UK FINANCE

NAVIGATING THE PATH TO RESPECTABILITY:

Making sense of the financial crime risk posed by cryptoassets and how to manage it appropriately

September 2021

In partnership with: PLENITUDE

CONTENTS

FOREWORD

Economic crime threats are continually evolving, impacted by the emergence of new technologies, services and products, and the cryptoasset sector is no exception. Ten years ago, Bitcoin mining had become the token of choice for darknet markets with over a third of cryptoasset transactions estimated to be illicit. Today the direction of travel is very different. International standard-setters such as the Financial Action Task Force (FATF) have laid down the challenge for the crypto sector to become a regulated gatekeeper to the legitimate economy, with the UK and other countries legislating to bring cryptoasset firms within regulation for anti-money laundering and counter-terrorist financing.

This paper aims to support financial institutions as they navigate this transitional period. While the anti-money laundering regime is meant to support a risk-based approach this can be difficult to apply to the cryptoasset sector, given the semi-anonymous nature of cryptoassets and the fast pace of change across technology, business models and regulation. While many cryptoasset firms are developing and applying innovative technological approaches to financial crime controls, there are also new types of cryptoassets, exchanges and tools being used to enhance anonymity and defeat KYC and fraud prevention techniques. By summarising the range of cyptoasset business activity, associated financial crime risk and good practice, this paper aims to help financial institutions inform their risk appetite and take a more considered approach to risk management.

This paper also considers how the financial and cryptoasset sectors could partner and work together on a more collaborative basis in order to drive a more effective approach to risk management and the protection of consumers. Bitcoin was originally described by its pseudonymous inventor, Satoshi Nakomoto, as "a new electronic cash system that's fully peer-to-peer, with no trusted third party", but today's cryptoasset sector includes many legitimate cryptoasset firms that have taken on the trusted gatekeeper role and are actively collaborating with law enforcement and regulators. This partnership approach can be developed further to support more effective financial crime risk management such as intelligence sharing, blockchain analytics to trace and risk assess cryptoasset transactions and distributed compliance opportunities such as blockchain-based KYC platforms.

It is in everyone's interests for crypto regulation to succeed on the basis that cryptoasset adoption is increasing exponentially, however, the financial crime and and consumer protection risks need to be managed and different parties have varied roles to play. The regulated private sector has a critical role in ensuring that legal compliance translates into effective risk management, but policy makers and regulators also need to apply a risk-based approach. Policy makers in the UK are tailoring financial crime regulation to the risks and business models of cryptoasset firms, seeking to strike the right balance between reducing the harms of illicit finance and supporting innovation that benefits consumers and the economy. Regulation and clarity on expectations is only the first step and needs to be supplemented with an effective licensing process and effective supervision.

Given the rise in cryptoasset fraud, investment scams and consumer protection concerns, it is important that regulators help financial institutions to take workable and proportionate steps to protect customers, including issuing guidance on how to manage exposure to unregulated exchanges and unregulated products and services. It is clear that cryptoassets and the underlying technology offer a range of compelling use cases for financial and payment systems, that will enable further transformation of the financial services industry and other sectors, provided that the risks can be managed effectively. Efforts to enhance mutual understanding, support collaboration and deliver an effective regulatory framework with the required clarity will help the UK realise the potential of this new sector for consumers and for economic growth. We hope this paper contributes to these efforts and provides a useful perspective for both financial institutions and cryptoasset firms.

BOB WIGLEY
Chairman
UK Finance

ALAN PATERSON
Founder and Managing Director
Plenitude

INTRODUCTION

Today, the rapid adoption of blockchain technologies, and the cryptoassets they support, are on their way to revolutionising global financial and payment systems in terms of clearing, settlements, trade finance and de-centralised finance. As the numbers of cryptoasset-related ventures multiply and we see the exponential growth in the number of institutions and individual investors holding cryptoassets, how should financial institutions respond?

Simply saying "we don't bank crypto" is an increasingly hard line to toe given the significant opportunities the underlying technology creates, notwithstanding regulators have made cryptoasset risk a priority and most institutions have some degree of crypto exposure – whether they know it or not[1]. In short, confronting financial crime through cryptoassets is now an essential part of safeguarding the financial system from criminals, adopting a truly risk-based approach and enabling a nascent and fast-growing industry to flourish.

This paper seeks to provide a balanced view and to understand (and demystify) regulated cryptoasset business models from crypto ATMs to exchanges, P2P sites and ICO issuance – how they are exploited by bad actors, and what risks they pose to banks and the traditional financial sector. It will address the full spectrum of financial crime risks (AML, CTF, sanctions, fraud etc) and identify techniques and best practice for banks and other financial institutions to assist managing cryptoasset risks (e.g. darknet purchases, privacy coins and ransomware), be it indirect risk from customer transactions or direct risk from banking cryptoasset clients. It will also assess how financial institutions can adapt and adjust their risk appetite to the sector where total volume and value of transactions exceed illicit activity by many orders of magnitude[2].

The paper will seek to answer the following questions:

1. What do we know about the true calibration between threat, vulnerability and risk posed by cryptoasset providers to wider financial institutions?
2. What are the principal ML/TF compliance challenges posed by cryptoasset providers and how can the industry effectively mitigate these relative to risk exposure (with reference to known typologies)?
3. Why should both sectors work together for the benefit of the UK?
4. How can both sectors move towards a mutually agreeable balance of risk and acceptable controls? And what role does the regulator have to play?
5. What action is required to encourage wider and safer adoption of cryptoassets with both retail and institutional investors in light of the known financial crime risks?

It is increasingly clear that the blockchain ledger on which Bitcoin transactions are recorded is an underutilised forensic tool that is beginning to be used more widely by law enforcement and the intelligence community to identify and disrupt illicit activities. This opens up compliance opportunities for financial services firms and cryptoasset providers to deploy investigative and forensic capabilities (including techniques to trace transactions on the blockchain) and red flags for recognising and reporting potentially suspicious transactions. This offers a realistic possibility of a new paradigm in the association between traditional finance and cryptoasset providers.

The pace of change regarding regulatory and supervisory developments in the cryptoasset sector (through legislative change, a fast developing regulatory framework, and newly drafted guidance) offers insights for both financial institutions and cryptoasset firms in setting their financial crime control frameworks. By assisting firms to implement strategic changes to ensure effective financial crime risk management and meet the expectations of regulators, there is hope that a pathway for closer relations, regulatory parity and effective risk management is on the horizon.

1 **https://cointelegraph.com/news/banks-failing-to-identify-up-to-90-of-suspicious-crypto-transactions**
2 According to a recent study by blockchain analytics firm Chainalysis, illicit activity among all cryptoassets as a percentage of total cryptoassets activity from 2017 to 2020 was less than one percent.

CHAPTER 1: TECHNOLOGY AND BUSINESS MODELS

1.1 TECHNOLOGY

The following chapter outlines the technology and business models which exist within the cryptoasset sphere, outlining the ways and means that they are applicable to the anti-money laundering (AML) / counter-terrorist financing (CTF) environment.

1.1.1 Distributed ledger technology

A distributed ledger, sometimes called a shared ledger, or distributed ledger technology (DLT), is a synchronised set of digital data, with capabilities and benefits which go far beyond traditional centralised or paper-based ledgers. The distributed ledger database is spread across several devices on a peer-to-peer network, where each device replicates and stores an independent and identical copy of the ledger, without any central administrator. When an update occurs on the ledger, consensus is determined by consensus algorithms, and all devices update themselves with the new, validated copy of the ledger.

Distributed ledger technology can be spread across multiple sites, countries, or institutions, and offers a viable structural alternative to centralised ledgers held by corporations, businesses, and governments. The data stored in distributed ledgers is accessible and highly reliable due to their decentralised and immutable nature; and DLT could therefore prove to be a valuable forensic resource to allow financial institutions, law enforcement, and the intelligence community greater insight into cryptoasset transactions to assist them with the identification and disruption of illicit and criminal activities.

1.1.2 Blockchain

A blockchain, which is a form of DLT, is an ever-growing chain (or list) of records called blocks. Each block contains information regarding the block before it in the chain. As additional blocks are added to the chain, they reinforce the information in the blocks before it. Blockchains are secure by design: the blocks are linked together using cryptography, and the data in any given block cannot be altered without also altering all subsequent blocks in the chain. As a result, blockchains are highly resistant to both malicious and accidental manipulation.

The blockchain was invented to serve as the public distributed transaction ledger of the cryptoasset Bitcoin and has inspired other applications and blockchains widely used by cryptoassets.

Global efforts to combat money laundering and financial terrorism are incredibly expensive for both governments and financial institutions and, considering the hefty regulatory penalties levied on the financial services sector for failing to comply with know your customer (KYC) regulations in recent years, the sector is turning to blockchain-based solutions to help ensure compliance.

Given that blockchains are decentralised, if adopted in the financial sector for KYC purposes they would allow financial institutions to accumulate data from multiple authoritative service providers into one single validated, cryptographically secure, and immutable database. Due to the reliability of such databases, there is an argument that governments and financial institutions should be allowed to rely completely on the data, thereby removing the need for any further routine ID checks and retaining a vital evidentiary trail.

