Whereas in the traditional space, you see a transaction from Bank of Montreal to HSBC bank, your trail stops as an investigator at Bank of Montreal, you just see the funds go into HSBC, and you stop it, and you report it as a suspicious transaction. But with the blockchain, you could go back, ad infinitum, back to transaction zero, ultimately. So, the question is, how far back do you go

[731] Ibid.
[732] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.455.
[733] O'Malley, P., & Hutchinson, S. (2007). "Reinventing Prevention: Why Did "Crime Prevention" Develop So Late?" The British Journal of Criminology, Vol. 47 Issue.3, p.16.
[734] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.2.
[735] Chambers-Jones C. (2018). "Money Laundering in a Virtual World." In: King C., Walker C., Gurulé J. (eds) The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan.

> in your investigation to report a suspicious transaction on your customer? And where this law enforcement then has to take over if they feel like it's relevant, and they want to do an investigation on a certain subject, right? Because it gets a little more murky and gray in the blockchain industry. Because that transparency of the transaction goes back to zero. So that's kind of where it gets murky. And I don't think we really have any standards. Just a matter of where do you stop? And where does the public sector take over? And again, our standards are very low for reporting. So, I feel like we can stop at a pretty shallow threshold, whereas law enforcement obviously has to prove a conviction" (B2, Private/Reporting Entity, Chief Compliance Officer.)

The informational quality necessary to law enforcement/intelligence by private/reporting entities is a double-edged sword whereby 'suspicious' transactions are reported, without certainty in their illegality, resulting in an overflow of information to LEA/intelligence.[736] In other words, similar to other sectors, there is evidence of defensive reporting to minimize regulatory/LEA enforcement actions,[737] where "financial institutions rarely admit to filing defensively, as it would signal noncompliance and failure."[738] This dilutes the value of suspicious transaction reports from a law enforcement/intelligence perspective.

As for the obligations with regard to this space, the lack of clear oversight required by nations towards the uniqueness of the crypto private sector is unhelpful since '*with the blockchain, you could go back, ad infinitum…the question is, how far back do you go in your investigation to report a suspicious transaction on your customer?'*[739] In the context of a cross-border phenomenon, this dilutes the proactive oversight required by private/reporting entities to effectively implement transaction monitoring and reporting. Different agencies classify this crypto

[736] Stavros Gadinis and Colby Mangels (2016). "Collaborative Gatekeepers." 73 WASH. & LEE L. REV. 797, 859 citing Peter E. Meltzer. (1991). "Keeping Drug Money From Reaching the Wash Cycle: A Guide to the Bank Secrecy Act." 108 BANKING L.J. 230, 231.
[737] Előd Takáts, (2011). "A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement." 27 J. L. ECON. & ORG. 32, 59-60.
[738] Teng Z. (2014). Defensive SAR filing: An unnecessarily heavy burden on the AML field. ACAMS. p.4.
[739] B2, Private/Reporting Entity, Chief Compliance Officer

phenomenon differently, whether as a security, commodity and/or property,[740] as opposed to its regulation across all agencies.[741] The threshold for what is suspicious versus what is unusual is blurred among nations, and there is currently no set standard, aside from varying monetary thresholds, where private/reporting entities should engage in proactive risk assessments and formulations as opposed to the bare minimum:

> "My experience is that, and some of my clients have admitted this. What is the bare minimum to avoid legal sanction? What is the stipulation of the letter of the law? Because that is the guidance for what I do. And that begs a few questions. Firstly, the effectiveness of the regime. It's well written and documented, where we're spending hundreds of millions of dollars on this challenge. And we're not catching a fraction of the bad actors. So that's the first thing. The effectiveness of it. The second thing is that the letter of the law has led to significant processes and procedures and personnel. And the return on that investment is minimal. In fact, it's laughable as to how much we spend." (B3, Private/Reporting Entity, Head of AML & Sanctions)

The *'bare minimum to avoid legal sanction'*[742] on behalf of private/reporting entities calls into question the overall objectives of the AML regime. When spending '*hundreds of millions of dollars… And we're not catching a fraction of the bad actors*'[743] is, arguably, superficial growth akin to what Levi et al. rightly emphasized about the growth of AML without an ability to evaluate its effectiveness.[744] The "significant investment on the part of the organizations concerned"[745] is not capturing the ethos of the fundamental 'duty to report crime.'[746] The ethos of the duty to report crime, at a fundamental level, stems from the fact that "domestic laws and enforcement institutions

[740] Morton, D. T. (2020). "The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy." Loyola University Chicago International Law Review, Vol.16 Issue.1, 129-143.
[741] McDonald, D. C. (2021). "Coining New Tax Guidance: How the IRS is Falling Behind in Crypto." University of Miami International and Comparative Law Review, Vol. 28 Issue.1, 151-180.
[742] B3, Private/Reporting Entity, Head of AML & Sanctions
[743] B3, Private/Reporting Entity, Head of AML & Sanctions
[744] Levi M., Reuter P., Halliday T. (2018). "Can the AML system be evaluated without better data?" Crime, Law and Social Change, Vol. 69, 307–328.
[745] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 480.
[746] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1.

are quite simply inadequate to detect and deter the full range of global-digital crimes."[747] Realizing this, Sungyong addresses the ethos of global-digital era transnational crime in that horizontal cooperation (state-to-state) alone is 'inadequate' and that vertical cooperation is necessary "between state entities and choke point private actors."[748] In the crypto-specific context, criminals "leverage technology to conduct operations at a greater distance . . . which provide both physical and legal protection for offenders . . . while complicating governmental efforts to detect, investigate and disrupt transnational crimes and illicit activities."[749] The rationale of the role private/reporting entities have in the context of crime is indeed essential, but arguably, not practical when superficial compliance is conducted, which does not effectively address risks, as a respondent noted:

> "I think about this a lot in in transaction monitoring. So, you might have a transaction monitoring system that's running, it has a rule set. But if that rule set hasn't been customized to your business model, and to the actual risk, if you're just running something out of the box, then it probably doesn't fit as well as you might want it to, in terms of where your actual risk sits in terms of what you should expect from your customers. And that's something that we see often where someone will say, we just implemented this transaction monitoring system, we have this sea of alerts, none of them make any sense. So, we're just really going through and resolving them on mass." (B1, Private/Reporting Entity, Founder & Chief Compliance Officer.)

This approach by regulated entities where a '*rule hasn't been customized to your business model*'[750] is indeed following the '*the letter of the law,'*[751] but is not addressing the *'actual risk.'*[752] The overall aim of AML regulations is *"*to elicit a high level of outcome in terms of AML

[747] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.78
[748] Ibid.
[749] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.94 citing from Joseph Schafer, (2018). "International Police Cooperation, in Criminology."
[750] B1, Private/Reporting Entity, Founder & Chief Compliance Officer
[751] B3, Private/Reporting Entity, Head of AML & Sanctions
[752] B1, Private/Reporting Entity, Founder & Chief Compliance Officer

effectiveness from self interested FIs."[753] The operative phrase is 'outcome,' that is, does the compliance framework indeed achieve the intended objective of "maximizing the number of *true* suspicious transactions."[754] In essence, the "outcome in combating money laundering is measured through the number and value of true suspicious transactions (TSTs), i.e. financial transactions which are actually useful to identify money laundering operations."[755]

The FATF is clear on its approach regarding the basic minimum requirements in risk-based approaches for crypto compliance programs. As different entities "within a sector may pose a higher or lower risk depending on a variety of factors,"[756] Recommendations 10-21 apply to VASPs in the same manner as they apply to Financial Institutions.[757] FATF nonetheless imposes two specific qualifications; the first is USD/EUR 1,000 threshold for occasional transactions and the Travel rule applied in a "modified form".[758] Above the threshold, market participants in this space must conduct customer due diligence (CDD) (Rec. 10), the travel rule (Rec. 16), and the implementation of recommendations despite secrecy laws (Rec. 9).[759] Furthermore, "Recommendations 9, 22, and 23 also have indirect applicability in this space."[760] Where secrecy

[753] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.4
[754] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.5
[755] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.3
[756] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.15
[757] Ibid.
[758] It also makes it clears that Recs 10-21 apply to both VAs and VA financial activities.
[759] Although Rec. 9 does not explicitly mention VASPs – the FATF has stressed that this recommendation "is intended to ensure that financial institution secrecy laws do not inhibit the implementation of the FATF Recommendations. As with FIs, countries should similarly ensure that secrecy laws do not inhibit the implementation of the FATF Recommendations to VASPs." FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.48
[760] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.48

laws (Rec.9), designated non-financial businesses and professions (DNFBPs) customer due diligence (Rec.22) and other measures in the form of gatekeeper participations (Rec.23) are paramount in the holistic lifecycle of financial crime. A central aspect of AML for private/reporting entities is applying a risk-based approach (RBA), as evidenced by the FATF focus on supervisors to be "proactive in raising material issues and concerns with other Supervisors."[761] This has supported a culture of compliance environment among private/reporting entities to do the bare minimum in addressing risks, ticking the box, and proceeding with *business as usual*. As private/reporting entities are in the profit-based arena as opposed to public safety or public policy, resources and business considerations play an important factor in determining and tailoring compliance infrastructures. However, currently, it is suggested that a risk-based approach may not be the best avenue to frame compliance frameworks, but rather, an intelligence-led based approach. This is evidenced by the high-costs and low returns of AML regimes whereby in 2020, spending on AML compliance reached USD$213 billion and USD274 billion in 2022 globally,[762] while total estimated laundered funds are USD$2 trillion, almost nine times as much.[763] The returns on these compliance infrastructures are indeed not only 'laughable',[764] but more so dangerous.

Risk-based Approach to Intelligence-based Approach.

According to the RBA, the reporting criteria ought to be adjusted along standards of evidence (decisional-bars) based on the actual risk of money laundering.[765] The risk-based

[761] Ibid., p.105
[762] LexisNexis Risk Solutions (2022). "True cost financial crime compliance." LexisNexis.
[763] Money Laundering Overview (no date) United Nations: Office on Drugs and Crime.
[764] B3, Private/Reporting Entity, Head of AML & Sanctions
[765] Axelrod, R. M. (2017). "Criminality and suspicious activity reports." Journal of Financial Crime, Vol. Issue.3, 461–471; Lowe, R. J. (2017). "Anti-money laundering – the need for intelligence." Journal of Financial Crime, Vol. 4 Issue. 3, 472–479.

approach was originally introduced to overcome over-reporting to an FIU without type-II errors (false negatives)[766] increasing. While the rationale might appear to be sound, in the ML/TF context, the RBA is still subject to debate. [767] In terms of practicality, all financial crime cannot be stopped all the time. However, there is an emerging school of thought which shifts the focus from a risk-based approach to an intelligence-based approach ("IBA") to increase the effectiveness of compliance infrastructures.[768] In essence, this approach "is based on "intelligent reporting" (as opposed to automatic reporting, which is based on specific objective criteria."[769]

IBA encompasses sharing practicable and actionable data, with the cooperation of LEA/Intelligence. This would not only allow regulators to conduct oversight of what is missing but, equally, give credit to what has been found. This is contrary to the current supervisory approach of a zero-sum game whereby the focus of assessments is on what is missing. In essence, Eren has done work on this idea of a zero-sum game where "analysis allows for the front office framing of the "loss" of a client due to offboarding on suspicion of ML as a zero-sum game. AML wins, the bank loses."[770] This is stemmed from the idea that "hegemonic message of compliance as cost center continues."[771]

[766] "A Type II error means that a transaction is flagged as legitimate, but in reality, it is an AML event**"**: Rambharat, Bhojnarine, (2012). "Statistical Intelligence Units." CHANCE, Vol. 26 Issue.1, 16-21.
[767] Verhage, A. 2014. "Compliance Officers and the Uneven Playing Field in AML." The European Financial Review.
[768] Moving From Risk-Based AML to Intelligence-Led AML (2022) YouTube. Global Compliance Institute. "So, it's interesting that the FATF talks about a risk-based approach, I would like to talk more about an intelligence-led approach, because that's getting more specific into what information you're sharing. And that's not necessarily about sharing topologies. That's useful. But there's a limit on the usefulness, but it's about sharing practical, actionable data"
[769] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 480
[770] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime, p.10
[771] Ibid.

Similarly, IBA would allow obliged entities to have an *active* role in identifying suspicious transactions.[772] Where the *active* role encompasses "their micro-level, firm specific analyses of risk with an analysis of risks arising across the financial system as a whole."[773] FATF's focus on the RBA is relatively narrow where it is "central to the effective implementation of the revised Financial Action Task Force (FATF)…including the risks relating to new technologies, should inform the risk assessment process of countries and obliged entities and, as per the RBA, should guide the allocation of resources as appropriate to mitigate these risks."[774] This narrow focus, in the context of business considerations, creates the 'cost center' and a 'non-revenue-generating function' which is "firmly entrenched framing of the AML role."[775] What is missing is that by focusing on a RBA, by extension, private/reporting entities are also missing other components, such as the overall effectiveness and responsiveness of an AML program, as opposed to just the 'bare minimum'[776] requirements. This will inevitably force regulators to go in with heavy-handed enforcement. The IBA, like the RBA, is central to KYC and CDD data gathered, gleaned, and compliance infrastructures improved continuously. Where the frameworks are constantly reassessed to improve internal controls, as a respondent noted:

> "Unusual doesn't mean suspicious. Unusual means, there may be something here, or there may not be anything here. But it's a trigger for you to do some investigation. If you've got a client at zero risk for money laundering, and then you see unusual activity, your systems should flag that up, and have a way of investigating it. And either eliminating it, because it's not suspicious at all, or it requires further investigation. So, at some point, you got to ask yourself, we've got to get all these red flags. What are we doing? There was no "what are we doing?" So, somebody put in a system to red flag these on your transactions. And

[772] Black, J., & Baldwin, R. (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, 181–213; Dalla Pellegrina, L., & Masciandaro, D. (2009). "The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Review of Law and Economics, Vol. 5 Issue. 2, 931–952.
[773] Black, J., & Baldwin, R. (2010). "Really responsive risk-based regulation. Law and Policy." p.12
[774] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris,
[775] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime, p.10
[776] B3, Private/Reporting Entity, Head of AML & Sanctions

> all we saw in the records was a set of initials and "not suspicious," but no rationale for why it wasn't suspicious. And no collation of these reasons into a set of analyses of the underlying reasons why something was unusual, but not suspicious. And that's one of the areas where they seriously underestimated the amount of work that would be needed to erect a system of monitoring transactions. It's a lot of work. It involves both computer and manual systems and involves judgments, it involves knowledge of financial transactions that are connected to various types of predicate offences. So that you can link a transaction to a possible predicate offence. Now, the authorities have said all along, you don't need to understand whether that transaction was linked to the predicate offence of theft, murder, or kidnapping. You don't need to know the specific predicate offence that it might be connected to, what you need to understand is that it fits all marks of transactions which are likely going to be connected to a predicate offence." (A2, Public/Regulator, – Director of AML).

Suppose the entity submitting the unusual transaction report is unsure of the predicate offence committed in relation to the transaction in question. How can LEA/intelligence use that data to determine the offence in question?[777] Since the point of intelligence sharing is "maximizing the number of *true* suspicious transactions,"[778] to be "actually useful"[779] to identify money laundering operations,[780] where *'unusual doesn't mean suspicious.'*[781] In this sense, conflating unusual with suspicious when there '*no collation of these reasons into a set of analyses of the underlying reasons why something was unusual, but not suspicious'*[782] frustrates the very role of AML and its desired outcomes since "an anti-money laundering investigator is tasked with reviewing the transactions to determine the legitimacy of the activity."[783]

[777] Intelligence is only as good as the data provided – as in the classic saying, garbage in, garbage out.
[778] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.5
[779] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.3
[780] Dalla Pellegrina, Lucia and Masciandaro, Donato, (2008). "The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View." Paolo Baffi Centre Research Paper No. 2008-22, p.3
[781] A2, Public/Regulator, – Director of AML
[782] A2, Public/Regulator, – Director of AML
[783] Forgang, George, (2019). "Money Laundering Through Cryptocurrencies." Economic Crime Forensics Capstones, p.7

Amongst key stakeholders, a concrete intelligence-sharing framework exists in section 314 of the U.S. Patriots Act. This allows banks to communicate with each other in relation to transactions. While most countries are establishing information-sharing infrastructures based on di minimis requirements, or like Canada, such information-sharing does not exist.[784] There is value in those continuous communication gateways to submit intelligence packages as opposed to sporadic anomalies and to be able to share information in a safe and trusted way in real-time. However, these vertical partnerships[785] are challenging to establish formally due to legal and bureaucratic barriers and resulted in "ample evidence of informal relationship building that would expedite information flows and make SAR reporting more useful to intercepting crime,"[786] which "skirted the boundaries of legality, but which would otherwise be caught in bureaucratic processes."[787] This is particularly amplified in cross-border relationships and often boil down to data protection and privacy considerations.

For comparison, in the airline industry, communication and intelligence are shared all the time in the context of KYC and CDD, and rarely, if ever, do customers push back on the objectives of the overall airline policies.[788] The reason is that it is more graphic when planes fall from the sky

[784] "Canada is the only common law country that does not allow public-private tactical-level information sharing to support law enforcement investigations (i.e., outside public/private exchange of information in an STR, from RE to FINTRAC; and outside of a production order, from law enforcement to REs). At the FIU level, FINTRAC is unable to share tactical information related to their STR intelligence back to regulated entities or to request follow up information from regulated entities on the STRs filed." Retrieved from Maxwell, N.J. (2021) Canadian Legislation, Supervision and Operational Processes for Information-Sharing to Detect Money Laundering and Underlying Crime, set in the Context of International Practices. Future of Financial Intelligence Sharing (FFIS)

[785] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1

[786] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime, p.6

[787] Ibid.

[788] This is not to say that customers are always satisfied with airline operations or wait-times in processing luggage and so forth, rather, it is to suggest that customers go through the process and airlines/airports willingly exchange intelligence, for the sake of security.

or explode. Such visual events evoke more of a reaction and sense of absolute protection requirements where customers are willing to go through the due diligence process, most if not all the time to avoid the graphic destruction of an airplane falling while on board. The impact of an airplane crash is highly visible. In contrast, AML is not so easily visible or sensationalized, i.e., the destruction and calamity tied to the intricate transactional life cycle are often invisible to the public eye. Firearms, human trafficking, organs trafficking, wildlife trafficking, pedophilia, extortion, assassinations, kidnapping, forced labor and slavery, and other such crimes are not always readily transparent when they are occurring thousands of kilometers away in the darkness, and sometimes within their own geographical locations, from a given consumer or entity. To put it bluntly, ignorance is bliss.[789] However, AML is a moral obligation, not a basic compliance function based on regulators' threats of fines whereby a box is checked, and entities proceed with *business as usual*, since society should include "good citizens reporting a crime or a moral duty to participate."[790]

Over 30 years ago, in 1989, FATF was established, however criminal activities and money laundering typologies have evolved. Moreover, the explosion of new technologies, including crypto, has allowed plugging in data for potential actionable improvement of controls more effectively, as opposed to similar degrees of scrutiny for one entity with multiple unusual transactions. This focus on individual transactions is quite counter-productive and will lead to type I errors (false positives) with risk-based systems. Rather, the focus, from an intelligence perspective, should be on customer behavioral activity over time. These types of analytics are

[789] In nil Sapiendo Vita Iucundissima Est (Latin translation: As knowing nothing, life is most delightful) Syrus, p. 85–43 BC – Sententiae
[790] Spiller, Keith & L'Hoiry, Xavier. (2019). "Watch Groups, Surveillance, and Doing It for Themselves." Surveillance & Society. Vol.17, p.290

deployed by banks to leverage data to extract valuable information,[791] however, a holistic analysis has yet to be extended for inter-connected relationships which may exist among products and customers.[792] In the context of new frontiers of accessible data, a respondent noted with regards to the financial picture of a given person's profile:

> "If you're living well beyond your means, a lavish lifestyle, but you don't have a job that supplies, a million dollars a year, yet you live that way, there's a discrepancy there. And that can be one piece, one circumstantial evidence that we can use, in addition to all of our other investigative aspects, but to show that the dollars just don't add up. The financial component just doesn't match." (C1, Law Enforcement/Intelligence, Director.)

Actionable Data

Actionable data follows an intelligence-based approach where action and implementation are useful for "tactical and strategic decisions."[793] Actionable data has been portrayed to be commercially useful in the context of data mining technologies and Big Data analytics to condense immense data in order to have actionable insights for market competitiveness.[794] In the context of AML/CFT, in a basic sense, actionable data is information obtained where a Regulator/LEA/Intelligence can digest the information to successfully pursue a particular course of action.

[791] Hassani, H., Huang, X. and Silva, E. (2018). "Digitalisation and Big Data Mining in Banking. Big Data and Cognitive Computing." Vol. 2 Issue.3, p.18; Hassani, H., Huang, X. and Silva, E. (2018). "Banking with blockchain-ed big data." Journal of Management Analytics, Vol.5 Issue.4, p.256–275.
[792] Giriuniene, G. Katin, I. Kazimianec, M. Skyrius, R. Zilinskas, R. (2018). "Guide to Big Data Applications." Switzerland: Springer International Publishing, Ch 17, p 451-487
[793] Royal Canadian Mounted Police, (2015) Criminal Intelligence Program.
[794] Hassani, H., Huang, X. and Silva, E. (2018). "Digitalisation and Big Data Mining in Banking. Big Data and Cognitive Computing." Vol. 2 Issue.3, p.18; ; Hassani, H., Huang, X. and Silva, E. (2018). "Banking with blockchain-ed big data." Journal of Management Analytics, Vol.5 Issue.4, pp.256–275.

Regulatory Technology (RegTech) has been suggested to be able to collect and digest, extensive amounts of data for automated extraction of actionable data.[795] Indeed, the effectiveness and efficiency of RegTech have been suggested to improve internal and external processes for supervised entities and banks.[796] However, actionable data exists in *duality*, as in, it exists for both commercial and intelligence purposes for nations.[797] In the context of Multinational Financial Institutions (MFIs), actionable data collected by, and available to, authorities is minimized when MFIs de-risk payment systems or other means of value transfer in underdeveloped or financially underserved countries.[798] This provides an avenue for "banking services at lower tier banks with less robust compliance procedures."[799] Where, in the context of the overall AML regime objective, driving banking "through less transparent methods become substantially more difficult to track and secure."[800] Conclusively, "financial exclusion is a risk to financial integrity."[801]

As the RBA proports that entities should be re-investing in compliance frameworks, there is no cohesiveness when there is subjectivity in compliance, and as a result "forces banks either to depend on (outdated) stereotyping criteria or to develop their own criteria, with the result that

[795] Mann, P (2017) Regtech: The Emergence of the Next Big Disruptor, available at https://bit.ly/2gFm2XL; Deloitte (2017) Regtech is the new FinTech, available at https://bit.ly/2IetXui
[796] Toronto Center (2017) "FinTech, Regtech and SupTech: What They Mean for Financial Supervision." H
[797] Dr. Michelle Frasher (2016). "Information Statecraft: States, Financial Institutions, Individuals and the Politics of Counter-Terrorism Data" – cited from Frasher, Michelle and Agnew, Brian, (2016). "Multinational Banking and Conflicts among US-EU AML/CFT Compliance & Privacy Law: Operational & Political Views in Context." SWIFT Institute Working Paper No. 2014-008.
[798] De Goede, M. (2012). "Speculative Security: The Politics of Pursuing Terrorist Monies." University of Minnesota.
[799] Ramachandran, V, Collin, M, and Juden, M. (2018). "De-risking: An Unintended Negative Consequence of AML/CFT Regulation.". "De-risking: An Unintended Negative Consequence of AML/CFT Regulation." In Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.251
[800] Ibid.p.252
[801] de Koker, L., & Jentzsch, N. (2013). "Financial Inclusion and Financial Integrity: Aligned Incentives?" World Development, Vol. 44. p.2

banks determine the threshold for Reporting."[802] Thus subjectivity in RBA is based on idiosyncratic analysis where "judgement calls are inherently subjective and often involve considerations of striking a balance, as part of a risk assessment/ risk management approach."[803] As Iafolla's evidence at the Standing Committee on Finance in the Canadian House of Commons outlined that "there are issues related to the quality of intelligence generated, and frankly issues of privacy and fairness, when individuals are reported not for the suspiciousness of their financial transactions but for reasons that are fundamentally subjective."[804] Remarkably, Iafolla's research opined that "the degree of subjectivity associated with suspicion-based models of intervention is not denied within reporting entities."[805] Consequently, the lack of objectivity and consensus relating to 'how much suspicion' is "needed to act accordingly is a shared-concern in the broader field of policing, from street stops to counterterrorism practices."[806] This is further complicated in the crypto crime realm where blockchain '*could go back, ad infinitum…the question is, how far back do you go in your investigation to report a suspicious transaction on your customer?* '[807]

Since private/reporting entities are not themselves intelligence organizations, deputizing them as such created unsteady foundations to meet the expectations of regulators in compliance assessments, where a 2015 survey of AML professionals found that "62% of respondents see 'increased regulatory expectations' as the greatest AML compliance challenge faced by their

[802] Verhage, A. (2017), "Great expectations but little evidence: policing money laundering", International Journal of Sociology and Social Policy, Vol. 37 No. 7/8, p. 483
[803] Zavoli, I. and King, C. (2021). "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis." The Modern Law Review, Vol. 84: p.13 citing from L. Gelemerova, (2008). "On the frontline against money-laundering: the regulatory minefield." Vol. 52 Crime, Law and Social Change, p.47.
[804] Standing Committee on Finance, Canadian House of Commons (2018) no.143, 1st session, 42nd parliament, evidence by Vanessa Iafolla.
[805] Anthony Amicelle, Vanessa Iafolla, (2018). "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing." The British Journal of Criminology, Volume 58, Issue 4, p.852
[806] Ibid.
[807] B2, Private/Reporting Entity, Chief Compliance Officer

organization."[808] This is due to the ever-evolving nature of financial crimes, furthermore with new products/services emerging in every market and jurisdiction. The information sharing required to be useful and actionable is that "the state alone is not, and cannot effectively be, responsible for preventing and controlling crime."[809] This reality requires involvement not only a select department in the individual entity, but all levels of an entity for the information to become useful and actionable.[810] The practice of this, however, is wholly different, as demonstrated by the discussions in the chapter, where bare minimum requirements are sought by reporting entities, unclear subjective risk analytics and an overall view that compliance functions are a zero-sum game.

The penetrating question, then, becomes how can private/reporting entities have a consistent and reliable set of actionable data that is useful to LEA/Intelligence? This question has already been considered in the context of technical and innovative solutions, whereby proofs-of-concept are constantly deployed since such systems "depend to a large extent on the combination settings of surveillance, risk and (ab)normality."[811] It has been suggested that actionable data, through granting of access to multi external stakeholders, after being stripped of confidential or sensitive information, is, or would be, a way for stakeholders to be more "forthcoming with their data, and possibly more amenable to comply with regulatory reporting requirements."[812] This

[808] Ramachandran, V, Collin, M, and Juden, M. (2018). "De-risking: An Unintended Negative Consequence of AML/CFT Regulation." In Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.243
[809] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.453
[810] Paul Hendriks, (1999). "Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing," Knowledge and Process Management Vol. 6, no. 2 p.91.
[811] Anthony Amicelle, Vanessa Iafolla, (2018). "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing." The British Journal of Criminology, Volume 58, Issue 4, p.858
[812] Di Castri, Simone and Grasser, Matt and Kulenkampff, Arend, (2020) "The 'DataStack': A Data and Tech Blueprint for Financial Supervision, Innovation, and the Data Commons." BFA Global. p.16

approach, however, is counter-productive, costly, and never-ending, resulting in a continuous whack-a-mole environment where short-term threats are addressed, as opposed to the very issue of the approach itself. The focus should not only be on instruments (tools) but also on the agency (entities). Thus, my argument is that it is not in fact *only* the multiplicity of compliance tools which are utilized for controls to combat AML/CFT, but rather, the focus should be on the very culture of agencies that guides compliance infrastructures. Therefore, the following discussion will discuss these cultures, and the means to incentivize a culture of cooperation as opposed to compliance.

Cultures of Compliance or Cultures of Cooperation?

In terms of a compliance approach, regulated entities pursue compliance '*where it's passable from a regulatory perspective, but they're not really thinking through it on a deep risk level.*'[813] The combination of a holistic approach to technical compliance along with effectiveness, is important, in that the FATF assesses nations alongside two primary metrics, compliance and effectiveness. That is the means that the FATF monitors nations implementation with the global AML/CFT regime. While nations are autonomous in implementing these soft laws,

> "In terms of laws and regulations, 76% of countries have now satisfactorily implemented the FATF's 40 Recommendations… However, many countries still face substantial challenges in taking effective action commensurate to the risks they face."[814]

[813] B1, Private/Reporting Entity, Founder & Chief Compliance Officer.
[814] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5

Espoused theories of cooperation have very different real-world applications. As there is a sharp distinction between theory and practice, as theoretical knowledge is not the basis for practical knowledge whereby "Intelligent practice is not a step-child of theory… Efficient practice precedes the theory of it."[815] Understandably, in terms of practicality, it has been argued that true applicability is "the knowledge that can come only from practical experience."[816] While this is not a one-size fits all proposition, it is indicative of the underlying rationale, in that, theory is only as good as its ability for application – otherwise, it remains just that, a theory. This is supplemented by proofs-of-concepts of any domain where theories are applied, tested, adjusted and ultimately, validated. Cooperation itself has been repeated by multiple international watchdogs, notably the Egmont group which promotes cooperation and standardization across AML regimes.[817] The cooperation espouses "close ties between public and private bodies ensure successful AML programs and valuable information to authorities that enable better interstate FIU cooperation."[818] This is against the backdrop of Garland's theory of responsibilisation where the practical reality is such that "the state alone is not, and cannot effectively be, responsible for preventing and controlling crime."[819] In the national context, section 314(a) of the U.S. Patriot Act[820] provides, although with multiple barriers, an avenue for LEA and private enterprises to share *lead information.* Section 314(b) allows financial institutions to share AML/CFT information with each

[815] Ryle, Gilbert, (1949/2002). "The Concept of Mind." Chicago: University of Chicago Press. p.16
[816] Scott, James C. (1998). "Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed." New Haven: Yale University Press. p.6.
[817] Another notable examples would be the Organization for Economic Cooperation and Development. (OECD) 1980. Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Broder Flows of Personal Data. [2013]; The US NSA Surveillance Programme, surveillance bodies in various Member States and their impact on EU Citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs.
[818] Frasher, Michelle and Agnew, Brian, (2016). "Multinational Banking and Conflicts among US-EU AML/CFT Compliance & Privacy Law: Operational & Political Views in Context." SWIFT Institute Working Paper No. 2014-008,
[819] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.453
[820] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001

other, through a secure avenue.[821] In practice, however, this option has "fallen short of expectations."[822]

In the context of the cultures for compliance, respondents across all three category groups expressed a sharp distinction between the current cultural approach of compliance and the *ethos* of cooperation, whether between LEA-LEA (where nation-nation cooperation is included), LEA-private or private-private:

> "In terms of effective investigative frameworks, one of the issues that always comes out in mutual evaluation reports is the lack of interagency cooperation. But if they had a good understanding of it, they would have been able to put a framework in to share information with law enforcement authorities. And I illustrate that, because that comes through in a lot of countries, both high-capacity countries like Canada, and Australia, and low-capacity countries in the Pacific or Nepal or Pakistan, they have the same issue." (A3, Public/Regulator, Executive Secretary)

From the standpoint of LEA-LEA, FATF (Rec. 2) deals with national cooperation and coordination, while Rec. 36 – Rec.40 deals with international cooperation through mutual legal assistance and other forms. Given the cross-border nature of sophisticated laundering enterprises, there is a collective Mutual legal assistance principal spectrum. There is a general obligation to assist one another in investigative measures,[823] information requests on bank accounts/transactions,[824] monitoring of transactions,[825] and transfer of persons.[826] Mutual legal assistance as well in principle, does not rest on the procedural requirement for formal requests, but

[821] Ibid.
[822] Frasher, Michelle and Agnew, Brian, (2016). "Multinational Banking and Conflicts among US-EU AML/CFT Compliance & Privacy Law: Operational & Political Views in Context." SWIFT Institute Working Paper No. 2014-008. p.19
[823] Article 16 Warsaw Convention
[824] Article 17 &18 Warsaw Convention
[825] Article 19 Warsaw Convention
[826] Article 18 Palermo Convention & Article 7 Vienna Convention

reciprocal spontaneous information sharing.[827] These principles, or theories, are wholly different in practice. Where in the context of the 2022 migrant smuggling report, FATF noted:

> "The lack of information on the performance of AML/CFT systems also points to the need for enhanced interagency cooperation, especially between LEAs and migration authorities. Without an understanding of the ML and TF cases, and their nature, a sufficient understanding of the strengths and weaknesses in the AML/CFT system cannot be generated, and informed improvements cannot be enacted. The lack of domestic cooperation also suggests a need for strengthened understanding across law enforcement of the importance of conducting proactive parallel financial investigations for all major proceeds-generating offences."[828]

From a private-private/ LEA-private, in terms of the very culture which precedes compliance functions, a respondent noted bluntly:

> "There's a culture of compliance, there isn't a culture of advancing the interests of the country. So, culture is a big problem. I think the way to address the culture is to galvanize the industry with the regulator and law enforcement. I'll come back to the intelligence model, that [Intelligence Unit anonymized] needs to do better than say, our role is to check on you. And whether you're doing what you're supposed to be doing. [Intelligence Unit anonymized] should be, I can help you do a better job. I can share things with you. So, if you're more effective, and if I help you, you can give me more. And then law enforcement is more equipped. So that entire relationship, that culture needs to be addressed. And my conversations with risk officers, specifically are that this is a grudge buy because we're spending too much money. And we don't understand it. There's nothing that comes off it. And the other thing that's wrong with the regime is that sanctions present the bigger risk here. Money laundering is huge. Terrorist financing can be devastating. Sanction is a big challenge. And so that we don't have a regulator with that portfolio is a big challenge. So, all we're doing as [Country Anonymized] is leveraging our banks' footprint in the US and hoping that our banks do a good job." (B3, Private/Reporting Entity, Head of AML & Sanctions)

[827] Article 20 Warsaw Convention
[828] FATF (2022). "ML/TF Risks Arising from Migrant Smuggling." FATF, Paris, France, p.37

From LEA/private standpoint, they need to not only be a watchdog but an equal participant where they say, '*I can help you do a better job. I can share things with you.'*[829] An increase in vertical cooperation outlined by Sungyong would effectively "eschews top down `command and control' regulation and favours instead experimentation and sharing of best practice, the informal alignment of expectations."[830] Unfortunately, using the Financial Stability Board as an example, "there has been no sign of that sort of systematic data collection and sharing."*[831]* From a private/reporting entity standpoint, given this '*culture of compliance'*[832]*,* it is then not surprising that both private and regulator cooperation efforts lacks '*a good understanding of it.'*[833] This lack of understanding stems in part from private enterprises approaching compliance with a 'grudge buy,'[834] where there is a "hegemonic message of compliance as a cost center."[835] This is understandable given that the role of for-profit enterprises is precisely just that, for profit. When there is *'spending too much money. And we don't understand it. There's nothing that comes off it,'*[836] then the compliance cultures are based on principles of *"*an economic drive for reduction."[837] If criminals have profitability considerations "with excellent incentives to experiment, adapt and learn,"[838] horizontal and vertical cooperation should also have incentives to blunt criminal activity.

[829] B3, Private/Reporting Entity, Head of AML & Sanctions
[830] Guilfoyle, Douglas, (2012). "Somali Pirates as Agents of Change in International Law-Making and Organisation." Cambridge Journal of International and Comparative Law, Volume 1, Issue 3, p.100
[831] Ramachandran, V, Collin, M, and Juden, M. (2018). "De-risking: An Unintended Negative Consequence of AML/CFT Regulation." in Colin King, Clive Walker and Jimmy Gurule (eds.), The Palgrave Handbook of Criminal and Terrorism Financing Law (Springer International Publishing, Cham 2018). p.258
[832] B3, Private/Reporting Entity, Head of AML & Sanctions
[833] A3, Public/Regulator, Executive Secretary.
[834] B3, Private/Reporting Entity, Head of AML & Sanctions.
[835] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime, p.10.
[836] B3, Private/Reporting Entity, Head of AML & Sanctions.
[837] Spiller, Keith & L'Hoiry, Xavier (2019). "Watch Groups, Surveillance, and Doing It for Themselves." Surveillance & Society. Vol. 17. p.290.
[838] Guilfoyle, Douglas (2012); Somali Pirates as Agents of Change in International Law-Making and Organisation. Cambridge Journal of International and Comparative Law, Volume 1, Issue 3, p.103.