The concept of a blockchain-based KYC platform is being developed by large organisations such as IBM, which has completed a successful proof-of-concept of its “Shared Corporate Know-Your-Customer” project in conjunction with Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, and Cargill.

KYC verification using blockchain ultimately supports financial institutions with the administrative KYC processes required by regulation. It has the potential to be far more efficient than traditional methods of verification, including at a greatly reduced cost.

1.1.3 Decentralised finance (DeFi)

Decentralised finance (commonly referred to as DeFi) is a blockchain-based form of more traditional financial products, which operates peer-to-peer without any intermediary. It operates using smart contracts on blockchains, typically the Ethereum blockchain. DeFi platforms allow users to trade cryptoassets, use derivatives to speculate on price movements on a wide variety of different assets, generate interest in savings-like accounts, lend to or borrow from others, and in some cases even insure against various types of risk exposure. In theory, any existing centralised financial service could be transferred to a similar DeFi service, without needing to rely on the traditional gatekeepers of such services.

Rather than transactions being made with or through a centralised financial intermediary (such as a brokerage, exchange, or bank), decentralised transactions are made directly between DeFi participants using decentralised applications (commonly referred to as DApps) and mediated by smart contract programs. Many DApps can interconnect and work together to create complex financial services.

DeFi protocols are accessible and can be used by anyone, which creates something of a conflict: on one hand, customers in countries with limited access to centralised financial services would be able to start using DeFi services; on the other hand, this also allows for malicious actors to leverage DeFi for criminal activities. Financial institutions need to consider both sides of this coin, while controls should be in place to ensure that requirements for financial crime compliance are met.

The Financial Action Task Force published its updated guidance covering DeFi in July 2021, applying standard AML and KYC requirements to DeFi[3]. This was the first significant effort to regulate the DeFi industry, and further regulatory guidance on the topic is sparse. One area that needs further clarity is where liability lies if a DeFi protocol fails to work as designed.

DeFi is likely to become more widely adopted by financial institutions if regulatory bodies publish positive DeFi legislation and regulation. Further, anti-money laundering activity in the DeFi space could be enhanced by financial institutions performing KYC activities for newly onboarded customers, allowing a DeFi service to comply with AML regulation and wider financial crime compliance.

As DeFi is relatively nascent technology, further research is needed to assess the viability of cooperation between centralised financial institutions and DeFi services, but it is likely that such cooperation will bring benefits not only to centralised financial institutions, but also to DeFi and its customers.

1.1.4 Stablecoins

As the cryptoassets market has grown, there has been increasing interest in less volatile digital currencies. So-called "stablecoins", such as Tether or USD Coin, attempt to provide price stability via collateralisation (i.e., by tracking the value of assets, including fiat currencies like the U.S. dollar, exchange-traded commodities such as precious metals or industrial metals, or other less volatile cryptoassets) or through algorithmic mechanisms of buying and/or selling the asset (or derivatives of the asset) to which the stablecoin is pegged.

Stablecoins have evolved into a significant part of the crypto ecosystem in recent years, as they attempt to offer the best of both worlds: the lower levels of price volatility seen in traditionally stable assets such as fiat currencies, and the rapid processing and enhanced security and privacy offered by cryptoassets.

3 **https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf**

According to cryptoasset data provider CoinGecko[4], at the time of writing, Tether, the largest stablecoin by market capitalisation, has a 24-hour volume of £44 billion versus Bitcoin's £27 billion, and its market capitalisation has increased to £45 billion from £8 billion one year ago. The usage of stablecoins is expected to continue growing, and many different companies are exploring the viability of stablecoins for global payments and remittances.

Even though stablecoins have become an important part of the blockchain ecosystem, they did not garner much regulatory attention until Facebook's announcement of its Libra project in June 2019. Almost immediately, many financial authorities around the world issued cautionary statements on Libra, citing the potential risks of disruption to the global financial system. Since then, stablecoins have been subject to increasing scrutiny and questions about their regulation, supervision, and oversight. Financial authorities have come to realise that stablecoins warrant enhanced scrutiny, particularly due to their cross-border reach and potential scale[i].

To mitigate the risk of stablecoins creating new opportunities for financial crime, particularly given the possibility of peer-to-peer transactions, all entities that are part of a stablecoin ecosystem should comply with global standards. This includes the providers of stablecoins themselves, and should cover financial crime compliance across anti-money laundering, data protection, market integrity and combating the financing of terrorism.

Future regulation will need to focus on who is permissioned to issue global stablecoins and gain access to the payment systems of central banks, and this is likely to have material implications; not only for stablecoins, but also for digital tokens as a whole.

1.2 BUSINESS MODELS

1.2.1 Cryptoasset developers and issuers

Due to the interchangeability of both terms attributed to various participants in the ecosystem (which includes developers, designers, entities who issue cryptoassets, and other intermediaries) the EU Regulations (Prospectus Regulation) narrows their characteristics to the legal issuer of the securities. Although issuers do not necessarily need permission to issue tokens, they may still need to comply with certain requirements, e.g. prospectus and transparency requirements, or AML/KYC. Cryptoasset exchanges can also act as issuers[5].

1.2.2 Miners or transaction processers

In the world of cryptoassets, mining refers to the act of extracting new tokens and introducing those tokens onto their respective DLTs (or, in other words, their blockchains)[6]. The process involves sophisticated computers tasked to solve complex computational mathematical problems, although the degree of complexity is dependent on the specifications of the cryptoasset in question. Some tokens may only require an internet browser to mine, whereas others (i.e., Bitcoin) may require a considerable amount of processing power and energy to mine. In any case, the integrity of the mining process is ensured by the Proof of Work it produces; the mechanism that sets out the rules and difficulty required to extract valid tokens[7].

The mining process does come with its negative externalities, however. At present mining is a source for environmental concerns as some preliminary research shows the energy consumption to mine certain cryptoassets is nearing single digits of global consumption, however, there has been no official research to create a direct link with carbon footprint emissions. The role of the miner could also extend to transaction validation. Considering a transaction request is essentially a change to the state of the network, the transaction needs to be validated, partially using the computational processes used in the mining process to authenticate the transaction[8].

4 **https://www.coingecko.com/en**
5 PS19/22: Guidance on Cryptoassets
6 **https://cbeci.org/mining_map**
7 Proof-of-work (Pow) | ethereum.org
8 Proof-of-work (PoW) | ethereum.org

1.2.3 Trading platforms and exchanges

A cryptoasset exchange provider/trading platform is a business or sole practitioner whose main activity involves (but is not necessarily limited to) offering cryptoassets as an issuer or creator. Its activities involve exchanging (or making arrangements with a view to exchanging) cryptoassets for money or money for cryptoassets, or simply the exchange of a cryptoasset for another cryptoasset[9].

These definitions come with a caveat, however, as cryptoasset platforms are continuously growing their product offering, some may act as liquidity providers, wallet providers, or financial intermediaries through their peer-to-peer feature, and/or offer a variety of other cryptoasset financial instruments. As of January 2021, exchanges are all required to not only comply with anti-money laundering/terrorist financing regulations, but also to register with the FCA.

1.2.4 Investors

Considering the infancy of cryptoasset adoption in terms of its use for its intended purposes, it can be said that any entity purchasing cryptoassets is an investor. This would include institutional investors, financial institutions, regular businesses, and retail investors.

1.2.5 Wallet providers and custody service providers

Wallet providers are defined as "a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer cryptoassets on behalf of its customers, or private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets, when providing such services"[10].

To expand on this definition, it is important to highlight that wallets, in contrast to traditional monetary accounts, do not themselves store the value of cryptoassets. Instead, they store public cryptographic keys and their corresponding private keys. As all cryptoassets are intrinsically stored and visible on their respective blockchain, they cannot be stored anywhere outside of their network. Wallets vary in functionality; some may offer to store one single cryptoasset, while others store a multitude of different currency which may not necessarily operate on the same blockchain. In essence, the key characteristics of wallets are their ability to allow users to store their private keys associated with a blockchain ledger, as well as providing an interface by which users can store, send, receive, and monitor balances, and by design have security protocols in place to protect users' funds.

Custodial services expand the functionality offered by wallets, enabling larger financial institutions or high-net worth individuals to delegate the management and storage of their digital assets to a third party with more technical expertise in securing assets and administering them[11].

1.2.6 Financial intermediaries

Cryptoasset intermediaries include any party that facilitates the purchase of a cryptoasset, such as agents dealing in investments as a principal, arranging deals in investments, making arrangements with a view to making investments, sending dematerialised instructions, brokers, and to a certain extent exchange platforms acting as intermediaries through their peer-to-peer trading features.

1.2.7 Liquidity providers

Liquidity, being the ease of being able to convert one asset into another without affecting its price, or it being subject to a long chain of transactions; a liquidity provider in the context of cryptoassets refers to decentralised exchange users who fund liquidity pools with their own holdings to ease the liquidity between illiquid trading cryptoasset pairs and, by doing so, receive compensation. In other words, it is the creation of a market upon which traders can exchange assets which would not otherwise have a direct trading relationship on an exchange provider[12].