Thus, incentivizing cooperation is key, which will be discussed further, but for present purposes, a respondent outlined the incentivization:

> "So, to the private sector and ecosystem, why should I comply? Is there efficiencies on their end that will assist or make it better for them? What can we do that might be able to make it easier for us to identify criminals, but not provide too much of a burden to the ecosystem? Or take away what made the crypto space enticing? The enticement to them is privacy and security. Okay, I don't want to take away all that. But how do we identify the criminal components?... I know to avoid us (private/reporting entity) getting in trouble, avoid us (private/reporting entity) getting shut down" (C1, Law Enforcement/Intelligence, Director.)

A unified culture of 'how do we identity the criminal components'[839] as opposed to the 'bare minimum to avoid legal sanction'[840] would certainly transform cultures of mere compliance to proactive cooperation since "individuals with cooperative incentives are significantly more likely to pool unshared information with other team members than the individuals with competitive incentives."[841] Exacerbating matters, resources once present and used for compliance frameworks are no longer adequate to address a new, fast-changing landscape with "new risks, most obviously for the consumers of financial services, but also for the integrity of the financial system as a whole."[842] While this fast-changing landscape offers increased risks, it also provides increased opportunities for "the ease of capturing digital information and the vast instantaneous reach of this information,"[843] in order to create "new and fluid working relations,"[844] to provide new operating

[839] C1, Law Enforcement/Intelligence, Director.
[840] B3, Private/Reporting Entity, Head of AML & Sanctions.
[841] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.108 citing from Claudia Toma & Fabrizio Butera (2009), Hidden Profiles and Concealed Information: Strategic Information Sharing and Use in Group Decision Making, 35 PERS. SOC. PSYCHOL. BULL 793, 803–04.
[842] Fenwick, Mark and Vermeulen, Erik P.M., (2020). "The Future of Finance: Why Regulation Matters." Tilburg Law School Research Paper Forthcoming, p.4.
[843] Spiller, Keith & L'Hoiry, Xavier. (2019). "Watch Groups, Surveillance, and Doing It for Themselves." Surveillance & Society. Vol.17. p.291.
[844] Ibid. p.298.

paradigms "with higher expectations in relation to the quality of financial transactions reports."[845] However, the resource allocation both regulators and regulated entities have deployed with complacency is not capturing the breadth and depth of risks that have emerged in recent years. As one interviewee opined:

> "Underestimating resources is a historical fact both in the federal government and in the private sector. Banks, in particular, have traditionally always underestimated the amount of work they have to do to implement these measures. And the government has traditionally underestimated the amount of investigation that was needed to investigate some of these crimes." (A2, Public/Regulator, – Director of AML).

Barriers to Cooperation

In the context of information/knowledge sharing, "culture has been identified as one of the largest obstacles in various studies on knowledge sharing."[846] Despite that there are no shortage of calls to cooperation amongst international and national supervisors,[847] dating back to 1989 to fundamentally "establish[ing] and maintain[ing] channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information" and "[c]o-operat[ing] with one another in conducting enquiries . . . concerning: (i) The identity, whereabouts and activities of persons suspected of being involved . . . ; (ii) The movement of proceeds or property derived from the commission of such offences."[848]

---

[845] Anthony Amicelle, Vanessa Iafolla, (2018). "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing." The British Journal of Criminology, Volume 58, Issue 4, p.855.

[846] Rahul Bhaskar and Yi Zhang, (2007) "Knowledge Sharing in Law Enforcement: A Case Study," Journal of Information Privacy and Security 3, no. 3: p.55

[847] U.N. Convention Against Transnational Organized Crime, Dec. 13, 2000, 40 I.L.M. 335 (2001); U.N. Convention on Corruption, Dec. 9, 2003, 43 I.L.M. 37 (2004); U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 28 I.L.M. 493 (1989); International Convention on Financing of Terrorism, Dec. 9, 1999, 39 I.L.M. 270 (2000).

19. Directive 2002/58/EC of the European Parliament and of the Council of, otherwise known as the 'e-privacy directive.'

[848] Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 28 I.L.M. 493 (1989) art. 9(1)(b).

However, even where the legal infrastructures do provide an avenue for cooperation, cooperation can be frustrated by the practical legal considerations of cross-border privacy, security and safeguards, where "barriers of sovereignty… hinder the crime detection-to-arrest process."[849] In the crypto crime world, the reduction of such barriers "is particularly essential for the deterrence of global-digital crimes, more so than for transnational-physical crimes."[850] In the private sector settings, reputational risk plays an important factor amongst competitive private enterprises which influences compliance decisions and, in turn, affects services and consumer relationships.[851] This reputational risk blurs the true nature of compliance and subsequent cooperation required to proactively enhance it where "financial institutions rarely admit to filing defensively, as it would signal noncompliance and failure."[852] As in the 9/11 attacks, it was recognized that poor cooperation, in the form of information sharing across LEAs, was a major contributing factor, in that "information sharing and communication networks like the Regional Information Sharing Systems (RISSNET) existed before 9/11/2001, they were deemed ineffective in the events following the terrorist attacks."[853] The Government Accountability Office confirmed this in that "even five years after September 11, 2001; law enforcement agencies at the federal, state, and local levels are not sharing knowledge to protect the country from future terrorist threats."[854]

[849] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.94
[850] Ibid.
[851] Frasher, M. (2015). "Data Privacy and AML Rules on a Transatlantic Collision Course." American Banker.
[852] Teng Z. (2014). "Defensive SAR filing: An unnecessarily heavy burden on the AML field." ACAMS. p.4
[853] Rahul Bhaskar and Yi Zhang, (2007) "Knowledge Sharing in Law Enforcement: A Case Study," Journal of Information Privacy and Security 3, no. 3: p.45.
[854] Ibid.

Besides culture, other research described other barriers that, in a tripartite analysis, contain organizational, individual and technological issues.[855] Equally, the practical barriers of time required to zero in on which party needs which information and lack of trust regarding possible misuse or credit-taking for the information obtained have been studied.[856] In this study, respondents from all three category groups were keen to identify the barriers to the cooperative efforts they seek from each other.

Private/Reporting Entities

In terms of barriers for private/reporting entities, the views expressed by respondents outlined the need for two things: i) a legal infrastructure for cooperation *and* ii) legal accountability that forces cooperation.

> "So, I think the trans-border issue is a key piece in terms of the count. The antidote to that is really information sharing and cooperation between law enforcement and investigations teams. I think another barrier is oftentimes that the legislative framework is very different between countries as they try to cooperate. One follows the British system, and another one is America. There's no shared legal cover, which I think is a big hindrance." (B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.)

The legal infrastructure for cooperation, that is, with an underlying ethos that stakeholders should be more "forthcoming with their data,"[857] is difficult since '*legislative framework is very different between countries as they try to cooperate,'*[858] where even "cooperation under a formal legal agreement can be largely 'informal' in action."[859] When "*one follows the British system, and*

[855] Andreas Riege, (2005) "Three-Dozen Knowledge-Sharing Barriers Managers Must Consider," Journal of Knowledge Management Vol.9, no. 3: p.24.
[856] Ibid.
[857] Di Castri, Simone and Grasser, Matt and Kulenkampff, Arend, (2020). "The 'DataStack': A Data and Tech Blueprint for Financial Supervision, Innovation, and the Data Commons." BFA Global. p.16.
[858] B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.
[859] Hufnagel, S. (2018). "A comparative legal history of international policing". In Comparative Policing from a Legal Perspective. Cheltenham, UK: Edward Elgar Publishing. p.20.

another one is America,' then, in effect, will create unbreakable "barriers of sovereignty."[860] In this vein, these barriers spillover onto the private/reporting sector where "AML professionals have been forming informal exchanges with the police,"[861] since private stakeholders are fundamentally seeking a 'shared legal cover.'[862] Indeed, there needs to be "legal harmonization and the setting of common or supranational norms"[863] in the context of AML/CFT. Harmonization sought to address this dilemma to galvanize countries to move to an 'all crimes approach,'[864] to address this cross-border dilemma.[865] Yet, these barriers still exist, where another respondent opined:

> "There's a lot of territorial pride in these countries, and they don't like these outside organizations coming in and telling them how to do business. They have to work on that. They have to work on their diplomatic nuanced communication to be able to force these entities to comply more. Now there's a lot of cooperation, because I said, you know, they could get put on this list (FATF grey and blacklists), which makes it more difficult, more expensive for them to operate. So, there is that. But these transnational organizations need more teeth because they're going to be the common denominator." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

The context of this interviewee's data of 'there's a lot of cooperation'[866] is the ability of collective nations, through the FATF, to '*put on this list (FATF grey and blacklists).'*[867] Yet, the issue persists in that nations must still utilize '*diplomatic nuanced communication to be able to force these entities to comply more.'*[868] This leads to the question of, in the context of global

[860] Kang, Sungyong, (2018). "In Defense of the Global Regulation of a 'Duty to Report Crime." Washburn Law Journal, Vol. 57, No. 1, p.94.
[861] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.4.
[862] B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.
[863] Ibid., and see generally S Hufnagel S and C McCartney (eds) (2017). "Trust in International Police and Justice Cooperation."
[864] Recommendation 1, FATF (2012).
[865] D Burchardt, (2017). "Intertwinement of Legal Spaces in the Transnational Legal Sphere." Vol. 30 Leiden Journal of International Law, Cambridge. p.305.
[866] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[867] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[868] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer

AML/CFT standards, who is, in fact, forcing compliance. The FATF standards are the globally recognized standards as the '*common denominator,'*[869] but '*these transnational organizations need more teeth.'*[870] A further aspect is diplomatic considerations which are dependent on a plethora of international relations factors which are beyond the scope of this research. There needs to be an appropriate legal infrastructure for private/reporting entities to be able to share information related to ML/TF, confidently, safely and securely. While the threat of 'naming and shaming' used by international watchdogs may provide a negative incentive,[871] simply, a bark with no bite is counterproductive to the objective of the AML/CFT regime. As such, private/reporting entities are fundamentally measured-risk takers, where they allocate resources to profit maximization. It has also been noted that parties may believe that the information that they hold is not a priority.[872] The question then becomes, how can a legal infrastructure provide an avenue for private/reporting entities to pursue their profit-maximization nature in conjunction with the ethos of the AML/CFT regime? This will be answered later in the incentivizing cooperation section.

Public/Regulator

The need for cooperation *required* amongst nations will never cease to exist. Cultural, economic and national priorities often impact national, international and inter and intra-agency cooperation. The commonality, however, is the unification around a common enemy, whether in terms of disease, calamity, war, famine or something else. Unfortunately, it takes a disaster to force nations to the table willing to build bridges and maintain them. As one respondent stated:

[869] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[870] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[871] Later discussed with positive incentives for galvanizing cooperation
[872] Lambert, David. (2018). "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model." Criminal Justice Policy Review. p.30.

> "I hope and I wish you well in that regard in terms of trying to change the thinking. But here's the thing and I think this is becoming a louder conversation piece in the market. It will take, unfortunately, a catastrophic event to change the mindset. So, if there is a terrorist attack in a country, financed by an attorney's trust account, then I think there will be something that gives. You know, the housing crisis in a country is kind of served by that particular issue. There might be something, but I think I, unfortunately, I think it's going to take something quite significant. Like an unfortunate act, you only have to look at the US and the UK and, France and you can see. It took something horrible before people actually started doing things." (B3, Private/Reporting Entity, Head of AML & Sanctions)

In the context of crime, national priorities and goals are mutable, where "national issues gave rise to particular foci of control interest—sometimes, like 'drug abuse', independently in different countries—before any co-ordinated international activity was even contemplated."[873] Indeed, '*It will take, unfortunately, a catastrophic event to change the mindset,'*[874] since as "community fears, and outrage escalate, media attention is peeked, and public officials voice public anger… can stir national and international interest."[875] As the calamity from WWII galvanized the creation of the United Nations to set aside war-fueled appetites and differences to unite and say in the first sentence of their preamble to their charter, "we the peoples of the united nations determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind."[876]

This reactive approach to the 'scourge of war' hammered cooperation amongst nations, at least in theory, to create a comprehensive UN body.[877] However, in practice, a reactionary approach by public/regulator does 'stir' the upgrade in "preventive and protective controls in

[873] Levi, M. (2022). "Combatting Money Laundering: Some Considerations for Security Professionals." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.286
[874] B3, Private/Reporting Entity, Head of AML & Sanctions
[875] Calder, J.D. (2022). "Burglary Research and Conceptualizing the Community Security Function, a Learning Organization." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.198
[876] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI.
[877] This is not to suggest that the UN is a fully functional cooperative body holding hands singing kumbaya but rather, the alternative of not having it leads to potential and possible disastrous worse scenarios.

reaction to real-life or improvised security incidents."[878] Another example would be the galvanization of stakeholders to create a successful peer-to-peer centralized database to share evidence and case information in relation to the distribution of child pornography in separate jurisdictions, with the goal and means both achieved.[879] National AML approaches cannot continue to be reactive. Instead, the industry must evolve to be proactive. National regulators must understand, that, just as preventative medicine is better than reactive medicine, so too, in the AML context, prevention is better than the cure. Even in the healthcare industry, where the primary objective is quite literally *health*, understand that maintaining regular and proactive oversight, where the action is taken before symptoms occur, is better than reactionary procedures where symptoms occur and spiral out of control.[880] In terms of practical application, a number of respondents noted the pressure points in the public/regulator category group:

> "So, the United States is extremely good in international cooperation, but they fail in implementing the standards across the boards in relation to designated businesses, like lawyers and accountants. And there are a lot of reasons for that. The UK is the same. So, there are challenges across the board with every one of our countries in implementing international standards, and then reasons vary depending on the country." (A3, Public/Regulator, Executive Secretary)

As the "*reasons vary depending on the country,"*[881] with respect to implementation, despite that "in terms of laws and regulations, 76% of countries have now satisfactorily implemented the FATF's 40 Recommendations,"[882] the basic fact that actual implementation is still an issue where "many countries still face substantial challenges in taking effective action commensurate to the

[878] Haelterman, H. (2022). "Script Analysis for Security Professionals: Past, Present and Future." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.539
[879] Eileen Larence, (2011). "Combating Child Pornography: Steps Are Needed to Ensure That Tips to Law Enforcement Are Useful and Forensic Examinations Are Cost Effective." GAO-11-334, Washington, DC: Government Accountability Office, p.30.
[880] Waldman SA, Terzic A. (2019). "Health Care Evolves from Reactive to Proactive." Clin Pharmacol Ther. Vol.105 Issue,1, p.10-13.
[881] A3, Public/Regulator, Executive Secretary
[882] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5

risks they face,"[883] is indicative of the teeth international AML/CFT standards have. The FATF, in effect, is a "non-contractual moral agency"[884] that "only goes so far"[885] where "its implementation relies heavily on the moral compass of individual corporate investigators and their employers and compliance is often difficult to enforce."[886] Thus, since the FATF is the '*common denominator,*'[887] it does '*need more teeth*'[888] to force actual implementation "in taking effective action commensurate to the risks,"[889] which will be discussed further in the incentivizing cooperation section. However, for present purposes, in the crypto realm, even the common denominator, lacks a clear obligation, as a respondent noted:

> "Jurisdictions can decide to register entities that offer products or services in their jurisdiction, that's a choice that the jurisdiction will make, but it's not a FATF obligation. The FATF obligation is to only register entities that are incorporated. So that's why there's a lot of cooperation that's required on this because, you know, Japan needs to know whom Singapore has registered, if you registered them, okay, you're registering them, who's registering them? who's supervising them? If they don't require them registered, but they're offering products and services, then I just want to make sure that there's another country at least supervising them, or is no one supervising them, but they're operating in my jurisdiction, but you don't have to register if they're operating in your jurisdiction, you only have to register if they're incorporated. So, it's a messy realm…there are definitely jurisdictions out there that are going further than that." (A1, Public/Regulator, Deputy Director)

The non-uniform application and implementation of FATF standards has created '*a messy realm.*'[890]A de minimis obligation of crypto oversight is simply not enough, where it's *'a choice*

[883] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5
[884] Meerts, C.A. (2022). "Private and Corporate Investigations: Internal Security Governance Within Organisations." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.658
[885] Ibid.
[886] Meerts, C.A. (2022). "Private and Corporate Investigations: Internal Security Governance Within Organisations." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.658
[887] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[888] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[889] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5
[890] A1, Public/Regulator, Deputy Director

that the jurisdiction will make, but it's not a FATF obligation,'[891] since "jurisdictions can also choose to require VASPs to be licensed or registered before conducting business in their jurisdiction or from their jurisdiction."[892] To put it bluntly, since traditional banking is subject to AML/CFT intervention, FATF's emphasis on "countries may choose to extend their AML/CFT regimes to include other digital assets and entities"[893] is imprudent. Where, by implication, a *choice* in regulation amongst nations, in the context of a cross-border high-velocity internet-operative pseudonymous crypto phenomenon, '*regulatory arbitrage, which is, if you don't like the regulatory environment in one country, no problems go to the next country. If you don't like that country, just go to other countries'*[894] becomes not only a possibility but a probability. The emphasis on the concrete structural importance of financial services, including the extension of AML/CFT standards to all operations, cannot be understated, where even in traditional banking, "in the operation of a developed capitalist economy has traditionally justified high levels of state intervention and regulation to ensure that banks and related actors do not undertake excessive risk."[895] The penetrating question then becomes, how can nations engage, fully and proactively, with FATF standards to ensure uniform application? This will be addressed further in the incentivizing cooperation section.

Law Enforcement/Intelligence

It is important to note that the objectives of LEA/Intelligence differ significantly from profit maximization which fuels the private/reporting entity category group, and political

[891] A1, Public/Regulator, Deputy Director
[892] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Paris, p.5
[893] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Paris, p.36
[894] B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs
[895] Fenwick, Mark and Vermeulen, Erik P.M. (2020). "The Future of Finance: Why Regulation Matters." Tilburg Law School Research Paper Forthcoming, p.4

considerations which fuel the public/regulator category group. In a basic sense, LEA/Intelligence is fueled, primarily, by protecting society from bad actors.[896] In this vein, LEA/Intelligence identified the following factors in their collaborative operations:

> "Stakeholder collaboration. The [anonymized] works with industry partners through the [anonymized], a new national security-focused sub-group comprised of financial institutions including the four main banks and [anonymized] in addition to other Commonwealth agencies. We work closely with financial institutions on education to assist them in identifying suspicious transactions and therefore submitting suspicious matter reports to [anonymized] which are of greater value to LEA." (C5, Law Enforcement/Intelligence, Commander – Counter-Terrorism Investigations)

The data suggests that education in the context of production of valuable suspicious reporting is *'of greater value to LEA.'*[897] This is particularly important since, as discussed in the previous section on actionable data, in the context of financial crime, the point of such information is to "detect suspicious transactions and confidentially report them to intelligence and law enforcement authorities."[898] Thus, the role of LEA/Intelligence in protecting society from bad actors does not only involve law enforcement but, by extension, education of stakeholders concerning ways to assist this role. This reliance on the private actors "who are often crime victims or facilitators, instead of frontline law enforcement officers"[899] thus speaks to private/reporting entities' role in what Garland described as 'active citizens.'[900]

> "I very much believe in collaboration between my regulatory partners as well. So international and domestic, and I assume law enforcement would feel the same, right. You need that cooperation and assistance. But then legislation that actually supports you to undertake investigations in a timely manner, would also be another factor." (C3, Law Enforcement/Intelligence, Manager Regulatory Operations.)

---

[896] This is not to say that there isn't power struggles or qualities which resemble political expediency but rather, the nature of LEA/Intelligence itself is to combat crime as opposed to profit-maximization and/or regulation.
[897] C5, Law Enforcement/Intelligence, Commander – Counter-Terrorism Investigations.
[898] de Koker, L., & Jentzsch, N. (2013). "Financial Inclusion and Financial Integrity: Aligned Incentives?" World Development, Vol. 44. p.5.
[899] Ibid.
[900] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.452.

The '*legislation that actually supports you to undertake investigations in a timely manner,'*[901] is a barrier reoccurring, where there are continuous considerations of legal barriers between the interest of LEA/Intelligence, that is, pursuing criminals, and the interest of individual actors, that is, fundamental rights where "legal limits on investigation and prosecution poses a formidable challenge."[902] Since every nation has due powers for LEA/Intelligence, "their power is not without legal and ethical limits."[903] Indeed, while LEA/Intelligence operates within a set of defined powers and capabilities,[904] criminals, by definition, operate without such restrictions and regard for legal and ethical limits.

> "[Anonymized] tends to be the big player, because they're a large agency, one of the largest, they get a lot of funding, so they have a lot of the mechanisms set up for task forces and collaborative environments, where a lot of data can go through them, and they collect a lot of it so that we can do what we call deconfliction. Just Deconflicting entities targets, you know, wallet address, if we have something going on. We want to run it through a program to make sure somebody else is investigating that same entity… And it's basically Deconflicting, you're saying, hey, to every other agency, does anybody have anything on this entity, XYZ Corporation, or this wallet address, and you're flagging it in the system." (C1, Law Enforcement/Intelligence, Director.)

Of the 3 respondent groups, LEA/Intelligence is the most proactive in pursuing collaboration in a manner to advance societal safety and security. As in the new era of the internet, the majority of the time in modern LEA/Intelligence operations is collecting and digesting data which goes beyond local jurisdictions.[905] In the course of LEA/Intelligence operational circles,

---

[901] C3, Law Enforcement/Intelligence, Manager Regulatory Operations.
[902] Dripps, Donald A., (2016). "The Civil Side of Criminal Procedure: Back to the Future?" Ohio State Journal of Criminal Law, Vol. 14, No. 1, San Diego Legal Studies Paper 16-242, p.1.
[903] Robbins, Ira P., (2021). "Sham Subpoenas and Prosecutorial Ethics." American Criminal Law Review, Vol. 58, No. 1, American University, WCL Research Paper 2021-05, p.1.
[904] This is not to suggest that LEA/Intelligence do not step outside of such bounds or violate it, but rather, there is a framework in place, i.e., rules for the playing field, that they must abide by.
[905] Rick Brown, (2018). "Understanding Law Enforcement Information Sharing for Criminal Intelligence Purposes," Trends and Issues in Crime and Criminal Justice, no. 566, p.1.

information sharing is an important component in the lifecycle of any operation.[906] In contrast, hoarding information not only can stop investigatory efforts, but can also provide a shield for sophisticated criminal enterprises.[907] The penetrating question then becomes: How, if at all, can regulatory efforts along with private enterprises facilitate the role of LEA/Intelligence to combat ML/TF by providing valuable and actionable data, or at the very least, remove barriers for them to effectively operate? It is this question that we now turn to.

Discussion – Incentivizing cooperation

This study found that the greatest efforts to cooperate amongst all three category groups are by LEA/Intelligence and blockchain forensic providers, who are well-versed in technical tracing and clustering-based analytics.[908] When expressing this exact sentiment, a respondent noted:

> "I'll tell you, that's a pretty accurate statement, because, we've been working very closely with a lot of them since inception. And I remember, days of meeting with these companies, when there were one or two people on the company, even the large ones Chainalysis, Elliptic. You're meeting with the CEO, the CTOs, and you're talking with a start-up company, and they wanted to start collecting, they're starting to do blockchain analytics. And, now their companies have hundreds of people and they're globally opening up footprints all over the world. And, it's good because we still have that relationship. And we rely on them heavily. And I think it is this type of space that's opened up, it's kind of broken down a lot of silos that we used to have. I mean, it used to be government shows up somewhere and a lot of times, industry or finance, whoever hesitant to work with you, because there's a lot of fallout there might be implicated, I don't want to give up live data, stuff like that. Where now I think everybody just realizes in this space, you're not getting anywhere unless you have a complete collaboration circle with all the parties involved, because everybody owns a little different piece. And that's what's right." *(C1, Law Enforcement/Intelligence, Director)*

[906] Andreas Riege, (2005). "Three-Dozen Knowledge-Sharing Barriers Managers Must Consider." Journal of Knowledge Management 9, no. 3, p. 24.
[907] Ibid.,
[908] This is not to suggest that public/regulator groups and private/reporting entities do not care about blunting illicit flows or do not engage in some proactive efforts, but rather, that is not the very nature of their role in the market for either profit-maximization or multi-national political governance considerations.

I return now to the questions posed in the preceding subsections regarding how to incentivize cooperation by the 3 different categories of respondents.

I. Private/Reporting Entities: How can a legal infrastructure provide an avenue for private/reporting entities to pursue their profit-maximization nature in conjunction with the ethos of the AML/CFT regime?

It is important to note that "that profit maximization does not absolve individuals engaging in unethical behaviour."[909] The FATF objective has been portrayed to "protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction."[910] The objective has been visually illustrated by Dr. Gordon Hook, Executive Secretary at the Asia Pacific Group on Money Laundering (APG), to contain two-fold sub-objectives: i) identify, investigate and prosecute criminals and ii) trace and confiscate criminal assets.[911] As such, it might be suggested that the ethos of the AML regime, in the context of emerging technologies, is "to take a functional approach that can accommodate technological advancements and innovative business models."[912]

In terms of the private/reporting entities category group, there is a school of thought relating to the ethos of coordinative efforts, *co-operative banking,* "where banks performing similar services and functions treat each other as peers and such multilateral relationships coalesce

[909] Clyde, Paul and Sivadasan, Jagadeesh and Karnani, Aneel G. and Manchanda, Puneet and Narayanan, M. P., (2018). "The Social Impact of Profit-Maximizing Firms." p.8
[910] FATF (2012-2023). "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." FATF, Paris, France.
[911] "As bland or common words are easily glossed. The word 'legislation' in this quote could easily be substituted with 'FATF Recommendations" citing from Dr. Gordon Hook (2022). "Beneficial Ownership And Trusts: A Critical Analysis Of A Central FATF Definition And Its Failure To Meet Policy Objectives."
[912] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.22.

into trade associations."[913] The market consideration thus becomes a choice between: 1) whether it is more profitable to engage in the same AML compliance, where the "average annual cost of financial crime compliance per organization has risen by double-digits since the pandemic began in 2020",[914] or 2) is there another mechanism to increase returns on investments in compliance such that the exponential spike of costs is halted and investments reflect proportionate returns. As illustrated, the focus on compliance technologies (tools), as opposed to the culture of the agency (entities), has led to increased costs with minimal returns.

The way forward, it is suggested, can be by way of providing *positive incentives* where "employee incentives at all levels should reward behavior that supports a positive AML culture."[915] This is because "personal attitudes to risk management/compliance matter in risk compliance behavior."[916] This in-turn would provide positive incentives for private/reporting entities to proactively engage in a culture of cooperation, despite the "hegemonic message of compliance as cost center."[917] It is essential for private/reporting entities to negate this 'cost centre' mentality, and instead, clearly embody that AML/CFT compliance is "behaviour that is expected and rewarded."[918] This is a form of responsibilization emphasized by Garland; for an 'active citizen,'[919] which is all the more necessary since the reality is that "regulators are usually over-

[913] Iris H-Y Chiu (2017). "A new era in fintech payment innovations? A perspective from the institutions and regulation of payment systems." Law, Innovation and Technology, Vol.9 Issue. 2, p.6 n.33 citing from Altamura, C.E. (2016). "European Banks and the Rise of International Finance: The post-Bretton Woods era" (1st ed.). Routledge.
[914] LexisNexis Risk Solutions (2022). "True cost financial crime compliance." LexisNexis.
[915] KPMB (2016). "Building a strong Aml Culture - Seven building blocks to help you measure and improve your AML culture."
[916] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.10.
[917] Ibid.
[918] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.2.
[919] Garland, D. (1996). "The Limits Of The Sovereign State: Strategies of Crime Control in Contemporary Society." The British Journal of Criminology, Vol. 36 Issue.4, p.452.

burdened by rules. They cannot enforce every one of these rules in every firm at every point in time."[920]

There was research measuring the "effects of financial incentives and workplace culture on risk compliance,"[921] where it was understood that "non-compliance is extremely costly for financial institutions and for society as a whole. Harm to customers produces reputational damage and necessitates expensive remediation programs."[922] During day-to-day business "staff may find it easy to comply with risk management policies in normal circumstances, but when a business is struggling to meet short-term profit targets, staff may be tempted to let risk management policies slide. It is exactly at these pressure points that staff seek clarification regarding the *true priority* of the organisation; a favourable risk culture may ensure that staff comply with risk policy despite the competing requirement to produce profits."[923] In this research by Sheedy, Elizabeth & Zhang, Le & Tam, and Kenny of 269 finance professionals, it was concluded that *"fixed payment* increases full compliance by 25.1 percentage points, suggesting that the impact of eliminating variable remunerations systems is potentially very important for changing compliance behaviour. *Risk Culture* also significantly increases full compliance by 16.3 percentage points, relative to the case of profit-focused culture."[924] This relative priority is important, since private/reporting entities are profit-maximizing entities, "the behaviour of leaders or respected co-workers are important

[920] Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, p.3
[921] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.1.
[922] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.2.
[923] Ibid.p.3
[924] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.9

contributing factors in organisational culture in the workplace."[925] Indeed, it is not only positive financial incentives which play a role, but also reinforcing a positive 'risk culture,' defined as "the shared perceptions among employees of the relative priority given to risk management, including perceptions of the risk-related practices and behaviours that are expected, valued, and supported."[926]

II. Public/Regulator: How can nations engage, fully and proactively, with FATF standards to ensure uniform application?

From a strict statutory perspective, every nation has laws in place for accountability. For example, in corporate structure accountability, where staff are accountable to managers, managers are accountable to the officers, the officers are accountable to the board of directors, and ultimately, the board is accountable to the shareholders (shareholder primacy). At the fundamental root of these corporate structures is the accountability for everyone in the organization where there are managers managing the managers. While this is not always practicable due to power dynamics, uneven distribution of wealth, and quantitively superior groups stacking a board for votes who rally through legal maneuvering, the principle is still the same, there are direct powers which can be exercisable by someone higher in the corporate ladder to enforce accountability. These powers carry teeth in a myriad of forms.[927] Expanding that analogy to the international AML regime, FATF, is a body without teeth, as in soft laws, not hard laws. This approach allows nations and regulators to not pursue AML cooperation, out of obligation but rather out of politically changing

[925] Ibid.p.3
[926] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.3 citing from Sheedy, E.A. , Griffin, B. , Barbour, J.P. , (2017). "A framework and measure for examining risk climate in financial institutions." J. Bus. Psychol. Vol. 32 Issue.1, p.101–116 .
[927] Monetary, employment-based, and/or legal.

whims,[928] in support of their divergent "protection of their national interest."[929] When FATF uses language of "*choose* to require VASPs to be licensed or registered,"[930] and "implement the level of due diligence commensurate with the *perceived* risk,"[931] nations will inevitably and justifiably pursue national interest primarily, and global standards of a cross-border dilemma secondarily, if at all. As in the classical saying, clean your own house first before meddling with another's.

Returning to the perceptions of risk, these 'risks' are based on the "common risk model that risk equals probability times impact."[932] The calculations are based on, *inter alia*, the current and past behaviour of a regulated firm/individual.[933] Where the risk-based approaches are "using risk analyses to guide all regulatory operations,"[934] is such that fundamentally "risk scoring may provide a very ready basis for detecting high risk actors, but it may offer far less assistance in identifying the modes of intervention that are best attuned to securing compliance."[935] As such, "poor compliance histories and underperforming risk control systems are often reflected in high risk scores."[936] As previously expressed, regulators "cannot enforce every one of these rules in

[928] Every nation's political election process, where an ideologically different political party is elected, by extension, causes a change in policies, priorities and ultimately, resource allocation by the new political party.
[929] T. Omenma and S. D'Amato (2022). "Changing Threats and Challenges in International Relations: Debating (in)Securities and Ways to Manage Them." In: Gill, M. (eds) The Handbook of Security. Palgrave Macmillan, Cham. p.104.
[930] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Paris, p.5.
[931] FATF, (2012). "Specific Specific Risk Factors in Laundering the Proceeds of Corruption Assistance to Reporting Institutions." Paris. p.8.
[932] Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol.32 Issue.2. p.7.
[933] See Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, p.7-12
[934] Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, p.8
[935] Ibid.
[936] Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, p.7

every firm at every point in time."[937] It is then particularly problematic in the context of AML/CFT standards 'set' by the FATF, which cannot be 'enforced.' In contrast, national bodies, as well as international bodies like the United Nations or the International Criminal Court can 'enforce' law, with due powers to arrest, charge, fine, prosecute and imprison, while the FATF, a 'regulator' of global money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, cannot. Since "many countries still face substantial challenges in taking effective action commensurate to the risks they face"[938] in the face of non-penalizing[939] AML/CFT standards, then why should private/reporting entities be compelled to do so when their host nations do not?

The information, meetings, reports, evaluations and typology exercises which come out of the FATF, while indeed enlightening, one must ask, so what? The cost of not obeying the 'law'[940] in any nation is precise if/when an entity or an individual is caught, but what is the 'cost' of not obeying the FATF standards? Does FATF have an 'enforcement' and 'accountability' mechanism? Are there front-line officers like the UN police? Is there a special operations tactical quick reaction force like the UN 'peacekeeping operations,' which currently includes more than 97,000 personnel from over 120 countries?[941] Is there a structure like the ICC Detention Centre located within a Dutch prison complex in Scheveningen?[942] To put it bluntly, no. The FATF is not a law enforcement agency, nor a private/reporting enterprise. Yet, it characterizes itself as an "inter-

[937] Black, Julia and Baldwin, Robert (2010). "Really responsive risk-based regulation." Law and Policy, Vol. 32 Issue.2, p.3
[938] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5
[939] If naming and shaming on grey or blacklist was a 'penalty,' then nations would have taken "effective action commensurate to the risks they face."
[940] Whether legislation, regulation, standards and/or directives of national regulators – in essence, rules set to govern a particular matter.
[941] Military peacekeeping (no date) United Nations.
[942] ICC detention centre - international criminal court (no date). International Criminal Court.

governmental body [that] sets international standards that aim to prevent these illegal activities and the harm they cause to society."[943] If then it is a public/regulatory 'inter-governmental body,' where are its mechanisms that 'enforce' the standards 'set.' If enforcement of its standards, that is, true accountability, to "prevent these illegal activities and the harm they cause to society"[944] is not in its mandate, then the necessary conclusion is that it is a policy-making body without teeth, resulting in nations not "taking effective action commensurate to the risks they face."[945]

The danger to this, which has been crystalized, is the non-uniform *effective* implementation of FATF rules across the board and nations, containing a myriad of considerations for each nation-specific and FATF recommendation-specific implementation. Further, this approach will not effectively counteract ML/TF in this new internet-operative cross-border high-velocity phenomenon. It has been suggested that "because of the decentralized nature of blockchain, and the different regulatory approaches being taken, tracing these fast-growing markets is virtually impossible."[946] The fact that FATF and FATF-style regional bodies are not treaty-based, carrying certain powers with teeth, with respect to money laundering, terrorist financing and proliferation of weapons of mass destruction, is thus problematic to say the least.

To overcome this, international bodies need a clear *negative incentive* to force national and multi-jurisdictional cooperation. Naming and shaming on lists, at its core, is a negative incentive, i.e., a deterrent, a stick approach, to force national compliance with FATF recommendations.

[943] Who we are (no date). FATF.
[944] Who we are (no date). FATF.
[945] FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, p.5.
[946] Arner, Douglas W. and Castellano, Giuliano and Selga, Eriks, (2022). "Financial Data Governance: The Datafication of Finance, the Rise of Open Banking and the End of the Data Centralization Paradigm." University of Hong Kong Faculty of Law Research Paper No. 2022/08, European Banking Institute Working Paper Series 2022 - no. 117, p.56

However, it does not carry legally binding force as a national legal instrument or as, for example, the International Criminal Court with due powers to prosecute, fine, confiscate and imprison.[947] Since FATF is the 'common denominator'[948] in the context of AML/CFT, then it should be able to enforce its mandate. In contrast, a certain jolt of lightning would strike any regulator's backbone (figuratively) if they were summoned before the ICC to answer for their conduct as opposed to a well-funded wine and steak picture-based on-site evaluation by any FATF assessor for a few days. Recognizing this, the very basis of the UN and ICC was established to have teeth. My contention is that the FATF and its regional bodies must follow suit to manage the managers and regulate the regulators. Any and all other efforts without teeth will still lead to the same result, uneven implementation of FATF rules causing a '*messy realm.*'[949] Since the FATF standards do not have teeth, it has thus cast doubt on the international efficiency of international coordination relating to the efficacy of AML/CFT.[950]

A further consideration here is how regulators engage with the private sector. A respondent expressed the active role public/regulators can apply not only on the global stage but in their own backyard to incentivize cooperation between them and a private/reporting entity:

> "But one of the other ones is recognition of participating or assisting law enforcement and the public bodies like [Anonymized Public Body]. [Anonymized] got recognized for helping out with human labor, and [Anonymized] got recognized for trafficking, helping create project protect. I think there's not enough of that. I think a lot of MSBs are doing good things like I mean, I got a letter from [Anonymized Public Body] commending us on our intelligence and what we provide, and I've passed this to a few consultants in the industry, and they've like, I've never seen a letter like this, and they do happen. But I think recognition is one of those incentives too, because we don't do enough of that. And even

[947] The ICC does not enforce its powers against nations per se, but individuals and key stakeholders in nations in line with the principle of complementarity. See The Principle of complementarity in practice (2009), informal expert paper, International Criminal Court.
[948] B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer
[949] A1, Public/Regulator, Deputy Director
[950] Caroline Binham, (2016). "Anti-money Laundering Rules Need to be Toughened Up, Warns FSB." Financial Times.