9 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
10 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
11 The Money Laundering and Terrorist Financing (Amendment) Regulations 2019
12 Liquidity provider/CoinMarketCap.com

1.2.8 Payment and merchant service providers

The FCA considers payment and merchant service providers to be entities that offer as a service the ability for consumers to transact with merchants using cryptoassets. Considering the monetary nature of these transactions which at the starting point involves the transfer of fiat currency via a cryptoasset, these entities fall within the scope of ML/TF regulations, Payment Services Regulations, Electronic Money Regulations as well as other Regulated Activities Order[13].

13 PS19/22: Guidance on Cryptoassets


20 EURO
50 EURO
100 EURO
200

CHAPTER 2: MONEY LAUNDERING AND TERRORIST FINANCING

Cryptoassets' reputation as a medium of exchange and a platform for decentralised financial activity has suffered by association with illicit activity since its creation. The perception of Bitcoin as a complicit platform for criminal exchange of value[ii] has tarnished the wider cryptoasset landscape as did its perceived role as the darknet currency of choice[iii]. This remains the perception of many despite evidence to indicate that, considered in proportion to the increasing size of the cryptoasset market, this is increasingly less of an issue and the fact that cryptoassets provide a traceable ledger of actively providing transparency on all transactions.

As an area of continuing growth and expansion, cryptoassets would always carry commensurate regulatory concern. However, there are additional AML/CTF risk factors to bear in mind, with blockchain analysis company Chainalysis stating that: "*...cryptocurrency's decentralized, semi-anonymous nature makes it a uniquely appealing option for criminals, and their embrace of the technology has helped shape its overall reputation*"[14]. Furthermore, the Covid-19 pandemic has undoubtedly accelerated the take up of this challenger technology, but at what potential cost?

As with all financial products there are opportunities for malicious actors to utilise cryptoasset based technology for the purposes of financial crime, be that for the movement and conversion (placement and layering) of the proceeds of acquisitive crime; or potentially for the purposes of terrorist financing; as well as increasing opportunities for cryptoasset scams e.g., ICO scams or fraud (frauds were by far the highest-earning category of crypto crime in 2019[15]). However, the same analysis highlights that:

"*Despite this picture of risk, it is worth noting that the crypto-asset industry is experiencing tremendous success in combating illicit activity. While the total volume of illicit activity in crypto assets has grown in absolute terms; illicit activity today still accounts for less than 1% of all transactions. A dramatic reduction from 2012, when 35% of crypto-asset transactions were illicit*[16]."

In addition, "*...the upside is that unlike cash and other traditional forms of value transfer, cryptoassets are inherently transparent. Every transaction is recorded in a publicly visible ledger*"[17].

With the right tools, it is possible to see how much of all cryptoasset activity is associated with criminality, home in on high harm types of crime and share insights with law enforcement and the industry to curb its impact and stop bad actors from abusing the system. For example, a 2020 BAE systems report, commissioned by SWIFT, noted that "*identified cases of laundering through cryptocurrencies remain relatively small compared to the volumes of cash laundered through traditional methods*"[18]. So what do we know about this relatively small volume of cases where cryptoassets are used for money laundering?

Specific enablers of financial crime fall into several categories including the use of privacy coins, mixing services/tumblers and P2P (Peer to Peer) activity. In much the same way as the utilisation of traditional banking, disguising the origin, ownership and control of assets are key requirements for successful money laundering.

Cryptoasset activity, where quasi-anonymous and unregulated, can provide a 21st century means of money laundering and terrorist financing. Money launderers will therefore focus attention on jurisdictions imposing poor regulatory oversight of cryptoasset exchanges, where limited or zero KYC controls are implemented. It is therefore a given that anonymity is a key driver for criminals wishing to utilise cryptoassets and exchanges to launder the proceeds of their illicit activity.

14 **https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report**
15 Ibid.
16 Ibid.
17 Ibid.
18 Understanding the money laundering techniques that support large-scale cyber-heists, Follow the money, baesystems.com/SWIFT, 2020.

Privacy coins offer elevated levels of anonymity and obfuscation, enhancing money laundering capability using obfuscated public ledgers, unlike Bitcoin which uses fully transparent public ledgers. According to Elliptic:

"*The use of privacy coins for laundering purposes is also heightened where the exchanges that criminals attempt to exploit are unlicensed and non-compliant. The FATF's report on crypto-asset red flags draws special attention to unlicensed and non-compliant exchanges that offer privacy coins as an area of specific and significant risk.*"[19]

However, it is noteworthy to observe the different appeal to criminals between certain crypto tokens. Monero, for instance, is referenced in numerous reports as being almost wholly used by illicit actors[20] while other coins are increasingly less attractive to criminals given forensic tools and traceability capability deployed by law enforcement agencies and private sector investigators.

It should also be noted that it is in the purview of individual exchanges to decide whether to list a privacy coin,[iv] since listing such a coin may affect the ability to obtain regulatory licenses in established markets and with banking partners. Some privacy coins have optional privacy features which may make them more palatable to exchanges (e.g. ZEC unshielded transactions), while exchanges can take a considered decision not to list higher-risk coins. A registered exchange with a fully implemented KYC regime also removes some of the privacy features provided by such coins.

Mixing services/tumblers adds further obfuscation capability, providing the ability to create opacity around the source and origin of crypto asset funds. Such mixing services can be used to introduce illicit proceeds or stolen Bitcoin (placement) with the intention of mixing via tumblers creating an elaborate audit trail. ATMs also provide additional access to crypto currencies and the ability to transfer cash into cryptoassets. An additional risk occurs where the ATMs are not regulated or located in higher-risk jurisdictions.

P2P exchange activity enables direct interaction between crypto users. Decentralised networks are used by criminals to send funds to another destination (often cross-border), where there are crypto exchanges with less stringent or non-existent AML regulations. These exchanges can then in turn convert cryptoassets into fiat money (integration). In addition, there are further money laundering risks for crypto which follow traditional banking scenarios, such as money muling and the churning of assets. These activities should both raise familiar red flags despite being cryptoasset related.

However, it should be noted that despite an inevitable percentage of trades passing through legitimate exchanges being criminal in nature, this is no different to banks and traditional finance activity, with considerably less flow and volume. Furthermore, crypto exchanges in the UK are expected to apply the same amount of regulatory rigour around ML/TF controls and frameworks as traditional finance and banking institutions.

There are very few recorded incidents of terrorist financing (CTF) utilising cryptoassets than money laundering and attempted sanctions violations; however, as with conventional banking, CTF activity via crypto is difficult to detect and interdict.

"*It is possible that in 2020 and beyond, more terrorist organizations will embrace cryptocurrency as a fundraising tool and push for further advancements that allow them to take in more funds and enhance their privacy. Terrorist groups have proven adept at leveraging emerging technologies to advance their agenda, with groups like ISIS' mastery of social media being a prime example*[21]."

However, on 12 July *The Jerusalem Post* reported a story headed "Israeli Authorities Seize cryptocurrency transfer from Hamas"[22]. The article set out that: "*Once you go beyond the boundaries of the blockchain to the worlds of exchange platforms, you immediately lose anonymity and then, as in the present case, states and law enforcement agencies are able to locate and freeze the currencies used by criminal and terrorist organizations.*"

19 Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders, Elliptic, 2020.
20 **https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6**
21 **https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019**
22 **https://www.jpost.com/israel-news/israeli-authorities-seize-cryptocurrency-transfer-from-hamas-673564**

In summary then, whilst there are undoubtedly a variety of means for cryptoassets to be manipulated for nefarious purposes, regulatory scrutiny, cryptoasset businesses and law enforcement cooperation is key to disrupting the use of crypto-technology for criminal means.

CHAPTER 3: SANCTIONS EVASION

Widely used cryptoassets such as, but not limited to Bitcoin, Ethereum and Monero etc, are an attractive alternative to normal monetary currencies as they exist outside the realm of the traditional financial system and are therefore perceived as not necessarily being under the watchful eyes of regulators, law enforcement or multilateral institutions.

Evidence suggests that sanctioned actors and entities in jurisdictions worldwide are testing new ways of using cryptoassets to evade restrictions and continue their illicit activities. National Competent Authorities are seeing a rise in the use of cryptoassets by countries including Venezuela, Iran, and the North Korea as a way of potentially circumventing sanctions. However sanctioned actors cannot do this alone, they rely on the cooperation of other high-risk non-sanctioned jurisdictions to facilitate their activity.

Despite that, in the same way as traditional finance, the potential use of cryptoassets to evade sanctions can be detected by multiple red flags. Some of the most common identified red flags are when crypto-exchange customers use IP addresses, emails, telephone numbers and other potential identifiers that are registered or linked to sanctioned jurisdictions. The transactions themselves have no common purpose, however these actors are frequently sending and receiving funds to and from decentralised exchanges (DEXes) that do not require KYC information from the end-user and are often located in high risk and non-cooperative jurisdictions.