> when I was talking to [Anonymized], who's the Deputy Director of [Anonymized] intelligence, he was saying we don't do enough to recognize the industry and we want to try and do more of that. And I think that's one of those incentives is being recognized for helping the intelligence community" (B7, Private/Reporting Entity, Executive Director)

As the interviewee noted, "*recognition is one of those incentives too,"*[951] speaks to the fundamental role that not only private enterprises have within their organizations for positive incentives, but likewise from regulators to relay to the private industry "behaviour that is expected and rewarded."[952] Collens's research recognized the effect of these 'morale boosts,'[953] where LEA's news of investigation impacts reinforced "the morale-boosting effect of contributing to a greater cause."[954] The public/regulator entities would do well to engage in more positive recognition and assistance steps to '*do better than say, our role is to check on you'*[955] to say, *'I can help you do a better job. I can share things with you. So, if you're more effective, and if I help you, you can give me more.'*[956]

III. LEA/Intelligence: How, if at all, can regulatory efforts along with private enterprises facilitate the role of LEA/Intelligence to combat ML/TF by providing valuable and actionable data, or at the very least, remove barriers for them to effectively operate?

Fundamentally, FIUs should pursue "new ways for FIUs to work together to have a common output at the end – with actionable outcome".[957] The interconnected relationship between LEA/Intelligence and private/reporting entities in the context of AML/CFT forces heavy reliance

[951] B7, Private/Reporting Entity, Executive Director
[952] Sheedy, Elizabeth & Zhang, Le & Tam, Kenny. (2019). "Incentives and Culture in Risk Compliance." Journal of Banking & Finance. Vol. 107. p.2
[953] Eren, Colleen. (2020). "Cops, Firefighters, and Scapegoats: Anti-Money Laundering in an era of Regulatory Bulimia." Journal of White Collar and Corporate Crime. p.6
[954] Ibid.
[955] B3, Private/Reporting Entity, Head of AML & Sanctions
[956] B3, Private/Reporting Entity, Head of AML & Sanctions
[957] Meeting of the EU FIU Platform (10 June 2016). 10.00 - 17.00. Centre Borschette, Meeting Room AB-0D Rue Froissart 36, 1000 Brussels

on valuable and actionable data required from private/reporting entities. This, however, is complicated if private/reporting entities are engaged in defensive reporting, which increases the volume of questionable data, or a box-ticking culture of compliance, where AML compliance functions are passable from a compliance standpoint, but not an effectiveness standpoint.[958] Given that LEA/Intelligence heavily relies on experts in the field to conduct effective crypto-investigations, clustering and tracing,[959] LEA/Intelligence, as a result, resort to under-cover techniques.[960]

The primary barrier to LEA/Intelligence was said that "*blockchain analytic companies are still in the infancy of building out capabilities to trace multiple coins and trace across smart contracts and trace NFT's, there's not a lot of data that goes along with those."*[961] Similarly, traditional LEA/Intelligence was expressed to be primarily concerned with enforcing legal and jurisdictional barriers on a 'need-to-know' basis[962] as opposed to active information-sharing efforts where "the culture of law enforcement does not encourage knowledge sharing on a daily basis."[963] This causes ' institutional frictions'[964] and prevents proactive "reciprocity of information"[965] sharing efforts. As such, data gathering, sharing and attributions are expressed to be a primary obstacle for LEA/Intelligence. The proactive reciprocity of information is important in the context

[958] B1, Private/Reporting Entity, Founder & Chief Compliance Officer: "passable from a regulatory perspective, but they're not really thinking through it on a deep risk level.'
[959] Multiple blockchain forensic providers. Notably, Elliptic, Chainalysis, TRM Labs, Ciphertrace and others.
[960] C1, LEA/Intelligence, Director
[961] C1, LEA/Intelligence, Director
[962] Rahul Bhaskar and Yi Zhang, (2007) "Knowledge Sharing in Law Enforcement: A Case Study," Journal of Information Privacy and Security Vol.3, no. 3: p.55
[963] Ibid.
[964] David E. Lambert (2018), "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model." Criminal Justice Policy Review, p. 1259.
[965] Nyhus, A. Brian (2020). Captain, New York City Police Department. "Danger Close, The need for a nationwide deconfliction and notification system for all law enforcement agencies." Naval Postgraduate School. p.8

of "proactive meaning of prevention to 'act before the other' in order to prevent potential harmful events from happening."[966] At the core of proactive information sharing, is actionable data, to "incapacitate suspects before they act."[967]

Since actionable data exists in *duality* for commercial and intelligence purposes,[968] in the context of LEA/Intelligence, they are "responsible for staying a step ahead of the terrorists in these investigations, time is critical. Even a brief delay in an investigation may be disastrous."[969] It is suggested that the actionable data, as opposed to the *'bare minimum to avoid legal sanction,'*[970] required from private/reporting entities would considerably alleviate, or at least reduce, this barrier for LEA/Intelligence to conduct effective investigations. The standards set for private/reporting entities to collect at least bench-mark amount of actionable data, beyond de minimis requirements, but also to alleviate practical challenges for regulators, as evident in the following example "*all we saw in the records was a set of initials and "not suspicious," but no rationale for why it wasn't suspicious. And no collation of these reasons into a set of analyses of the underlying reasons why something was unusual, but not suspicious."*[971] This is reaffirmed by the rudimentary RBA on private/reporting entities as opposed to an intelligence-led approach where private/reporting

[966] A. Amicelle, (2013) 'The Eu's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance,' Liberty and Security in Europe, p.7
[967] Ibid., p.2
[968] Dr. Michelle Frasher (2016). "Information Statecraft: States, Financial Institutions, Individuals and the Politics of Counter-Terrorism Data" – cited from Frasher, Michelle and Agnew, Brian, (2016). "Multinational Banking and Conflicts among US-EU AML/CFT Compliance & Privacy Law: Operational & Political Views in Context." SWIFT Institute Working Paper No. 2014-008,
[969] A. Amicelle, (2013). "The Eu's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance." Liberty and Security in Europe, p.7.
[970] B3, Private/Reporting Entity, Head of AML & Sanctions.
[971] A2, Public/Regulator, – Director of AML.

entities are identifying relevant data, justifying it, and proactively sharing it in order to be able to confidently answer "*how do we identify the criminal components?"*[972]

In the context of this internet-operative cross-border high-velocity crypto phenomenon, the necessity for multi-stakeholder engagement is vital for, without it, criminals will continue to use and abuse this crypto phenomenon which indeed does have positive market utility in the financial sphere. The working groups developed,[973] are a good start and the focus should not only be on the training given to private/reporting entities but also on the nuanced differences of specific predicate offences and their correlation to specific transactional behaviour at a deep-analytical level. This two-way information sharing would strengthen the bridge of necessary information exchange between LEA/Intelligence and the private/reporting entities. Should private/reporting entities continue to merely tick the box, with a primary focus on profit maximization through impacts on customer relationships, there will continue to be "numerous difficulties when conducting enquiries, many of which centred around a fear of offending the customer. If bank staff are fearful of asking questions, it is clearly impossible to conduct satisfactory investigations."[974]

Finally, a clear operational leadership at LEA/Intelligence is required to clearly outline that information sharing is key and is just as part of the job as, say, basic ethics procedures or report documentation. If that were to happen, then information-sharing will likely increase.[975] The

[972] C1, LEA/Intelligence, Director.
[973] Some examples include: Europol's Virtual Currency Conference, the Europol Platform for Experts (EPE), Europol Financial Intelligence Public Private Partnership, the Tripartite Working Group on Criminal Finances and Cryptocurrencies.
[974] Vineer, Annalise. (2020). "Perceptions of Barriers to Conducting Effective AML Investigations." Policing: A Journal of Policy and Practice. 15. p.1
[975] Tsui, Eric, (2005). "The Role of IT in KM: Where Are We Now and Where Are We Heading?" Journal of Knowledge Management Vol. 9, no. 1, p.3–6.

fundamental importance of this style of leadership was stressed by one respondent in the following terms:

> "And I think that hits on important thing from a management level. I think managers in general are never good at relying completely on subordinates for their expertise, right? Usually, in a typical structure, you've gotten into the management role, because you have the experience you have expertise that can be drawn on. In this space, you have nothing to draw on, some folks don't have an education in this area. So, you have to rely on the folks below you to give you that insight. And if we're too stubborn to do that, criminal cases aren't going to be made, decisions aren't going to be well thought of. Because you don't understand the space. You can't make those decisions, but so we have to kind of get out of our own heads and kind of get out of our own way sometimes and listen to those that understand the space." (C1, Law Enforcement/Intelligence, Director)

In essence, given the newness of this emergent crypto realm, in the context of its illicit capabilities and use, it is essential to '*listen to those that understand the space.*'[976] This is an essential factor in what Hufnagel described as 'norm making', a "learning process where the norms, after they have been created, are tested at the national level and based on these experiences reframed to become more practicable and accepted."[977] Hufnagel opined that in the context of policing, "formal frameworks established by governments and imposed on police, such as supranational regional legislation, might be less reflected in practice than norms created by or with the input of practitioners in specific border areas."[978] Since in the new space of crypto '*you have nothing to draw on,'* it thus highlights that "consultation with all stakeholders are more accepted, facilitating their implementation, and can even lead to further innovation and lawmaking at practice level."[979]

---

[976] C1, Law Enforcement/Intelligence, Director
[977] Hufnagel, S. (2018). "Policing in the context of global, regional and transnational normmaking. Theories and Practice." In Comparative Policing from a Legal Perspective. Cheltenham, UK: Edward Elgar Publishing. p.44
[978] Hufnagel, S. (2018). "Policing in the context of global, regional and transnational normmaking. Theories and Practice." In Comparative Policing from a Legal Perspective. Cheltenham, UK: Edward Elgar Publishing. p.32
[979] Hufnagel, S. (2018). "Policing in the context of global, regional and transnational normmaking. Theories and Practice." In Comparative Policing from a Legal Perspective. Cheltenham, UK: Edward Elgar Publishing. p.47

The Role of Blockchain Forensics

The work of blockchain forensic providers is a key aspect of the crypto realm; indeed, without it, crypto products would either collapse or be fully susceptible to criminal misuse. There are extensive and increasing providers in the industry with a purpose of making the global crypto community safer and more trusted as a technological tool. In this emergent crypto space, financial flows may be available on a surface level. As a respondent noted:

> "What I think is missing sometimes from that conversation, is the fact that those financial flows are also more visible than they ever have been in human history" (B6, Private/Reporting Entity, Head of Legal and Government Affairs.)

As traditional providers,[980] are gatekeepers to the financial industry,[981] blockchain forensics have become the new gatekeepers of the blockchain industry. However, just as with other sectors, different blockchain forensic providers differ in how they are geared to function, from their capabilities to their intended output, as respondents noted:

> "So those three, law enforcement and regulators, to financial institutions, sort of large financial institutions that are thinking about how to engage with crypto. I think it's really what you're doing. So, we have a tool that we use across those three verticals. And that one tool includes a forensics tool, which is used as a tracing tool, essentially, to follow the flow of funds. And investigators use and compliance officers use that. And we also have a transaction monitoring solution, which is used primarily by financial institutions and crypto businesses as part of their crypto compliance stack. So, it is essentially, it's the same data set, the same tool being used across those three verticals." (B6, Private/Reporting Entity, Head of Legal and Government Affairs.)

> "So, there are a few things one is the kind of workflow. So, if you're a banker, the way you do your financial investigation is very different from if you were a police investigator, and how you conduct your financial investigation. They look for different things, they look for different data points. It also depends on whether an investigator needs to collect information from an evidence perspective, for example, to bring it to courts, if you need to bring things to a court of law, your evidence trail almost needs to be akin to a clean evidence track. Whereas if you're a financial investigator that just simply wants to move

[980] Accountants, art advisers, bankers, corporate service providers, lawyers, luxury goods dealers, notaries, private wealth managers and real estate agents
[981] FATF (2003) "Money laundering typologies 2003-2004."

> quickly and freeze funds, you're trying to just get to the quickest point of information, and you don't quite care about maintaining a solid evidence trail that will then hold up in a court of law, right. So, there's a few different this kind of those things, what bankers are doing is, they're essentially trying to protect their institutions. They're trying to maintain financial integrity, they're trying to identify negative trends or potential hazards to their own bank, and the reputational risks to try to find illicit funds. That's very different from what a law enforcement official does. And so, the tools themselves are geared differently. Really, instead of algorithmic structures, I think in the data, the way the data collection is handled, that really makes the difference and of the underlying technology." (B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs.)

A key aspect of crypto-related AML work concerns machine learning. While this is, of course, also present in other sectors where "machine learning and data-mining methods have been applied to discriminate fraudulent transactions and to predict whether new transactions are fraudulent."[982] It is particularly prominent in the crypto context by virtue of information flows on the blockchain. In brief, machine learning is the "discipline focused on designing computer systems that automatically improve through experience."[983] In essence, machine learning is "improving some measure of performance P when executing some task T, through some type of training experience E."[984] The dataset, which is used to train machine learning enabled generative models (whereby generative models fundamentally encompasses attempting to identify a language someone is speaking by first understanding different languages and then 'matching' the many languages to the spoken one).[985] At its core, machine learning's benefits have been argued as an innovative solution to improvements in performance, for example, the AML sector.[986] Where sets

[982] Han, Jingguang and Huang, Yuyun and Liu, Sha and Towey, Kieran, (2020). "Artificial Intelligence for Anti-Money Laundering - A Review and Extension." Digital Finance Vol. 2, p.19.
[983] Ferrario, Andrea and Loi, Michele, (2021). "Algorithm, Machine Learning and Artificial Intelligence." p.3
[984] Mitchell, T. M. (1997). "Machine Learning." (1 edition). McGraw-Hill Education. p.2.
[985] Sargur N. Srihari, (2010). "Machine Learning: Generative and Discriminative Models."
[986] Kumar, P. et al. (2022). "The fight against money laundering: Machine learning is a Game Changer." McKinsey & Company.

of "data feed ML models able to learn from data sets to 'self-improve' without being explicitly programmed by humans."[987]

Given privacy considerations, synthetic datasets are used to protect "consumer privacy, including through the generation and use of tailor-made, synthetic datasets, which are put together for the purposes of ML modelling, to create as-realistic-as-possible dataset comparable original data, without endangering pertinent personal information data."[988] In brief synthetic data is to "take an original (and thus sensitive) dataset, use it to train a machine learning enabled generative model, and then use that model to produce realistic, yet artificial data that nevertheless has the same statistical properties as the underlying, real data."[989] In other words, to create an as-realistic-as-possible dataset comparable to original data without endangering pertinent personal information data. Synthetic data has been theorized, scrutinized and validated by a number of academics exploring the potential positive effects as it has as "no room for leakage,"[990] as synthetic data has been found to be a valid alternative to original data.[991] This has been suggested to not challenge privacy but rather provides a "more refined approach to protecting privacy with synthetic data.,"[992] whereby "scientists can be as productive with synthesized data as they can with control data."[993]

[987] OECD (2021), "Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers." p.15.
[988] OECD (2021), "Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers." p.38.
[989] Bellovin, Steven M. and Dutta, Preetam K. and Reitinger, Nathan, (2018). "Privacy and Synthetic Datasets." Stanford Technology Law Review, Forthcoming, p.3-4.
[990] Ibid. p.27.
[991] Neha Patki, Roy Wedge & Kalyan Veeramachaneni, (2016). "The Synthetic Data Vault." In International Conference on Data Science And Advanced Analytics, p.400-10.
[992] Bellovin, Steven M. and Dutta, Preetam K. and Reitinger, Nathan, (2018). "Privacy and Synthetic Datasets." Stanford Technology Law Review, Forthcoming, p.4.
[993] ibid. p.27 citing from Neha Patki, Roy Wedge & Kalyan Veeramachaneni, (2016). "The Synthetic Data Vault." In International Conference On Data Science And Advanced Analytics, p.400-10.