How do sanction evaders use cryptoassets to elude the restrictions imposed on them? Here are the top five methods:

- **Privacy coins:** As noted above, these are a class of cryptoasset that power private and anonymous blockchain transactions by obscuring their origin and destination. Some techniques used include hiding a user's real wallet balance and address and mixing multiple transactions with each other to elude transaction monitoring. Privacy coins such as Monero (XMR), Dash (DASH) and Zcash are favoured by criminals and users of the darknet to evade detection.
- **Coin swap services:** Sanction evaders are moving from using large fiat-to-crypto exchange platforms and leaning towards coin-swap services to launder their funds. Some coin-swap services are often located in high-risk jurisdictions and do not require KYC information from their end-users, allowing sanctions evaders to swap stolen crypto tokens for clean tokens without fear of detection. North Korea's Lazarus Group used coin-swap services and DEXes to launder $280 million worth of stolen cryptoassets from Singapore's crypto exchange KuCoin[23].
- **Privacy wallets**: Privacy wallets have come under law enforcement scrutiny due to a number of investigations involving 'Wasabi Wallet' users. Reporting identified that the majority of Wasabi Wallet transactions allegedly ended at darknet marketplaces. Privacy wallets like Wasabi Wallet use a technique called coin-mixing, which combines transactions from multiple users into one larger transaction making it difficult to trace the illicit transactions[24].
- **Decentralised exchanges (DEXes) and finance (DeFi):** are peer to peer platforms that connect crypto buyers with sellers. They do not take custody of users' funds and can run autonomously without human intervention. DEXes and DeFi that are set up in high-risk jurisdictions often don't require KYC information from end-users. Because of their non-custody function, DEXes and DeFi are not currently regarded as a Virtual Asset Service Provider (VASP), which are subject to FATF based AML/CTF regulations. However, that is likely to change under new FATF Guidance on virtual assets and virtual asset service providers[25], which is likely to bring DEXes and DeFi under the definition of VASPs, making them subject to AML/CTF regulations.
- **Engaging in crypto-jacking[26]:** Is the dark side of crypto-mining where sanctioned countries hack both private and business computers to install software that enables them to use those power sources and resources to mine cryptoassets to raise illicit funds or to steal cryptoasset wallets owned by unsuspecting victims.

23 **https://www.reuters.com/article/us-northkorea-sanctions-cyber-idUSKBN2AA00Q**
24 Europol Cybercrime Centre report: Wasabi Wallet, 2020.
25 Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers.
26 Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield, Elliptic, May 2021.

In addition to these methods, sanctioned countries are going further to circumvent their restrictive measures by developing their own cryptoassets. In 2019, media reporting claimed that North Korea, Russia, Venezuela and Iran were investing resources in developing their own cryptoassets to evade western sanctions[27]. Since this report was issued, Venezuela has become the first country to create the first national cryptoasset called the 'Petro'. The token was pegged to the value of Venezuela's oil and mineral reserves. The US Treasury's Office of Foreign Assets Control (OFAC) took decisive action by simply considering the Petro as an arm of the sanctioned *Petroleos de Venezuela*, the state-owned oil company, and thus an extension of the Venezuelan government, quickly capturing the *Petro* under US sanctions legislation.

The Iranian PayMon dubbed the Crypto Rial is a cryptoasset backed by gold and will be issued jointly by four Iranian banks: Milli, Millet, Parsian, and Pasardjad. In a classic Mexican stand-off with the US, the Iranian government has openly admitted that one of the purposes of the Crypto Rial is to circumvent US sanctions. At the 'Chain Point 18' conference on 14 November 2018, Iran signed a trilateral blockchain cooperation agreement with Russia and Armenia[28].

Russian president Vladimir Putin later said that Russia is 'actively working' with partners to establish a financial system that is entirely independent of SWIFT. This alliance is rumoured to include Iran, China, Russia, Venezuela and Turkey and would allow Iran to access the international markets using the Crypto Rial with its partners. However, it remains notable that sanctions lists are public and the downside to this is that those on the list will not try to transact with their real name. Those that continue trying to evade will also use VPNs and mask their IP address.

Cryptoasset businesses and financial institutions must prepare for a tightening sanctions compliance environment. Preparedness is key, and compliance officers must take a proactive approach. The evolving nature of the techniques set out above require that compliance teams know what red flags to look out for, as well as having the capabilities to detect and block them. To do so compliance teams need to adopt the following approach and solutions[29]:

- Deploying effective blockchain monitoring solutions to prevent interactions with prohibited addresses;
- Managing your country risk exposure in order to identify signs of sanctions risks;
- Understand red flags and typologies which may instigate EDD and reporting of suspicious activity that may carry sanctions risks;
- Defining your investigative strategy: Where risks have been identified, are you equipped to investigate potential sanctions breaches and report them to the appropriate authorities?
- Embedding a comprehensive threat and risk assessment to measure overall levels of risk exposure, in order to design the processes and procedures necessary to mitigate that risk.

By fully utilising and taking advantage of the inherently searchable and transparent nature of the blockchain as part of day-to-day financial and trading activities, the technology underpinning cryptoassets becomes an investigatory tool providing investigators and frontline staff with a unique view of how to monitor and mitigate potentially illicit activity – above and beyond that of some forms of banking activity[v]. As regulatory and enforcement activity evolve to take account of a digital financial system exemplified by cryptoassets, there appears to be an opportunity to restrict and limit the opportunities for sanctions evaders to abuse a new and evolving technology.

27 Association of Certified Sanctions Specialist: Sanctioned Nations Investigate Launching Cryptocurrency to evade sanctions.
28 **https://www.aljazeera.com/economy/2019/1/27/iran-inches-closer-to-unveiling-state-backed-cryptocurrency**
29 For more information on how to manage sanctions risk as part of an overall financial crime compliance and risk management strategy see a host of material available from cryptoasset forensic providers such as Elliptic, Hainanese or DarkTrace.


mirror_mod.use_x
mirror_mod.use_y
mirror_mod.use_z
elif operation == "MIRR
mirror_mod.use_x
mirror_mod.use_y
mirror_mod.use_z
mirror_ob.select = 1
print("please select
OPERATOR CLASSE
Mirror Tool

CHAPTER 4: FRAUD AND CYBER CRIME

As the value of cryptoassets spirals ever higher, so have the scams related to them. According to new data from the UK's fraud reporting service Action Fraud, scams involving cryptocurrency investment rose 57 per cent across the UK in 2020, with a total of 5,581 reports made.

Investors lost a total of £113 million to crypto scammers in 2020, up from £76.6 million the previous year. Action Fraud regularly warns people to be wary of unsolicited Bitcoin investment opportunities or "money flipping" services across social media and email. As cryptoassets rise sharply in value, many other UK bodies are also urging caution.

It is a similar story in the US where the Federal Trade Commission[30] reported scammers are cashing in on the buzz around cryptoassets and luring people into bogus investment opportunities in record numbers. Since October 2020, reports have skyrocketed, with nearly 7,000 people reporting losses of more than $80 million on these scams. Compared to the same period a year earlier, that's about twelve times the number of reports and nearly 1,000 per cent more in reported losses.

The reality is that these reported numbers reflect the tip of an iceberg – many investors do not always report that they have been scammed, on the basis they are seen (by some) as part and parcel of the crypto industry and are investing small sums knowing that for newly issued tokens there is a significant risk of their value going to zero or promoters/ developers running away with the funds which is known as a "Rug Pull'. Most individual scams are so small that the authorities do not investigate or respond. Regulators around the world tend to prioritise cases involving significant sums, or violations that seem particularly egregious. Cases involving less than $100,000 tend to get a pass, and buyers have little incentive to chase after fraudsters on their own.

Chainanalysis[31] has estimated that this year alone over $2.6 billion has been grabbed. That figure doesn't include an alleged Ponzi scheme that came to light in South Africa in June this year. Local authorities put the haul at $3.6 billion worth of Bitcoin. These numbers in fact represent a marked decline from 2019, when fraudsters walked away with an estimated $9 billion. With a few outsize exceptions, most crypto scams seem to be getting smaller, however the number of people being scammed is increasing. From 2019 to 2020, the number of victims jumped 48 per cent to an estimated 7.3 million. Between the last three months of 2020 and the first three months of 2021, the number of unique scams rose nearly 18 per cent, to 1,335, according to Chainalysis.

On 10 August, it was reported that hackers pulled off the biggest ever cryptoasset heist, stealing more than $600 million in digital coins from token-swapping platform Poly Network, only for a 'white hat'[vi] to return nearly all the assets less than 48 hours later. Poly Network is a decentralised finance (DeFi) platform that facilitates peer-to-peer transactions with a focus on allowing users to transfer or swap tokens across different blockchains. This incident highlights the vulnerabilities with regards to DeFi networks and the wider issue around cyber-related crime in the crypto space.

Why has cryptoasset fraud become such a problem? Since their inception, the value of cryptoassets has proved to be extremely volatile, meaning investors can realise significant gains or losses. Like any relatively new asset class with the potential for very high returns, there is always a risk fraudsters will try to take advantage of it. When returns on savings in normal bank accounts are poor, depositors will also look for other places to invest their funds. Cryptoassets have regularly been in the news as offering huge returns, and companies offering cryptoasset services are well advertised. This attracts lots of novice investors, who tend to be more susceptible to fraud than professional investors.

The methods and tactics adopted by fraudsters cover a broad range of activities, some of which are covered in Chapter 5. However, historically the issuance of Initial Coin Offerings (ICOs) has realised the most significant fraudulent gains. New tokens can also be created and issued on blockchain networks such as Ethereum (ERC20) and Binance Smart Chain (BEP20), and anyone can create and launch a new token with the required technical skills. Other tactics include

30 **https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses**
31 **https://www.bloomberg.com/news/features/2021-07-08/crypto-scams-rug-pulls-bitcoin-hacks-billions-lost-when-shit-coins-go-to-zero**

investors being lured to websites that look like opportunities for investing in or mining cryptoassets that promise to immediately multiply the cryptoasset sent, but are in fact bogus or "giveaway" scams supposedly sponsored by celebrities or other known figures in the cryptoasset space.