The scholarship is continuing regarding the interplay between privacy-protection jurisprudence and new forms of data generation, where "data protection has grown in response to problems generated by new technology"[994] and, at its core, is a primary consideration to the new data-driven world we live in. Indeed, "much can be learned from making and ascertaining the differences in scope, rationale and logic between privacy on the one hand, and data protection on the other."[995] Where Gutwirth and Hert distinguished between privacy and data protection, where privacy is a 'tool of opacity,'[996] that sets/stops normative limits to power. While data protection is 'tools of transparency,' regulating and channelling necessary/reasonable power,[997] where "data protection explicitly protects values that are not at the core of privacy, such as the requirement of fair processing, consent or legitimacy."[998]

As for data pools, while there is no legal definition, in essence, they are a way, which comes in many different forms, whereby stakeholders agree to share digitized information for a particular phenomenon or market.[999] This increases the interoperability between stakeholders to function. By way of example, data within the car industry is used for advanced driver assistance systems.[1000] So too in the healthcare industry, where clinical trial data is held by pharmaceutical firms and public health authorities containing consumption and costs of pharmaceutical products.[1001] A

[994] S. Gutwirth and P. De Hert, (2006) "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. Claes, A. Duff and S. Gutwirth (eds), Privacy and the criminal law, Antwerp, Oxford: Intersentia, 2006, p. 62.
[995] Ibid.
[996] Ibid.
[997] Ibid.
[998] Supra. n.994, p.79.
[999] As expressed earlier of peer-to-peer systems in sex trafficking, firearms registries, airline industries, etc. See also Gaafar, Roba, (2022). "Pooling of Health Data For Biomedical Research."; Lundqvist, Bjorn and Murati, Erion, (2020). "Collaborative Platforms and Data Pools for Smart Urban Societies and Mobility as a Service (MaaS) from a Competition Law Perspective." Faculty of Law, Stockholm University Research Paper No. 75.
[1000] Jonas Frank, (2017). "Data Governance Regimes in the Digital Economy: The Example of Connected Cars."
[1001] Peter Groves et al, (2013). "The 'Big Data' revolution in firms." McKinsey.

further example is clinical patient information held by physicians, but might also be shared for financial data reporting requirements. The very digitization of core financial activities from the standpoint of private/reporting entities, have made it all the more possible to detect, deter and prevent financial crimes.[1002] In this study, respondents expressed the highly valuable nature of data, and the corresponding utilities for which they are used depend on the user's objectives. As a respondent in the LEA/Intelligence noted earlier:

> "Everybody has different parcels of data that we need to get our access to prove a crime. So yeah, there's a lot of gaps being filled. But it's also that market becomes infinitely larger" (C1, Law Enforcement/Intelligence, Director)

As blockchain forensics are still in the early stages of collecting data, a point emphasized by respondents,[1003] the data aggregation required to effectively conduct complete forensic work, including a full picture of a transactional life cycle between on-link and off-link transactional ramps is still being aggregated. The data pooling and/or trading,[1004] which is necessary for a fuller picture relating to a transactional lifecycle has been and will continue to central down to data governance considerations around privacy,[1005] since "digital financial products/services have

[1002] Douglas W. Arner et al. (2015). "The Evolution of Fintech: A New Post-Crisis Paradigm." 47 GEO. J. INT'L L. 1271; Patrik Alamaki & Daniel Broby (2019), "The Effectiveness of Regulatory Reporting by Banking Institutions."; Dirk A. Zetsche et al. (2020). "Digital Finance Platforms: Toward a New Regulatory Paradigm." University of Pennsylvania Journal of Business Law.

[1003] B9, Private/Reporting Entity, Senior Advisor on Government and Private affairs: "If you use a tool that's only been collecting illicit activity and kind of clustering them since 2018, or 2021, or 2020, you're missing out. Because it doesn't have that duration, that history of the blockchain to check against"
C1, Law Enforcement/Intelligence, Director: "And then when these blockchain analytic companies are still in the infancy of building out capabilities to trace multiple coins and trace across smart contracts and trace NFT's, there's not a lot of data that goes along with those"

[1004] Néstor Duch-Brown et al, (2017). "The economics of ownership, access and trade in digital data." 1 JRC Digital Economy Working Paper; Dan L Burk, (2015). "Patents as Data Aggregators in Personalized Medicine." Vol. 21 Issue.2, Boston University Journal of Science and Technology Law 233–255

[1005] Derived from the Latin term "privatus" which means separate from the rest. At its core, to separate personal information from that of a government, group and/or public, it has become foundational for individual rights of happiness, speech, worship and dignity: Dialogus de Scaccario: The Course of the Exchequer. Edited and translated by Charles Johnson, F. E. L Carter, and D. E. Greenway. 2nd ed. Oxford: Oxford University Press, 1983.

direct implications on data privacy and confidentiality."[1006] As has been expressed by early emerging technologies of yellow journalism,[1007] to allow "what is whispered in the closet [to] be proclaimed from the house-tops."[1008] As the market for crypto products is expanding, data aggregation by blockchain forensics is not only an important piece of the puzzle, but more so, an essential foundation in blockchain forensic investigations.

[1006] OECD (2021), "Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers.", p.38
[1007] Sensationalism and crude exaggeration
[1008] Samuel D. Warren & Louis D. Brandeis, (1890). "The Right to Privacy." 4 HARVARD L. REV. p. 195

Chapter 7 – Conclusions

Overview

The final chapter will summarize key points from this thesis and outline steps forward. The pertinent themes of security, privacy and safeguards will be analyzed to 'protect the integrity of the international financial system.' While from a financial system standpoint, the "spillovers to other parts of the financial system from the stress in the crypto industry have been minimal. The lack of spillovers to date may be attributable in part to the relatively limited number of interconnections between the crypto ecosystem and the banking system."[1009] This lack of interconnections, while maybe good to alleviate capital stress on the market, it has, arguably, frustrated interoperability needed for AML requirements,[1010] and as such, opened pandora's box of newly profitable innovations of evil.[1011] From a financial crime perspective, the crypto ecosystem, not in and of itself, but rather, the capabilities to exploit it, have seen a surge to over $20 Billion in illicit use in 2022.[1012] The myths espoused by Crypto marketers,[1013] maximalists,[1014] and fundamentalists,[1015] regarding the uniqueness and newness of Crypto are not only false,[1016]

[1009] Board of Governors of the Federal Reserve System (2023). "Remarks by Governor Waller on Digital assets."
[1010] "Multiple reports analyzing the blockchain/DLT adoption by organizations have pointed out that blockchain integration with other systems (e.g., other blockchains or other non-DLT information systems) is one of the crucial challenges." World Economic Forum (2020). "Bridging the Governance Gap: Interoperability for blockchain and legacy systems. Technical Report.".
[1011] Refer to chapters 1, 3, 5 and 6 regarding: Pedophilia and Child Abuse, Extortion and Ransom, Financing of Weapons of Mass Destruction, Human Trafficking, Organ Trafficking, Darknet Narcotics' Amazon-Prime-style trade and identity thefts, and Terrorist Financing.
[1012] "This is a lower bound estimate — our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that this figure doesn't capture proceeds from non-crypto native crime (e.g., conventional drug trafficking involving cryptocurrency as a mode of payment)." Chainalysis (2023). "2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking."
[1013] Milton, I.J. (2022) Mike Tyson, Tom Brady: Celebrity crypto endorsements are disasters for fans, Bloomberg.com. Bloomberg. Available at: https://www.bloomberg.com/features/2022-crypto-celebrity-endorsements/.
[1014] Munster, B. (2019) Andreas M. Antonopoulos: Why Bitcoin Maximalism is unhealthy, Decrypt. Decrypt. Available at: https://decrypt.co/5253/andreas-antonopoulos-bitcoin-maximalism-adoption-ethereum.
[1015] Po-Keng Cheng. Fundamentalists in the cryptocurrency markets. 2022. ffhal-03679207f
[1016] Supra n.1009. "First, let's consider distributed ledger technology. The technology is simply a database management protocol that has various permissions regarding who can write to the database and who can read the database. Although

but have been categorically disproven.[1017] In examining the sophistication of illicit use and the considerations required to stabilize security, privacy and safeguards, interview data is helpful in identifying needed considerations to not only protect the financial system but also assist in answering: "*What can we do that might be able to make it easier for us to identify criminals, but not provide too much of a burden to the ecosystem?. "*[1018]

Summary of Chapters

In chapter 3, I outlined the history and brief technical specifications, that is, the communication infrastructure of the internet. This analysis assisted in bridging the discussion to communication gateways, nodes, utilizing the internet to send and receive messages, that is, the fundamentality of blockchain technology based off a distributed system of communication. The necessary considerations of conventional money laundering methods were then briefly discussed, in order to highlight emerging frontiers of dark payments, through Crypto, becoming more sophisticated – whereby an entire industry of blockchain forensics capabilities took form to track, monitor and trace such illicit use.

In Chapter 4, the current Crypto legal frameworks were discussed. In the context of FATF frameworks, the roots of these international laws have evolved over time to compensate for

---

this technology is fundamental for the creation of crypto assets, there is nothing in this technology that restricts it to being used solely in the crypto ecosystem. In fact, distributed ledger technology is being explored to potentially address a wide range of data management problems."

[1017] Appendix III – The 1992 Crypto Anarchist Manifesto "The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification."
D1, Professor of Computer Science: "I called Bitcoin, a lab experiment that escaped. It was not engineered. Nakamoto had the science, but not the engineering. There are variants of the blockchain that can support much higher transaction rates and have much better anonymity guarantees."

[1018] C1, Law Enforcement/Intelligence, Director

emerging threats and new intelligence considerations. As such, the pillars of the AML/CFT regime of, prevention and enforcement,[1019] have been continuously highlighted to nations, with arguably, non-steady results.[1020] The *inter* and *intra* national and international institutional frictions of sovereignty, nationality principle, ubiquity theory, and or subjective territoriality principle,[1021] play a substantial role in the FATF international frameworks.

In Chapter 5, the analysis shifted to build on the preceding basic-level knowledge in chapters 3 and 4, where Crypto was examined in light of interview data, literature, and reports. The themes of security, privacy and safeguards were scrutinized through sub-themes in order to tease out relevant data to contribute to knowledge. Remarkably, given the newness of Crypto *functions'* utility, and "*due to the evolving nature of blockchain and the virtual asset sector. Blockchain analytics is probabilistic and data produced has an inherent level of uncertainty associated with it."*[1022] As such, the themes identified by interview data assisted in highlighting commonalities *within* and *across* themes pertaining to all three category groups: Law Enforcement/Intelligence, Public/Regulator and Private/Reporting Entity. On this basis, a number of conclusions were drawn and supported by the data.

[1019] Reuter, Peter, and Edwin Truman. 2004. Chasing Dirty Money: The Fight against Money Laundering. Washington, DC: Institute for International Economics.
[1020] "In terms of laws and regulations, 76% of countries have now satisfactorily implemented the FATF's 40 Recommendations… However, many countries still face substantial challenges in taking effective action commensurate to the risks they face" FATF (2022). "Report on the State of Effectiveness Compliance with FATF Standards." FATF, Paris, www.fatf-gafi.org/publications/documents/effectiveness-compliance-standards.html
[1021] Koh, J. (2006). Suppressing terrorist financing and money laundering. New York: Springer; Stessens, G. 2000. Money laundering: A new international law enforcement model. Cambridge:
Cambridge University Press.
[1022] FATF (2021), Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France, p. 30

In Chapter 6, the thesis builds on the discussions of chapter 5, in order to highlight considerations in approaching this new hyper-velocity, cross-border phenomenon. As there will always be misuse and illicit use of any payment infrastructure, globally, the critical question for consideration, is what more can be done effectively and efficiently to minimize illicit use. In approaching such a question, interview data assisted in highlighting the cultural foundation of AML/CFT frameworks, and the operational prioritization when conducting AML/CFT work.

Crypto Wild West – Where is the Order?

In all Crypto myths and fetishizations of bandwagon profit-driven whales,[1023] it is important to recognize a wisdom-based timeless principle: "So let us regard this as settled: what is morally wrong can never be advantageous, even when it enables you to make some gain that you believe to be to your advantage."[1024] Crypto, in and of itself, is not morally wrong, but the societal attribution of 'value' to it, has provided multiple avenues for sophisticated and expediated forms of crime. 10,000 Bitcoins were 'valued' to be worth two pizzas in 2010,[1025] and tens of thousands of dollars 'valued' a single Bitcoin in 2020 and later, thereby attracting depraved innovations of evil.[1026] As for safeguards, compliance postulating is '*laughable,*'[1027] where spending on AML compliance reached USD$213 billion and USD274 billion in 2022 globally,[1028] while total estimated laundered funds are USD$2 trillion, almost nine times as much.[1029] The

[1023] Supra n.1913, n.1014, and n.1015 and Chapter 6 for "whales."
[1024] Cicero, Marcus Tullius. Selected works. United Kingdom, Penguin Publishing Group, 1971.
[1025] Kamau, R. (2022). "What is Bitcoin Pizza Day, and why does the community celebrate on May 9, 22." Forbes Magazine.
[1026] Refer to chapters 1, 3, 5 and 6 regarding: Pedophilia and Child Abuse, Extortion and Ransom, Financing of Weapons of Mass Destruction, Human Trafficking, Organ Trafficking, Darknet Narcotics' Amazon-Prime-style trade and identity thefts, and Terrorist Financing.
[1027] Refer to 'Cultures of Compliance' section in Chapter 6.
[1028] LexisNexis Risk Solutions (2022). "True cost financial crime compliance." LexisNexis
[1029] Money Laundering Overview (no date) United Nations : Office on Drugs and Crime. Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html

money has been laundered, with conservative estimates, un accounting for the total picture of illicit crime,[1030] and the heinous predicate crimes have been conducted, where the victims are arguably left, forever damaged. Order must be established to "*reign in these sorts of solutions."*[1031]

The Legal Definitions – Filling a Vacuum of Wild West

Crypto has been suggested to have "*all of the indicia of property"* where "*cryptoassets are therefore to be treated in principle as property."*[1032] Crypto has also been suggested to be funds,[1033] while FATF states that "*they may fall under other kinds of financial assets, such as securities, commodities, derivatives or fiat currency."*[1034] Hacker and Thomale define Crypto as "cryptographically-secured coupons which embody a bundle of rights and obligations"[1035] The fact that Crypto has yet to be defined suggests that the purported definitions do not portray its characteristics, and has led to confusion where "*How do we even explain what we're trying to regulate? When there's different definitions for digital assets, digital currency, virtual currency, Cryptocurrency, Crypto asset token. There's so many that it's a challenge."*[1036] In terms of definitions, Liechtenstein is an example where they did not rely on separate classifications and

[1030] Supra n. 1012. Where the absence of evidence is not evidence of absence.
[1031] B3, Private/Reporting Entity, Head of AML & Sanctions
[1032] UK Jurisdiction Taskforce (2019) Legal statement on Cryptoassets and smart contracts . Available at: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-
[1033] International Monetary Fund Staff Discussion Note. 'Virtual Currencies and Beyond: Initial Consideration'. (January 2021). SDN/16/03 https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.
[1034] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
[1035] Hacker, P. and Thomale, C. (2018) 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law', Degruyter European Company and Financial Law Review, 15(4). Available at: https://www.degruyter.com/view/journals/ecfr/15/4/article-p645.xml
[1036] C1, Law Enforcement/Intelligence, Director

consequently relied on a general classification as a new legal element for a new, abstract and neutral approach. The Liechtenstein Blockchain Act defines this general definition as:[1037]

> "a piece of information on a TT System [i.e., a DLT Transaction System] which can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights; and is assigned to one or more TT Identifiers [i.e., a Wallet-Address]"

Liechtenstein refrained from using terms such as blockchain and DLT, in order to cover all similar kinds of such technologies. Where TT Systems is defined as a "transaction system which allows for the secure transfer and storage of Tokens and the rendering of services based on this by means of trustworthy technology."[1038] Trustworthy technology is defined as "technologies through which the integrity of tokens, the clear assignment of tokens to TT Identifiers and the disposal over tokens is ensured."[1039] TT-Identifiers are defined as "an identifier that allows for the clear assignment of tokens."[1040]

FATF's treatment of the definitional aspect that "*they should be applied based on the basic characteristics of the asset or the service, not the technology it employs."*[1041] and then attributes potential *functions* of the technology to have different definitions of "*other kinds of financial assets, such as securities, commodities, derivatives or fiat currency"* is unhelpful, has created confusion, and according to the laws of logic, a contradiction. Without cryptographic technology, "*the basic characteristics of the asset or the service"* would not exist. Whereby Aristotle expressed that "It is impossible that the same thing can at the same time both belong and not belong to the

[1037] Liechtenstein Blockchain Act (2019). Liechtenstein. Available at: https://www.lcx.com/wp-content/uploads/2020_Liechtenstein_Blockcchain_Laws_Translation_English.pdf
[1038] Ibid.
[1039] Supra n.1037.
[1040] Supra n.1037.
[1041] Supra n.1037.

same object and in the same respect."[1042] Where A and not-A cannot be the same, where not-A is the contradiction of A. In this respect, "according to this principle, the definition of a thing will include the definitions of its parts."[1043] The Liechtenstein approach aligns with the analysis in Chapter 5, where the basic characteristic of the asset or service *is* the Cryptographic technology it functions on and should be treated accordingly.[1044] Since if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is not a dog.

Gateways – Interoperability between systems

As Oracles serve as a middleware for data and transactions sharing between entities securely and authoritatively,[1045] they are the bridge between the 'real' and 'virtual' worlds,[1046] in essence, the middleware of Data. As "60 percent of all Bitcoin traffic runs through three internet service providers, and Tor routes traffic for roughly half of Bitcoin nodes,"[1047] at some point, the Crypto will have to touch the 'real' financial system.[1048] The link between on-chain and off-chain movement is complicated not only by the lack of focus on Oracles, but also because "multiple reports analyzing the blockchain/DLT adoption by organizations have pointed out that blockchain integration with other systems (e.g. other blockchains or other non-DLT information systems) is

[1042] Horn, Laurence R. (2008). Contradiction. Stanford Encyclopedia of Philosophy.
[1043] Yu, J. (2001), The Identity of Form and Essence in Aristotle. The Southern Journal of Philosophy, 39: 299-312.
[1044] Daoud. G
[1045] Daoud. G.
[1046] Wintermeyer, L. (2021) Oracles: The invisible backbone of defi and applied blockchain apps, Forbes. Forbes Magazine. Available at: https://www.forbes.com/sites/lawrencewintermeyer/2021/10/14/Cryptohacks-oraclesthe-invisible-backbone-of-defi-and-applied-blockchain-apps/?sh=3aed379a182d.
[1047] Trail of Bits, Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers, June 2022, https://assetsglobal.websitefiles.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf.
[1048] Daoud. G Chapter 5: "The very objective of illicit actors is not to invest in costly sophisticated laundering typologies, computerized integrations and data operations to ultimately collect any Cryptographic codes (NFTs, Cryptocurrencies, tokens, etc.) irredeemable for any fiat currency accepted anywhere… That would be a foolish and non-revenue-generating utilization of resources for illicit enterprises."

one of the crucial challenges."[1049] Interoperability capabilities exist and are used.[1050] From a pragmatic standpoint, in the context of Crypto, being let out of the box, the simple reality was expressed by the following respondent:

> "There's going to be the Crypto option and the legacy option. And those two will have to learn to play together in the sandbox. So, if these legacy anti financial crime software producers aren't open to a Crypto forensic option, and the Crypto or the blockchain forensic firms aren't open to a legacy option, they'll both die." (B10, Private/Reporting Entity, Co-Founder and Chief Compliance Officer.)