In light of the potential exposure to fraud and concerns around consumer protection, UK banks are blocking payments to some cryptoasset trading platforms to protect customers following the dramatic spike in investment scam losses[32]. Mostly, though, authorities around the world are struggling to keep pace. A decade after Bitcoin was created, regulators are still grappling with how to police cryptoassets when the whole point is that they operate without governments or central banks. As more institutions and ordinary investors dip their toes into crypto new scams are bound to emerge.

Arguably fraud is the most significant financial crime risk that needs to be addressed and the level of fraud seen in crypto undermines the credibility of the industry as a whole. Better safeguards are required for investors, including the need for more robust ICO market regulations from governments and regulatory agencies to protect investors from severe losses. Big tech companies also have a role to play in terms of removing illegal and fraudulent content online, however efforts have been limited. Currently online fraud does not feature in the Online Safety Bill, but including it would likely incentivise tech companies to rapidly remove illegal content on the basis they might be subject to fines.

32 **https://cryptouk.io/safeguarding-against-scams/**

CHAPTER 5: BUSINESS ACTIVITIES FALLING WITHIN SCOPE OF MLRS

5.1 CUSTODIAN WALLETS

A custodial wallet provides a simple way for users to store private keys to access their crypto assets and also allows the user to send, receive or purchase cryptoassets from wallet to wallet, using unique access to the blockchain and the miners who validate all such transactions. A service provider will provide a wallet to safeguard your asset, rather like a bank has details on your account. These can be on a desktop or in a mobile application – individuals can make transfers and the provider safeguards and administers the customer's assets.

In 2019, a fake cryptoasset wallet application that imitated a company called 'Trezor' was found on the google Play Store. While the app looked genuine, it was quickly found out to be an app used to 'phish' for legitimate users account login details and to trick users into transferring cryptoassets to fraudsters.

Criminals frequently target vulnerable people to become money mules in the banking world, something which is becoming increasingly prevalent with cryptoassets. Crypto money mules are commonly being asked to purchase cryptoassets (occasionally from Crypto ATMs) and are then instructed to transfer cryptoassets to one or multiple wallets. With with the lack of KYC and evidence of source of funds, this is becoming a popular route for criminals.

5.2 CRYPTO ATMS

At their simplest level a customer feeds fiat currency (notes) into an ATM and selects the token they wish to purchase e.g. Bitcoin or Ethereum (depending on the machine provider) before entering a code that is either used to connect to the user's desired wallet, or will print a paper key (QR code) which they can redeem later. While cryptoasset ATMs have been around for some time, they have become increasingly popular due to the volatility of Bitcoin increasing to an all-time in 2021. This has led some companies to install crypto ATMs to meet increasing demand and realise the associated profit.

Many ATMs have no KYC checks in place – no passport, thumb print or awkward questions, simply money in, crypto out or vice versa. Without linking the transaction to an identity, many small sums of money (a process called smurfing) can enter the system and be transferred and cashed out worldwide – in effect enabling the 'placement' stage of the proceeds of crime. It has been alleged that ATMs have become a popular means to move illicit funds for drug gangs. Police are known to be concerned that enterprising ATM operators even have separate 'self-load' machines purely intended for organised crime gangs. This might tally with the, some might say, strange location of many crypto ATMs, such as nail bars, off licences and newsagents.

The 'layering' stage of the money laundering process is formed of an obfuscation of transactions, some of which occur on the blockchain through the multiple splits in the transactions, the use of money mules and the involvement of other money service businesses. Criminals can then benefit from the process by using the cash – by cashing out their tokens buying goods and services – or through 'integration' through the banking or other payment service providers. Although regulation is likely to reduce the vulnerability through more rigorous KYC requirements and most machines have the capability to scan passports or fingerprints, these are not always enabled by operators or thresholds are set quite high (c.£500-1000).

Demand has increased from 6,759 to 15,000 ATMs worldwide in the past year and the growth in ATMs has provided more opportunities for money mules and criminals to take advantage of the lack of KYC involved in the process. As these ATMs provide an extra layer of privacy and collect limited information about their users, it becomes difficult to link a potential money mules activity to money laundering. One investigation conducted by the Australian Federal Police (AFP) found a money mule network that laundered more than $3.5 million in stolen funds obtained from cybercrime. The trail led the AFP to a 22-year-old man who had received $18,000 in stolen funds into his bank account which he transferred on and took a five percent commission fee. Shortly after, it was reported that the man withdrew the cash and deposited this cash into a Crypto ATM in exchange for bitcoin.

5.3 ISSUANCE OF COINS (ICO)

An ICO, which is also known as an initial token offering or token sale, is used as a way of raising capital from the public by the sale of a coin or token in exchange for a fiat currency or more popular cryptoassets e.g. Bitcoin, Litecoin or Ethereum. Typically, businesses will develop a digital token, such as their own proprietary cryptoasset, and look to sell these tokens to investors in a bid to raise capital in return for existing cryptoassets rather than fiat currency. The trade of these tokens is recorded on the blockchain. Investors can in most cases sell on these tokens for profit on peer-to-peer exchange platforms should the value of the tokens increase. They are sometimes further incentivised into buying the tokens by being given the opportunity to share in profits generated from the business ventures that benefit from their investment.

ICOs are currently the most regulated aspect of cryptocurrencies. In most countries, ICOs are either legal, regulated or subject to future regulations. So far, only China and South Korea have explicitly banned ICOs in their respective jurisdictions. ICOs have become an increasingly popular means for enterprises to raise capital, however many have been wholly fraudulent due to their anonymity and ability to raise a substantial amount of capital in a short time frame. The main risks associated with ICOs are:

- **They may operate in an unregulated space** – *If they operate in an unregulated space this doesn't provide investors with any protection with regards to their investment.*
- **Lack of exit options and extreme price volatility** – *Coins can typically be subjected to market manipulation or investors may not be able to find an exit route for their investment.*
- **Inadequate information** – *ICOs commonly use the term 'whitepaper' to provide investors with information. However, this can be unaudited and at times misleading.*
- **Fraud** – *this is due to the high volume of ICOs shutting down and running away with the collected funds or simply being exposed as scams.*
- **Flaws in the technology** – *lack of access to the investor's coins.*
- **Genuine ICOs may be at risk from phishing scams** – *for example a scammer may fraudulently impersonate an organisation that is conducting a token sale and persuade buyers to send cryptoassets to a wallet unaffiliated with the ICO.*

5.4 EXCHANGES

Cryptoasset exchanges provide essential liquidity to crypto markets, acting as vital gateways between the fiat and cryptoasset ecosystems. Thus, exchanges inevitably feature heavily in cryptoasset-related money laundering activity. Despite a shift from money laundering through regulated exchanges to non-regulated exchanges that do not require KYC information, supervisors and legitimate exchanges are aware that they are still subject to attempted ML given they are subject of 95 per cent of trading activity. According to Cipher Trace, top exchanges have historically laundered a significant amount of bitcoin, estimated at US$2.5 billion at today's prices. Once ill-intentioned users are registered with exchanges, this can open the doors for hacks, scams, and phishing. Financial crime risks and typologies related to crypto exchanges include:

- Criminals will target non-compliant or unlicensed exchanges which they know they can exploit with little or no obstruction when moving between fiat and cryptoassets, or from cryptoasset-to-cryptoasset. Non- compliant

and unlicensed exchanges present significant systemic risks on the basis they enable a wide range of illicit actors to engage in large scale money laundering. However, using regulated and compliant exchanges can also add a veneer of legitimacy to a criminal's otherwise illegitimate behaviour. Legitimate exchanges can have a 'mixing' effect for criminals.

- Accounts are opened by numerous individuals within a short period of time using shared addresses, mobile devices, IP addresses and other common identity indicators.
- Conducting cryptoasset to fiat currency or cryptoasset-to-cryptoasset exchange at a potential loss e.g. when the value of a cryptoasset is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical explanation.
- Multiple customers make high-value onward transfers to common accounts in high risk jurisdictions with no clear apparent purpose.
- The account holder may not have any understanding of what the funds in the account are being used for when questioned. In a case of stolen identity, they may not even be aware that an account was opened in their name.
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.

Crypto exchanges can be centralised or decentralised. Centralised exchanges (i.e. Coinbase, Binance) are more user-friendly and the intermediaries provide custody of funds to the users. They play a fundamental role in the ecosystem and almost all cryptoasset transactions pass by these centralised exchanges, as these allow fiat-crypto exchanges. On the other hand, trading in centralised exchanges involves higher trading costs and a loss in liquidity, as the global liquidity of the cryptoassets is reduced to a marketplace[33].

In decentralised exchanges (DEXs) the users hold their private keys and operate on the blockchain directly with other users, without the intermediation of institutions[34]. DEXs are more financially inclusive than centralised exchanges, as users normally are not required to provide their personal details to third parties to participate and there is no enforcement of economic sanctions measures against designated users or users from sanctioned territories[35].

5.5 FIAT-CRYPTO

Fiat-crypto exchanges allow the buy-sell of cryptoassets using fiat currency. The exchanges that operate as platforms for this type of transactions interface with the traditional financial system, accepting cash (crypto ATMs), digital wallet/bank transfers and cards (credit/debit/gift) as payment methods. Users are often required to follow a KYC process before opening an account, this can include identity verification, face verification, and two factors authentication. Some fiat-crypto exchanges, however, allow customers to operate crypto below a certain threshold without requiring KYC.[36]

5.6 CRYPTO-CRYPTO

In crypto-crypto exchanges, cryptoassets can be traded for other cryptoassets. These are centralised exchanges that charge a commission fee for custody and services provision to users. As in the fiat-crypto exchanges, these exchanges are counterparties of the trades. However, transactions in crypto-crypto exchanges pose less risk of money laundering than fiat-crypto, as layering might occur, but this is not a method for placement or integration to the traditional financial system.

33 **https://consensys.net/blog/news/decentralized-exchanges-overview-benefits-and-advantages-over-centralized-exchanges/**
34 **https://coinsutra.com/decentralized-exchange-cryptocurrency/**
35 **https://www.forbes.com/sites/theyec/2020/12/01/the-rise-of-decentralized-cryptocurrency-exchanges/?sh=3373ecfc16e7**
36 **https://cryptocurrencyfacts.com/the-difference-between-fiat-currency-and-cryptocurrency/**

5.7 PEER-TO-PEER (P2P)

P2P exchanges are marketplaces where individuals can trade in cryptoassets without the use of third parties to intermediate. When a seller agrees to sell, the cryptoasset is allocated to an escrow account, the buyer can then access the asset upon payment in the agreed format. There is no set requirement for a user's ID verification and authentication, as payment processing is not conducted by the exchange. The trades occur dismissing a banking relationship, the P2P exchanges are facilitators of the transactions, not counterparties of each trade. Payment forms are flexible and at the discretion of the user. In addition to the inherent privacy of these one-to-one transactions, the exposure to money laundering risk increases with the use of payment methods that allow anonymity. The use of crypto ATMs ensures that transactions remain private. Digital gift cards as a payment method also represent a higher risk of money laundering, as these cards can be purchased without ID verification and do not require authentication checks to be activated[37].

37 Cryptotesters, 2021, The Best Peer-To-Peer Exchanges. https://cryptotesters.com/best-p2p-exchanges

CHAPTER 6: APPROACH TO REGULATION IN THE UNITED KINGDOM

As far back as 2014, the UK government was aware of a need to regulate cryptoassets. In August of that year, it announced a program to consider the risks and benefits of this novel form of currency. A key aim was to focus on the question of regulation. The program led to a call for information from key stakeholders with the government publishing its report in March 2015[38]. In that report, the government declared its aim to apply anti-money laundering regulations to cryptoassets. In March 2018, the Cryptoassets Taskforce was created, comprised of HM Treasury, the Financial Conduct Authority (FCA) and the Bank of England. The taskforce published its report in October 2018[39]. It concluded that cryptoassets pose a financial crime risk and stated the government's intention to bring them within anti-money laundering regulations.

The European Union's Fifth Money Laundering Directive had been published in May of 2018 and the taskforce stated that the government intended to be more robust in its regulation than this directive[40]. The deadline for the transposition of the Fifth Money Laundering Directive into domestic law was 10 January 2020. This was the date on which the 2017 Money Laundering Regulations (MLRs) were amended to bring cryptoasset exchange providers within their reach[41].

6.1 WHAT FIRMS MUST DO

The MLRs give the supervisory oversight of cryptoasset exchange providers to the FCA. Firms are required to register with the FCA before they can do business. To qualify for registration, a firm must satisfy the FCA that it is a fit and proper person. Previous convictions of any of the offences listed in the 35 paragraphs of schedule 3 to the MLRs leads to immediate disqualification. In the absence of any such prior convictions, the FCA must consider the firm's record of compliance with the MLRs, its risk of being used for money laundering or terrorist financing, and the level of its skills and experience in the market. The fit and proper test also applies to any officer, manager or beneficial owner of the firm.

The FCA is given a broader power to refuse registration if it is of the view that any information provided in support of the application is false or sufficiently misleading[42]. The FCA is obliged to respond to the firm's application within a period of three months. This is twice as long as applies to other businesses supervised by the FCA[43]. The cost of registration depends on the size of the firm. Those with a UK cryptoasset income of up to £250,000 need to pay £2,000 (the fee rises to £10,000 for firms with a greater income)[44]. Once registered, firms are obliged to comply with the FCA's requests for information and the FCA is given the power to impose directions on the firm in the conduct of its business.

In common with the other businesses covered by the MLRs, cryptoasset firms must conduct their business in compliance with these regulations. This means that they need to conduct assessments of their money laundering risk, create written policies, controls and procedures to mitigate this risk, and appoint an officer authorised to receive reports of suspicious activity. In addition, firms need to conduct due diligence on their customers at the beginning of a business relationship or for occasional transactions involving more than £1,000. Records of the due diligence process have to be kept for a period of five years from the end of the business relationship or last transaction[45]. The customer due diligence requirement also applies to firms which use machine automated processes to exchange money for crypto-assets or vice versa[46].

38 **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf**
39 **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf**
40 As above at page 41
41 **The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (S.I. 2019/1511), regs. 1(2), 4(1)(b)**
42 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Regulation 59
43 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Regulation 59(3A)
44 **https://www.fca.org.uk/cryptoassets-aml-ctf-regime/register**
45 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Regulation
46 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Regulation 27(7D)

In addition to their anti-money laundering obligations, firms must comply with the requirements set out in the FCA Handbook. Included among these are the 11 principles of business such as the requirement to ensure that financial promotions are fair, easy to understand and not misleading[47]. The FCA Handbook also states that firms must treat customers fairly[48].

6.2 WHAT ARE FIRMS DOING?

Firms have shown a willingness to comply with the registration requirement. Indeed, the FCA has not been able to process all applications before the deadline of 10 January 2021. This has led to the extension of this deadline, initially until 9 July 2021[49] and then to 31 March 2022[50]. The FCA cited the complexity and standard of the applications, and the Covid-19 pandemic, as the reason for its inability to process all applications by the initial deadline. By the end of June only six firms were registered with the FCA[51]. This is in stark contrast to the number of firms awaiting registration. In response to a question raised in parliament, the government stated that as of 24 May 2021, 167 firms had applications under consideration by the FCA and 77 new businesses had sought registration[52]. The government response also stated that 90 per cent of firms assessed had withdrawn their applications following their contact with the FCA.

6.3 THE FCA'S APPROACH

The withdrawal of such a large percentage of applications is significant as it suggests that either the FCA is adopting a particularly rigorous approach to the sector, or that the sector is particularly under prepared for the application process. Another possibility is that the FCA has not settled on a defined standard yet and is applying a particularly challenging application process as it searches for that standard. If this were not so, one would expect to see a larger number of resolved applications, be these by failure or by success. Of course, the risk profile and evolving nature of cryptoassets means the cautious approach by the FCA is understandable. There is a lot to be said for initially setting a low tolerance of risk. However, it is important that this does not come at the expense of the development of a new industry.