Since forcing interoperability can have unintended consequences to lock market participants into an inferior technology.[1051] The focus for AML/CFT checks should be on the choke points, that is, the pressure points, to capture illicit movement.[1052] Since these choke points have still yet to be addressed,[1053] for Crypto, "*the place where it has to touch the existing global financial system is the* plausible point *for regulation."*[1054] Failing which, being '*blocked in terms of visibility*' will continue to provide a systematic veil for criminal enterprises to engage in sophisticated on-ramp off-ramp typologies.[1055]

[1049] World Economic Forum (2020). "Bridging the Governance Gap: Interoperability for blockchain and legacy systems. Technical Report." p.4.
[1050] Refer to Chapter 5 for examples.
[1051] Jean Tirole (2006). "Standards and Intellectual Property: the view of an economist." Letter from the Regulatory Authority for Electronic Communications and Posts, No. 51.
[1052] "The biggest chokepoints and where we have our most success is when the on-ramping or the off-ramping of the virtual currency, so, for instance, getting it into the virtual currency realm. That is where we have our success in our undercover platforms and through our traditional money-laundering investigations." United States Congress (2023). "Terrorism And Digital Financing: How Technology Is Changing The Threat." No. LC67196.
[1053] B9, Private/Reporting Entity, Advisor on Public and Private affairs: "My biggest concern is that there's a huge amount of money that's going back and forth between Crypto and traditional banking, where we just simply are blocked in terms of visibility"
[1054] D1, Professor of Computer Science
[1055] Refer to Appendix IV, and Chapters 3 and 5 for typologies.

Defining Frameworks – Systemic or Sectoral Oversight?

Crypto was designed to disintermediate financial services,[1056] thereby bypassing the need for a centralized entity. Ironically, exchanges, custodians and wallet providers offer central functions to users of Crypto, where arguably, they are the 'new' centralized entities,[1057] requiring users to 'trust' them.[1058] This is evidenced by the fact that these centralized entities,[1059] hold information on the users, can accept or block transactions, and can share transaction data with other organizations. As standard-setting bodies make efforts to develop standards, they are "remain mostly focused on specific products (global stablecoins), issues (financial integrity), sectors (payments, securities, banking), or entities."[1060] This, however, in the face of cross-border high-velocity internet-operative phenomena, limits the effectiveness of non-harmonized and uncoordinated national approaches. The result is gaps left in the Crypto ecosystem, which remain material,[1061] whereby regulatory arbitrage is readily available to '*bypass sanctions…bypass law enforcement'*.[1062]

Domestic oversight treats Crypto differently across national legislations, leading to a non-harmonized cohesiveness internationally, where the innovations of Crypto *functions*

[1056] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Unpublished manuscript.
[1057] As the phrase in the Crypto industry is often touted "Not your keys, not your coins." Moreland, K. (2020). "Not your keys, not your coins. it's that simple." Ledger Academy; Key, A. (2022). "Not your keys, not your crypto: What to know before the next FTX-type meltdown." Decrypt.
[1058] Self-custody and pure cold storage are not involved in this, however, refer to note. 1059 for centralized entities' market reach.
[1059] Where it was estimated that 4.5% of these centralized entities hold 85% of all circulating Bitcoins: Ben Mariem, Sami; Casas, Pedro; Romiti, Matteo; Donnet, Benoit; Stütz, Rainer; Haslhofer, Bernhard, (2020). "All that Glitters is not Bitcoin—Unveiling the Centralized Nature of the BTC (IP) Network" IEEE/IFIP Network Operations and Management Symposium.
[1060] Bains, Parma, Arif Ismail, Fabiana Melo, and Nobuyasa Sugimoto, (2022). "Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets." IMF Fintech Note International Monetary Fund, Washington, DC.
[1061] The FATF's 12-month review of revised FATF standards concluded that many nations have yet to implement VA standards. Those who have are still in the early stages of supervisory regime developments. FATF (2020). "12-month Review Virtual Assets and VASPs." Paris, France.
[1062] A1, Public/Regulator, Deputy Director

overwhelmingly mismatch the speed of regulation.[1063] The "need for harmonization is not only apparent, but necessary."[1064] As such, the focus of regulations should be the 'new' centralized entities, since "banks and fintech firms vie for the same customers with similar services and by taking similar risks, they should be similarly regulated: same risk, same regulation."[1065]

Information Sharing

While Blockchain forensic work is fundamental to a healthy Crypto ecosystem, a central point worth repeating is that according to FATF, "effective information sharing is one of the cornerstones of a well-functioning anti-money laundering/counter-terrorist financing (AML/CFT) framework".[1066] For Crypto products, "cross-border information sharing by authorities and the private sector with their international counterparts is critical in the VASP sector."[1067] The reality however, of cross-border and interagency information sharing is described to have 'institutional frictions' and prevents proactive reciprocity of information-sharing efforts.[1068]

Given the friction in information-sharing efforts and coordination required by nations, the efficacy of the AML/CFT regime is cast into question,[1069] where '*one of the issues that always comes out in mutual evaluation reports is the lack of interagency cooperation.*'[1070] The very

[1063] Nesbitt, E. (2020). "The Scope of Cryptocurrency in the Information Age." In Maniszewska, K. & Piasecka, P. (Eds.), Security and Society in the Information Age Vol. 2. p.179-193. Collegium Civitas Press.
[1064] Chapter 4 discussing nation efforts to continuously harmonize regulations in this space.
[1065] Carstens, Agustín (2018). "A Institute of International Finance Board of Directors dinner: A level playing field in banking." Bank for International Settlements. p.4
.[1066] FATF (2016-2017). "Consolidated FATF Standards on Information Sharing. Paris , updated November 2017, p.6
[1067] FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." FATF, Paris, p.77
[1068] Andreas Riege, (2005). "Three-Dozen Knowledge-Sharing Barriers Managers Must Consider." Journal of Knowledge Management 9, no. 3, p.24
[1069] Caroline Binham, (2016). "Anti-money Laundering Rules Need to be Toughened Up, Warns FSB." Financial Times.
[1070] A3, Public/Regulator, Executive Secretary

objective of these information-sharing cooperative efforts, is, arguably, to extract actionable data which is useful for "tactical and strategic decisions."[1071] However, the risk-based approach does not currently serve this purpose where the "information sharing required to be useful and actionable has been demonstrated to involve not only a select department in the individual entity, but all levels of an entity for the information to become useful and actionable."[1072] This requires an intelligence-led approach for continuous improvement and information gathering, to think it '*through it on a deep risk level,*'[1073] as opposed to a reactionary based compliance tick-the-box approach, where emerging technological advancements have effectively been able to bypass AML checks.[1074]

Final word

Societal attributions of radically volatile and subjective value have reinforced the Crypto phenomenon.[1075] The money laundering problem paints a darker picture where "*the banksters have always said and always will that it's a big black hole where the information goes in. You never hear anything else. And the reason you don't hear is because they're not allowed to talk about it*."[1076] The dark world of payments where "bankers have been tolerating the laundering of proceeds of crime without obvious harm,"[1077] has been illustrated where "even extreme fines had

[1071] Royal Canadian Mounted Police, (2015) Criminal Intelligence Program.
[1072] Paul Hendriks, "Why Share Knowledge? The Influence of ICT on the Motivation for Knowledge Sharing," Knowledge and Process Management 6, no. 2 (June 1999): p.91.
[1073] B1, Private/Reporting Entity, Founder & Chief Compliance Officer.
[1074] Y. J. Fanusie, (2020). "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them," The Digital Social Contract: A Lawfare Paper Series ,p.1–23.
[1075] Daoud G. "10,000 Bitcoins were 'valued' to be worth two pizzas in 2010, and tens of thousands of dollars 'valued' a single Bitcoin in 2020 and later." No criminal would risk the punishments of FATF predicate offences for two pizzas. That is not worth the time, effort, resources and risk to conduct designated FATF predicate offences. The pepperoni is simply not worth calculating a serious risk-reward ratio.
[1076] C4, Law Enforcement/Intelligence, Director and Founder of Financial Intelligence Agency of [Country Anonymized]
[1077] Verena Zoppei, (2015). "Money Laundering: A New Perspective in Assessing the Effectiveness of the AML Regime." European Review of Organised Crime, Vol.2 Issue.1, p.140.

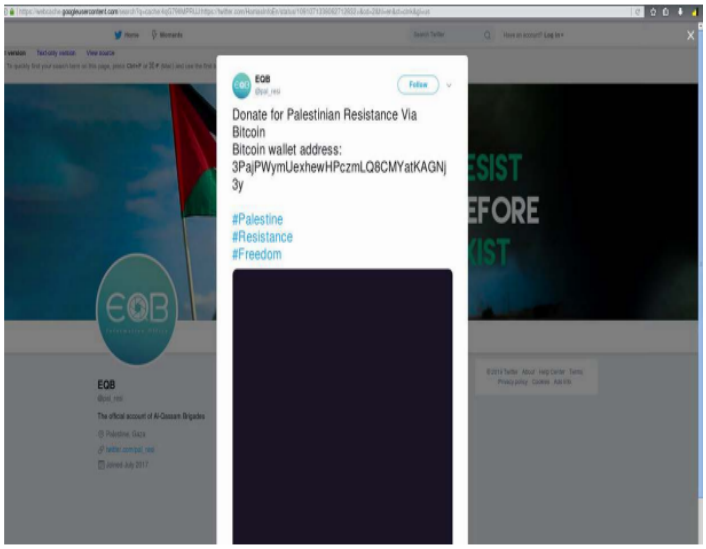
no impact on the banks' financial prowess."[1078] The distrust in traditional centralized financial institutions galvanized Crypto enthusiasts, where comparisons of 'value' are constantly sensationally debated despite the fact that "banks and fintech firms vie for the same customers with similar services."[1079]

Criminals capitalize on capital. Wolves capitalize on sheep. The guilty capitalize on the innocent, "Well, well, let's get on with it. . . ."[1080]

[1078] Erin Lawlor-Forsyth and Michelle Gallant, (2018). "Financial Institutions and Money Laundering: A Threatening Relationship." Journal of Banking Regulation Vol 19, Issue.2, p.147.
[1079] Carstens, Agustín (2018). "A Institute of International Finance Board of Directors dinner: A level playing field in banking." Bank for International Settlements. p.4.
[1080] Sartre, J. (1975). "No exit, (Huis clos) a play in one act: & The flies (Les mouches) a play in three acts." New York, A.A. Knopf. p.27.

Appendix I – Crypto Terrorism Financing

Al-Qassam Brigades Campaign

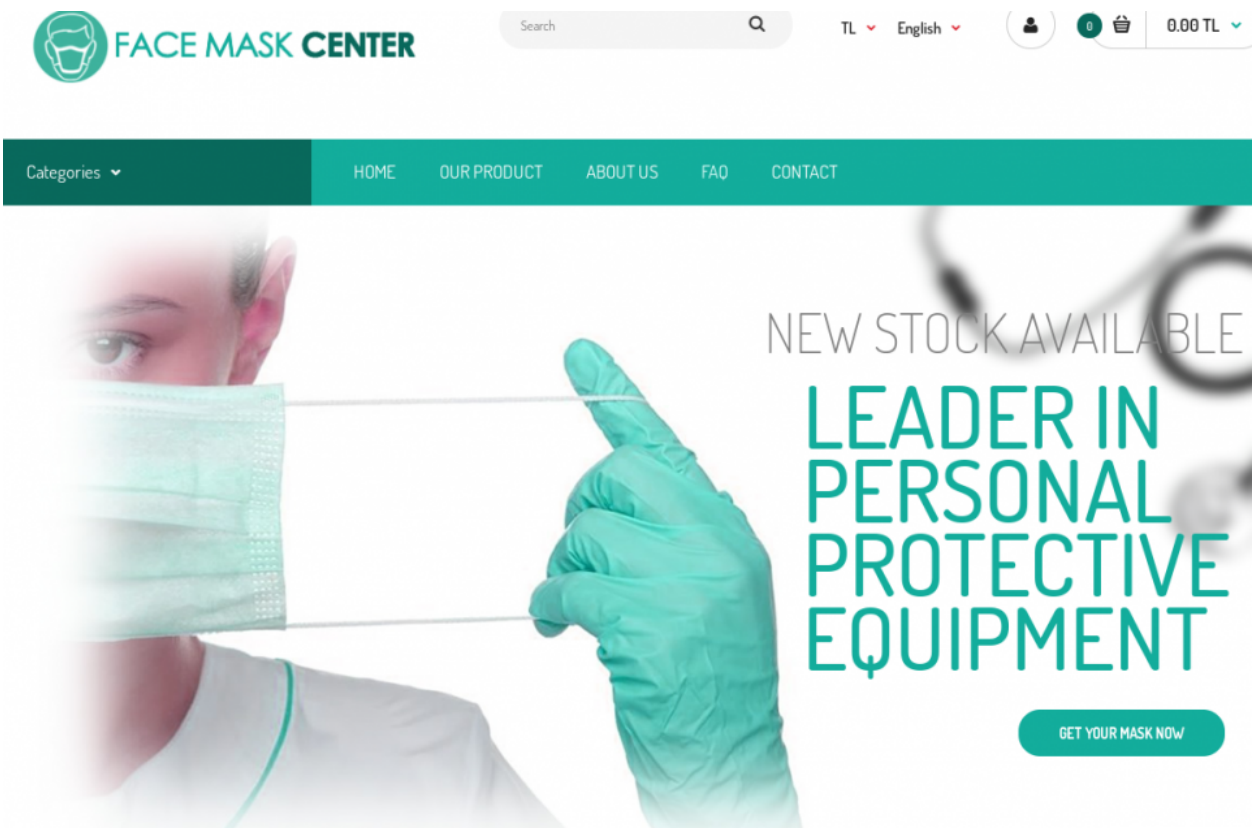


Source: The United States Department of Justice. (2020). "Global Disruption of three terror finance cyber-enabled campaigns."

Al-Qaeda Campaign

Source: The United States Department of Justice. (2020). “Global Disruption of three terror finance cyber-enabled campaigns.”

ISIS Campaign



Source: The United States Department of Justice. (2020). “Global Disruption of three terror finance cyber-enabled campaigns.”

Appendix II – Crypto Extortion

SamSam

#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:
Step1: You must send us 0.7 BitCoin for each affected PC OR 3 BitCoins to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.7 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: Redacted

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
* Our Site Address: http://jcmi5n4c3mvgtyt5.onion/familiarisingly/
* Our BitCoin Address: 1MddNhqRCJe825ywjdbjbAQpstWBpKHmFR

(If you send us 3 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC`s' in your comment)
(Also if you want pay for 'all affected PC`s' You can pay 1.5 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'

Test Decryption

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

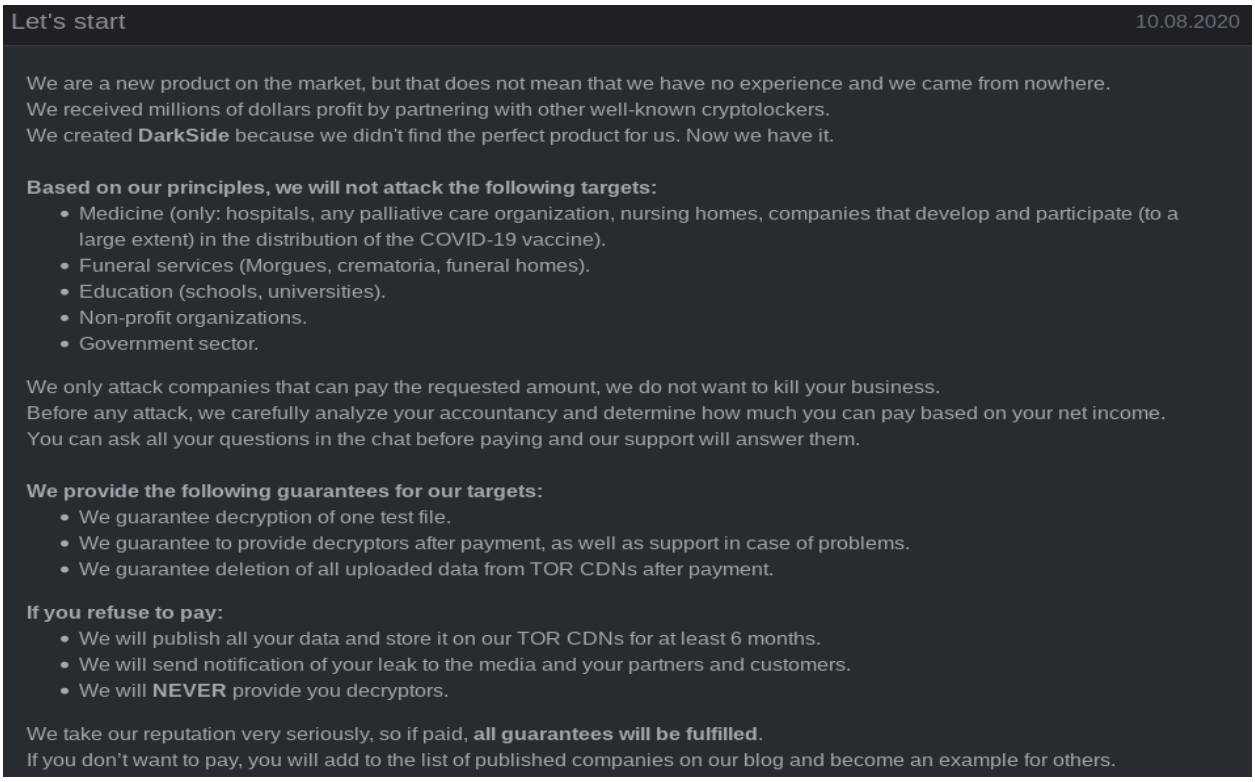
If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), Tel
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.

Source: Chuang, T. (2018). "Cyber attack on CDOT computers estimated to cost up to $1.5 million so far." The Denver Post.

CryptoLocker

Source: Chuang, T. (2018). "Pay us bitcoin or never see your files again: Inside the highly profitable underworld of Ransomware." The Denver Post.