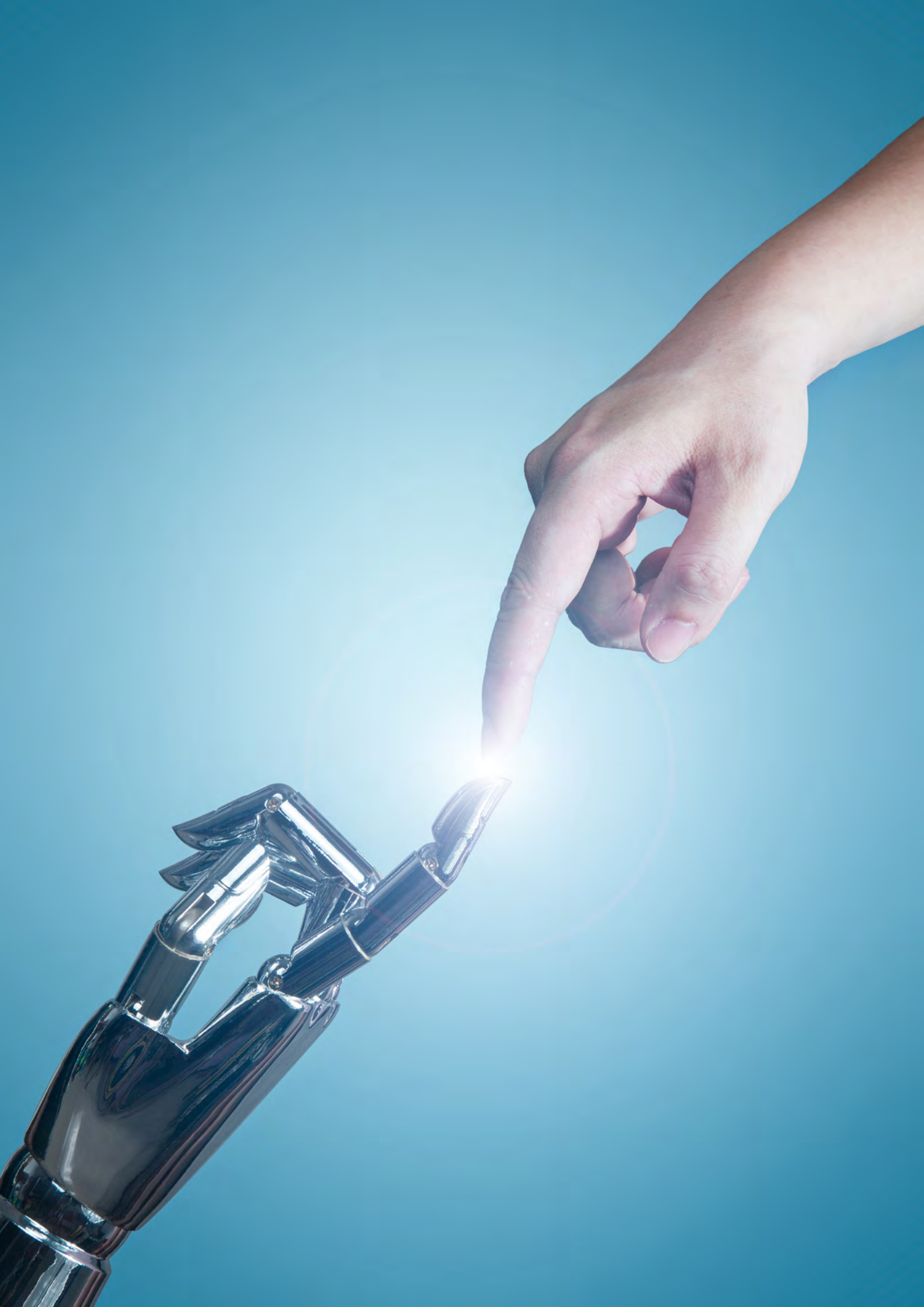
A further threat is that of driving firms underground. If firms do not see registration as achievable, they may elect to risk unregistered trading. This would undermine the aim of regulation. In a list updated as recently as 23 May 2021, the FCA counts upward of 100 firms which appear to be carrying on cryptoasset activity while not registered with the FCA[53]. That so many firms are prepared to engage in unregistered cryptoasset activity suggests that potential banking partners and other investors will continue to use the FCA's register as well as its warning list as a means of avoiding fraudulent firms, investment scams and clone firms[54]. Real time transation intervention for scams/fraud with confirmation of payee style warnings would be a possibility if the right datasets were available within the list.

If the UK is to effectively regulate the cryptoasset industry, it will need to make getting on the right side of regulation achievable. This means that it will need to have a clearly defined standard for firms to meet. Firms must know what this standard is and must feel that it is attainable. Firms would no doubt derive comfort from a clearly defined conduct regime of the type from which established businesses in the financial services world have long benefited. Based on international good practice for risk-based supervision, we could expect to see the FCA to define its standards and provide further guidance on its expectations further over the next 12 months as its analysis and interaction with the sector gives it a clearer view of firms' compliance.

47 FCA Handbook: COBS 4.2.1R, ICOBS 2.2.2R, MCOB 3A.2.1R, BCOBS 2.2.1R, CONC 3.3.1R and Principle 7.
48 FCA Handbook Principle 6
49 **https://www.fca.org.uk/news/press-releases/fca-establishes-temporary-registration-regime-cryptoasset-businesses**
50 **https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime**
51 **https://register.fca.org.uk/s/search?predefined=CA**
52 **https://questions-statements.parliament.uk/written-questions/detail/2021-05-24/6226**
53 **https://register.fca.org.uk/s/search?predefined=U**
54 **https://www.ftadviser.com/regulation/2021/05/18/fca-says-warning-list-is-essential-component-of-adviser-due-diligence/**

For their part, firms must be able to show that they can meet the requirements for registration. They must have a good understanding of their obligations under the MLRs and must be able to satisfy the FCA that they can meet these obligations. They can do so by producing evidence to show that they have a good understanding of the money laundering risks posed by their business and that they have taken sufficient steps to mitigate these risks. A well-drafted anti-money laundering policy is an important step in the right direction and cryptoasset firms could look to those who have been in the regulated sector for a longer period for guidance. A thoughtful, well-prepared application is likely to be well received by the FCA.

It is in the interests of everyone for regulation to succeed. Failure to adequately regulate the evolving crypto industry will further fuel the perception that it is unduly high risk and exposes investors to significant harm. This in turn may lead to a loss of confidence in the industry as a whole and would impede its ability to achieve its potential.



CHAPTER 7: BUILDING TRUSTED RELATIONSHIPS

7.1 PARTNERSHIPS

Building trust is neither quick nor easy. Many in the cryptoasset industry will feel that distrust in the nefarious use of cryptoassets is unwarranted, especially as the industry has progressed markedly in recent years. We hope that cryptoasset firms will use their current spotlight as an opportunity to bridge the trust divide, whilst the the banking sector can take the proactive actions taken by cryptoasset firms as comfort that they can impose a genuine risk-based approach to dealings with cryptoassets. However, the wider issues relating to fraud and consumer protection still need to be fully addressed.

A recent RUSI-ACAMS cryptoassets survey highlighted that the cryptoasset industry remains materially divided from other sectors over the perception of risk[55]. Governments and financial institutions view cryptoassets as a significant source of risk compared to contrasting views of those operating in the cryptoasset industry.

However, this analysis misses the fact that legitimate, well-intentioned cryptoasset providers and services are already engaged in numerous activities which demonstrate their commitment to regulatory compliance, strategic and tactical initiatives and cooperation with a range of partners. In the same way as traditional financial services firms such as banks or insurance providers have undertaken a journey of building confidence through partnership, cryptoasset firms have sought to reach out and collaborate on mutually beneficial activities for the purpose of reducing financial crime. Some examples of such activity includes (but are not limited to):

- Proactive tracking and tracing of funds (prior to and following regulation) to provide to regulators or law enforcement, to improve the visibility of potentially illicit activity given the inherent advantage provided by blockchain transparency;
- Cryptoasset exchanges have engaged in highly productive and illuminating cooperation with law enforcement, given their ability to monitor their customer base, suspicious transactions and where and when they enter the fiat monetary system;
- Through engagement with law enforcement, the police and other public authorities to educate and assist practitioners in cryptoasset technology including by providing training and publicising good practice when investigations intersect with exchanges (e.g. how to request data);
- Initiatives to share red flags and indicators related to financial crime typologies in an effort to identify bad actors and provide this to financial investigation units and law enforcement bodies.

Given these examples and the general appetite to address financial crime risks, it appears to be the time for legitimate, fully regulated and supervised cryptoasset firms to be invited to the public-private-partnerships' (PPP) revolution at the heart of fighting money laundering. These initiatives sit at the centre of a global intelligence-led approach to reducing money laundering – which effectively underpins wider, organised crime strategies. Collaboration between financial institutions, law enforcement and the regulatory community is at the heart of this cooperation, which is already demonstrating its effectiveness since the establishment of the UK's Joint Money Laundering Taskforce (JMLIT) in 2015[56].

55 **https://www.acams.org/en/ACAMS-RUSI-Crypto-Survey-Report**

56 JMLIT is a partnership between the National Crime Agency, the Financial Conduct Agency, 4 other law enforcement agencies (HM Revenue and Customs, the Serious Fraud Office, the City of London Police, the Metropolitan Police Service) and private sector partners. Private sector participants include over 35 financial institutions as well as investment firms, accountants and law firms. The JMLIT operating model has developed to include thematic Public Private Threat Groups, focusing on Money-Laundering, Fraud, Tax Crime, and Terrorist Finance. Time-limited cells focussing on targeted sub-threats sit under these standing Threat Groups. Live tactical intelligence is shared through the JMLIT operations groups, comprising vetted representatives from the Private Sector membership of JMLIT. Since its inception: (i) over 6400 accounts have been identified that were not previously known to law enforcement; (ii) over 4400 suspicious activity reports (SARs) have been filed by JMLIT partners, as a result of information shared; (iii) over 3700 accounts have been closed; (iv) over 235 arrests made; (v) £38m has been identified and under restraint; and (vi) 55 alerts/risk indicators have been issued to the wider sector.

Not only are such PPPs an important first step in the ability to deliver operational successes and efficiency gains (such as the real time ability to share and enrich intelligence), but they can also provide a framework to build positive relationships and dialogue between stakeholders. The establishment of a joint 'picture of threat' utilising evidence-based intelligence from the private sector is vital and should be expanded to include willing and trustworthy cryptoasset firms.

Our collective understanding of the ML/TF risks presented by cryptoassets has developed considerably in recent years through the sharing of case studies, indicators and red flags identified by law enforcement and the private sector, facilitating the sharing and understanding of information through initiatives such as JMLIT. It is easy to make a case for this to be extended to cryptoasset firms who can provide expert advice and guidance, allowing traditional financial firms and investigators the understanding of and ability to follow illicit transactions.

7.2 GOOD PRACTICE

Cryptoassets have suffered in the public eye by association with their early history, especially given that in the past Bitcoin was the token of choice for darknet purchases. However, we are now at the point where global take-up of cryptoassets has led to an improved understanding of the underlying technology and how that sits within a broader spectrum of financial crime risk – in the same way that certain forms of banking are considered higher risk than others, the same is true for cryptoassets[vii]. Concern around cryptoassets is now concentrated on potential fraudulent ventures such as speculative investment scams. Such investment scams are widespread and go far beyond cryptoassets e.g. forex and commodities trading.

With fraud and scams now the predominant form of financial crime risk associated with cryptoassets, banking institutions and cryptoasset providers alike are adjusting dataset or mechnisms to identify such activity. This, coupled with the fear of missing out given media coverage and the role of social media, risks tarnishing perceptions of the sector in general. As such, maintaining effective infrastructure and controls to mitigate hacking, theft, and fraud become a prerequisite for crpyotasset firms seeking to prove their credentials. Firms have the opportunity to demonstrate the strength of their intentions by applying policies and procedures documenting their compliance with the money laundering regulations.

Any continued association with cryptoassets should be seen through such a lens – malign actors jumping on the cryptoasset bandwagon to defraud vulnerable individuals rather than being defrauded by the technology itself or by businesses who offer legitimate cryptoasset services. Centralised exchanges in the UK, US and across the EU are within the AML/CTF regime and have Customer Due Diligence requirements similar to those of banks. As more people learn that centralised cryptoasset exchanges, where 90 per cent of activity takes place, are able to link wallet addresses to identifiable individuals then certain misconceptions should start to breakdown.

As of September 2021, only ten firms in the UK had been granted permanent licenses to operate as crypto-exchanges or custodian wallet providers, while over 160 firms have been placed on the "temporary registration list" pending further investigation into each firm's AML controls by the FCA. As firms have only been required to comply with AML regulation since January 2020, it is unsurprising that some financial crime frameworks are relatively immature compared to other financial institutions. Over the next six months it is imperative that firms invest in their frameworks to uplift them in line with regulation so that they can continue to operate in the UK. This is not just important from a regulatory perspective, but an improved understanding of the risks inherent to each business' operations and the controls in place to mitigate these risks, gathered through a firm-wide risk assessment, will build management's confidence in the business.

Where cryptoasset firms could benefit is by boosting their first and second line of defence professionals by taking on experienced individuals with demonstrable and respected competencies in tackling financial crime. This appears to be a growing trend as both firms and regulators are upskilling themselves in an effort to gain a firm grip on the potential intersection between cryptoasset technology and financial crime, be it AML, fraud or sanctions evasion. Recent appointments made to address FCC/AML framework obligations by industry participants appear to be addressing that respectability journey[57].

A new generation of cryptoassets and obfuscation tools with enhanced levels of security and anonymity threatens to create new risks for the sector and financial crime compliance professionals alike. Mixers, privacy coins, privacy wallets and IP anonymisers are examples of such techniques. What is less generally known is that there are ways and means for cryptoasset exchanges to demonstrate that they are alive to this threat and taking their compliance duties seriously. Such efforts need to be both operational and strategic and better publicised.

Cryptoasset exchanges can be at the heart of this proactive response. Well-known service providers are already acting in this regard. It is for each exchange to decide whether to list a privacy coin, and listing such a coin may well affect the ability to obtain regulatory licenses in developed markets such as the US, UK and EU. Additionally, it is not well known that some privacy coins have optional privacy features which may make them more palatable to exchanges and it is within the purview of exchanges' risk tolerance to list coins such as Monero. Furthermore, research and development of de-mixing is ongoing as mixing services are important in the obfuscation of funds from ransomware and other crimes.

Then there are the actions being taken at a frontline level, including offboarding accounts found to be transferring large and frequent amounts to privacy wallets and offboarding wallets using mixing services. These sit alongside initiatives with representatives from the sector to tackle ransomware and the ability of forensic firms to allow exchanges to identify accounts receiving or sending to known ransomware clusters triggering AML processes[viii]. As it becomes better known, such action will send a strong message to regulators that the industry is looking to clamp down on any services which look to skirt around AML controls.

7.3 INDUSTRY STANDARDS

Based on the above trends in good practice, there are indications that the maturing cryptoasset sector could develop its own industry standards for fighting financial crime. What standards can and should cryptoasset providers put in place to reinforce positive perceptions of industry leaders?

- Implement quick to activate evidence-based rules to prevent illicit activity, block illicit crypto addresses and customer friction rules;
- Tracking and tracing of funds to provide real-time intelligence to regulators or law enforcement given the visibility of blockchain as a payments system;
- Build or implement new modules in systems which can be quicker to pivot than traditional financial institutions, including sharing such information with financial institutions in real time;
- Proactive engagement with law enforcement, education and case referral including providing training and insight and publicising good practice when investigations intersect exchanges (e.g. how to request data).
- Outreach to relevant trade bodies to engage with standards setting bodies such as the Joint Money Laundering Steering Group (JMLSG) in order to contribute and refine the guidance they produce to assist financial institutions to comply with their AML/CTF responsibilities.

57 **https://www.coindesk.com/binance-us-hires-former-bank-regulator-brian-brooks-as-ceo**; **https://www.coindesk.com/ex-cftc-chair-chair-giancarlo-joins-blockfi-board-of-directors?utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz-_vgy8aRAsw0-F8DBBUUAkHumGcgsKoN5NNb2IFDv80Aexf4AQmqMIbygv7fFM_PuFreVGp**

CONCLUSION

Cryptoassets and their decentralised, quasi-anonymous nature pose a disruptive threat to traditional financial institutions. The same could have been said for MSBs, payment service providers and e-money providers over the last 20 years, which all stirred up significant debate regarding consumer protection and the integrity of the financial system. Eventually, traditional financial institutions have found ways to work with these other sectors and incorporate these new services into the wider financial ecosystem.

Achieving that elusive balance between innovation and regulation, with prominent voices weighing in – some touting cryptoassets as the future of finance and others raising concerns about the illicit finance implications of the cryptoasset ecosystem – make for a confused debate. While it is true that we don't know what we don't know about the cryptoasset market, the same remains true of illicit activity in the banking system and other sectors, as evidenced by multiple continuing scandals and enforcement actions.

Further application of KYC/AML regulations, long seen as effective by regulators, professional bodies, and multilateral institutions will help assuage financial institutions concerns about cryptoasset transactions. Equally a continued drive to identify illicit activity, prevent fraud, track and trace illicit funds and provide information to regulators and law enforcement will all stand the industry in good stead.

By reviewing practical ways for different sectors to work closely together, a potential roadmap for future collaborative ventures can emerge. Some examples of this might include inclusive public private partnerships and intelligence sharing, greater engagement with crypto sector trade bodies and how financial institutions can bring their experience to onboarding and offboarding of clients in order to comply with financial crime regulations.

It is worth dwelling on regulatory cooperation and how that might develop and influence the cryptoasset debate. As the AML/CTF regime develops and more supervisory and enforcement activity takes place, there is likely to be a better sense of how the regulator perceives a clearly defined conduct regime. Given the global nature of cryptoassets, an enhanced level of cooperation and collaboration between regulators and the industry is required. In line with regulatory objectives, this could lead to more efficient registration, supervision and consumer protection.

Banks are increasingly entering into partnerships with cryptoasset firms based on the increased profitability of the sector and client interest. Not only is it possible to provide accounts or other financial services to cryptoasset companies, as the sector grows at a rapid rate it is already being provided by banks' direct competitors and other marketplace service providers. Adequate compliance controls and risk mitigation measures, information sharing, public-private partnership and industry standards are part of the pathway to future partnerships and how these can be embedded across the industry.

Finally, beyond managing financial crime risk exposure there is the requirement to ensure appropriate safeguards are in place with respect to consumer protection, to address regulator concerns and encourage wider and safer adoption. The 'crypto crash'[58] in May this year was widely attributed to overleveraged trading by investors which can create extreme price volatility. Industry action includes crypto-exchanges putting in place sensible limits and controls with regards to the types of products investors can use and the levels of margin that are made available. We are already seeing action in this area from some crypto-exchanges, however there is more to do in order to fully assuage the concerns of regulators across the globe.

58 **https://www.cnbc.com/2021/05/25/bitcoin-crashes-driven-by-big-margin-bets-new-crypto-banking.html**

ENDNOTES

i On 7th January 2021, HM Treasury published a **consultation paper** outlining the UK's proposed regulatory approach to cryptoassets and stablecoins although it does not address financial crime risk explicitly.

ii The best-known example being the Costa Rican domiciled criminally complicit currency exchange and payment processor Liberty Reserve which was shut down by U.S. prosecutors in 2013.

iii A darknet marketplace operated as a TOR hidden service that was taken down by the FBI in 2013.

iv **https://www.ft.com/content/9685a2e0-e8d5-48f5-9c1f-66aea8cb1597**

v For instance, mirror trading and other forms of market manipulation stand out as being inherently more difficult to track and trace for financial crime activity.

vi A white hat is an ethical **computer hacker**, or a **computer security** expert, who specializes in **penetration testing** and other testing methodologies that ensure the security of an organization›s **information systems**.

vii Cryptoassets were judged to me medium risk in the UK's National Risk Assessment of Money Laundering and Terrorist Financing published in December, 2020.

viii Exchanges themselves conduct their own reconnaissance to identify customers engaging with such ransomware.