Darkside



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

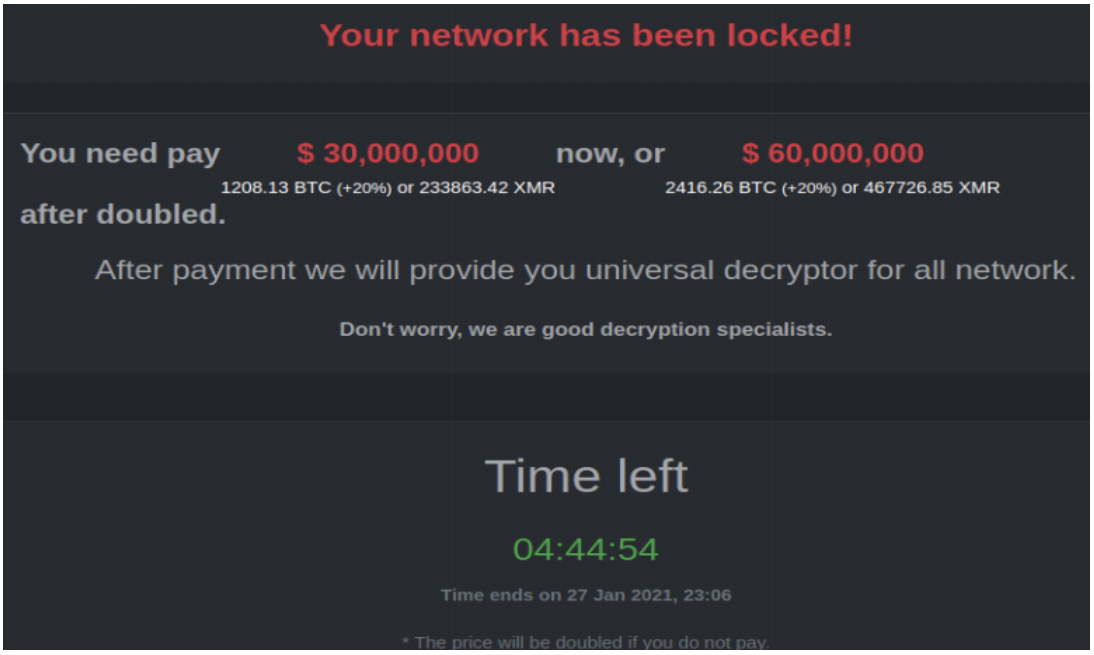
We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.



Your network has been locked!

You need pay $ 30,000,000 now, or $ 60,000,000
1208.13 BTC (+20%) or 233863.42 XMR 2416.26 BTC (+20%) or 467726.85 XMR
after doubled.

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

Time left

04:44:54

Time ends on 27 Jan 2021, 23:06

* The price will be doubled if you do not pay.

Source: "A closer look at the Darkside Ransomware Gang" (2021) *Krebs on Security*.

Appendix III – 1992 Crypto Anarchist Manifesto

Timothy C. May on 12:11:24 PST, Sunday, November 22, 1992

"*A specter is haunting the modern world, the specter of Crypto anarchy.*

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement Cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; Crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of Crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will Cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, Crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of

mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

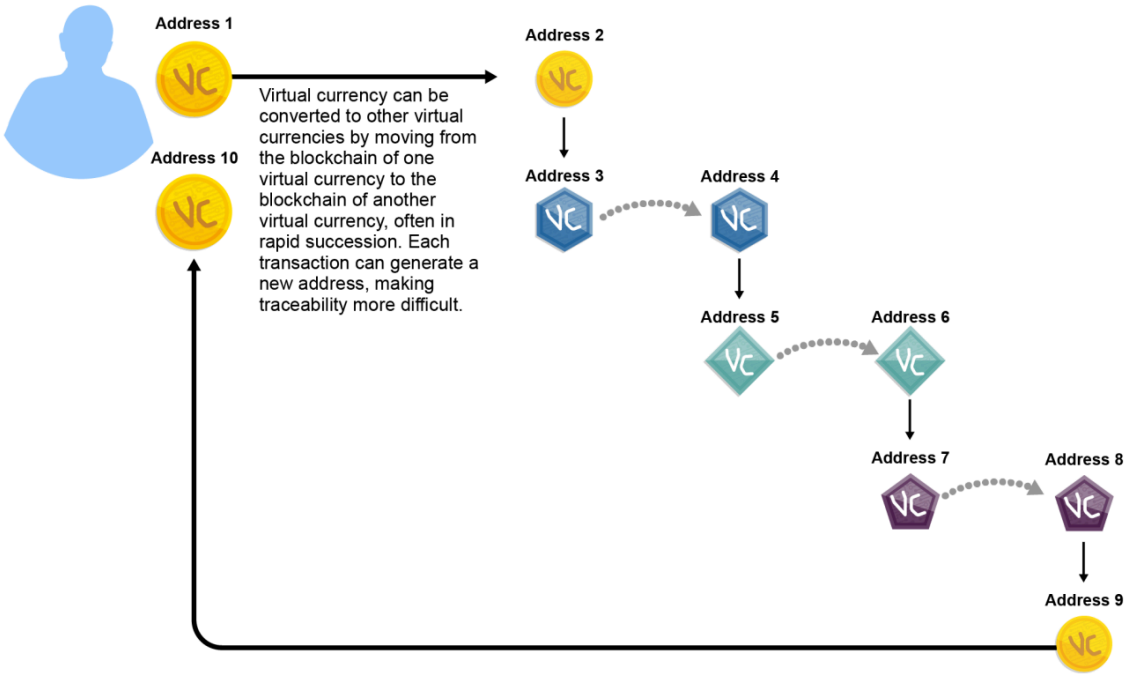
Arise, you have nothing to lose but your barbed wire fences!

```
Timothy C. May          | Crypto Anarchy: encryption, digital money,
tcmay@netcom.com        | anonymous networks, digital pseudonyms, zero
408-688-5409            | knowledge, reputations, information markets,
W.A.S.T.E.: Aptos, CA   | black markets, collapse of governments.
Higher Power: 2^756839  | PGP Public Key: by arrangement."
```

Source: May, T.C. (1992) "The Crypto Anarchist Manifesto."

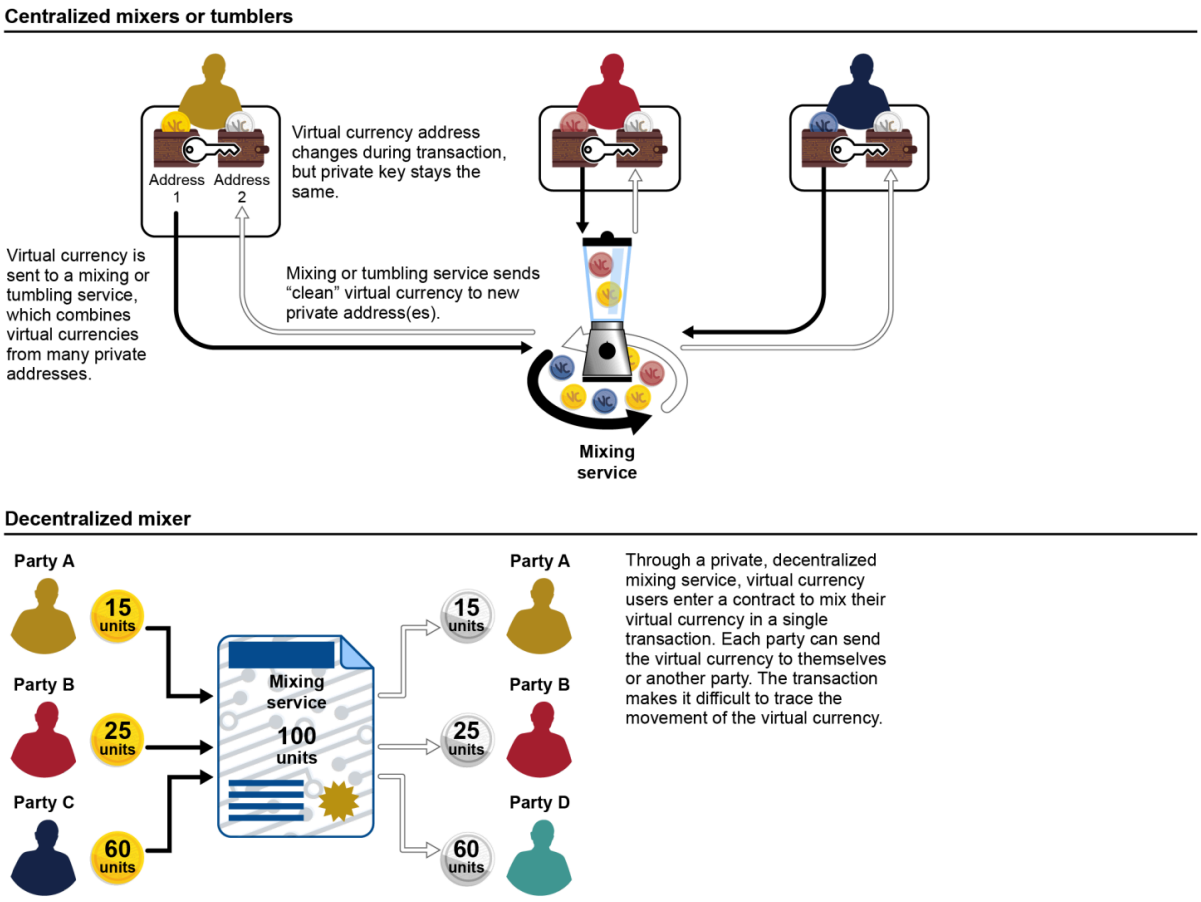
Appendix IV – Sophisticated Crypto Laundering Typologies

Chain Hopping



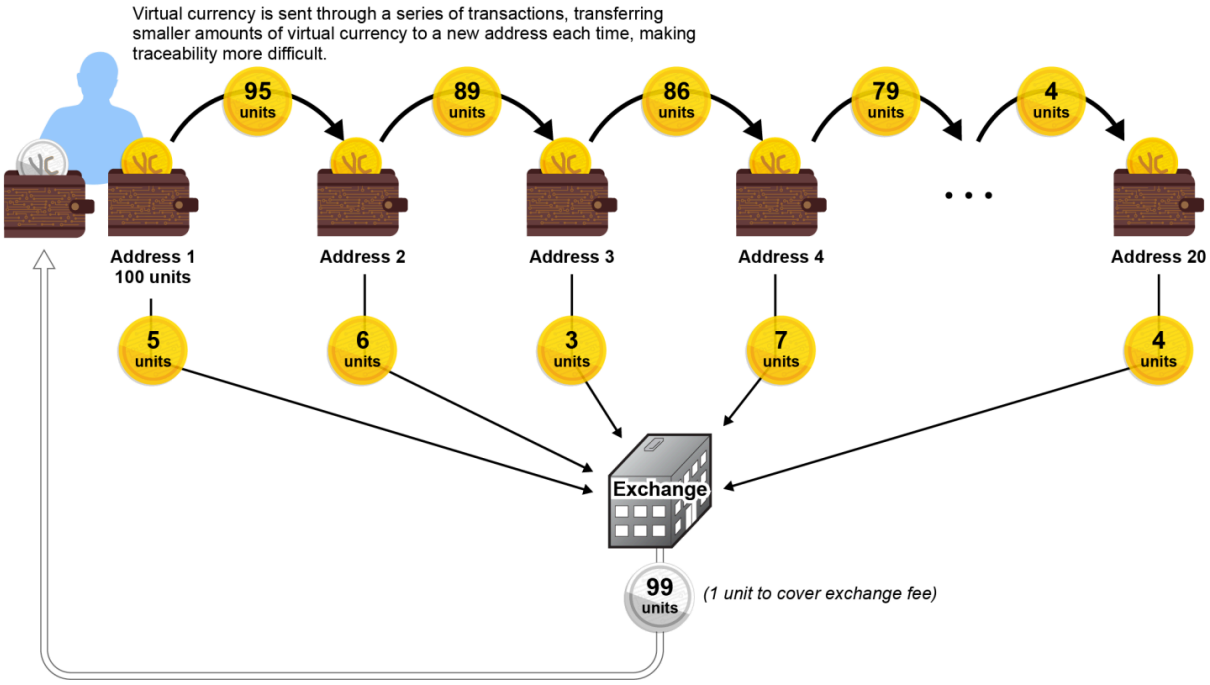
Source: United States Government Accountability Office (2021). "Virtual Currencies Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking." Analysis of United States Attorney General Digital Task force, Cryptocurrency Enforcement Network, GAO-22-105462, p.70.

Mixers and Tumblers



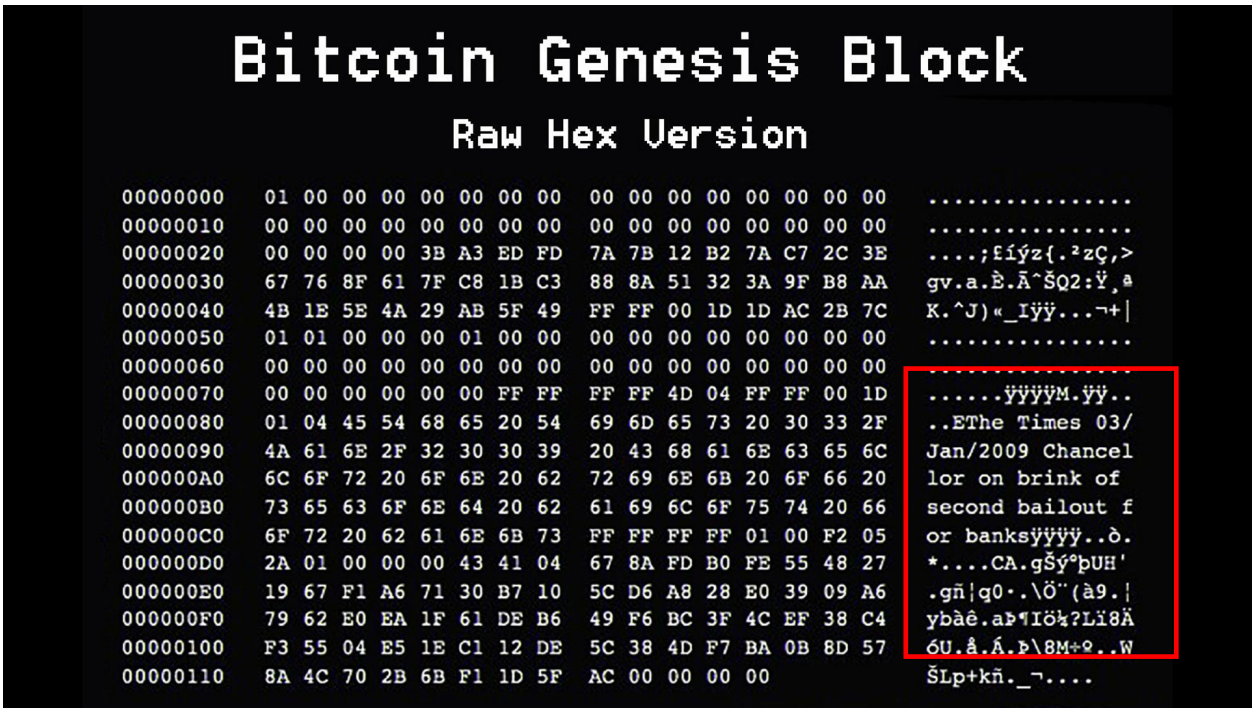
Source: United States Government Accountability Office (2021). "Virtual Currencies Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking." Analysis of United States Attorney General Digital Task force, Cryptocurrency Enforcement Network, GAO-22-105462, p.72.

Peel Chain



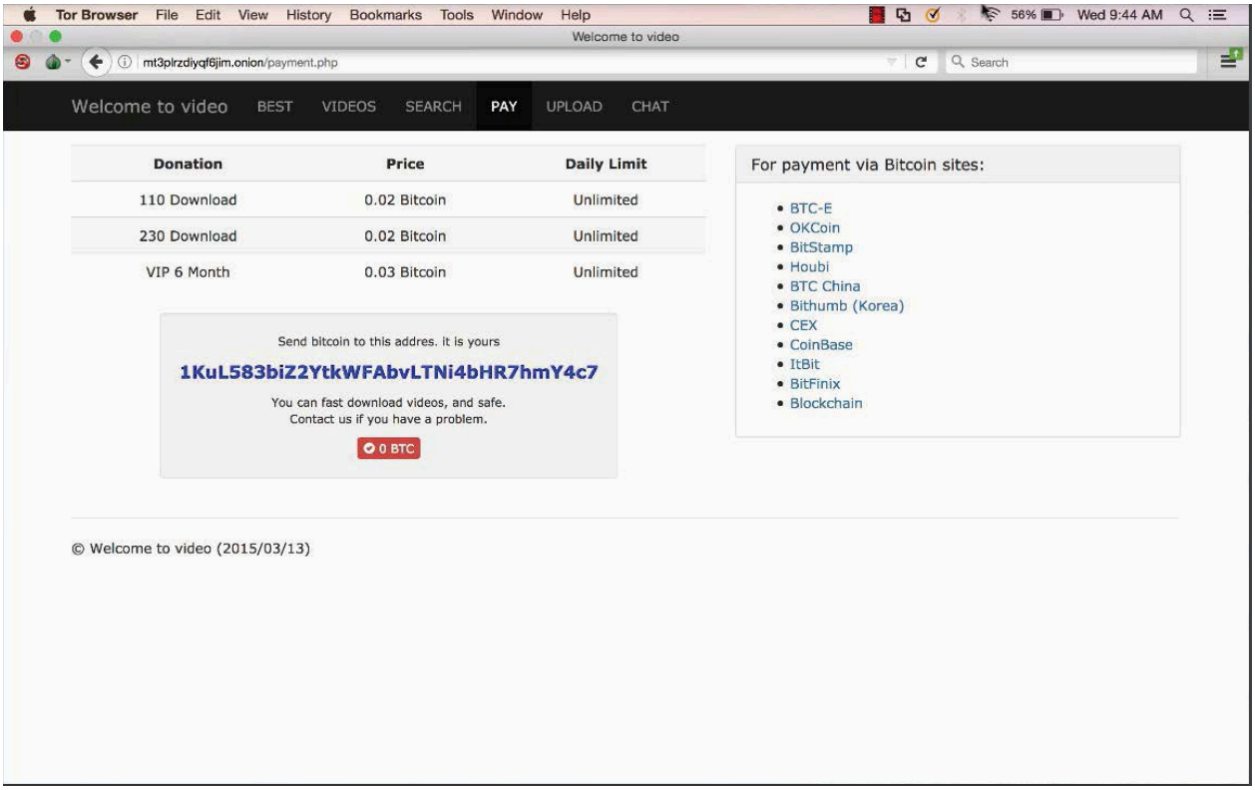
Source: United States Government Accountability Office (2021). "Virtual Currencies Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking." Analysis of United States Attorney General Digital Task force, Cryptocurrency Enforcement Network, GAO-22-105462, p.73.

Appendix V – Raw Hex Version of Bitcoin Genesis Block



Source: Giudice, D. (2022). "Bitcoin Gensis Block – Consensus Algorithm." Cryptonomist.

Appendix VI – Welcome to Video Webpage Screenshot



Source: Department of Justice, Office of Public Affairs (2019). "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin."