Anti-money laundering regulation of cryptocurrency: UAE and global approaches

Tareq Na'el Al-Tawil
Department of Management, College of Business Administration, Ajman University, Ajman, United Arab Emirates

Abstract

Purpose – The purpose of this paper is to provide a high-level analysis of the intersection emerging cryptocurrency sector with anti-money laundering (AML) regulations and risk-based AML diligence systems maintained by financial institutions.

Design/methodology/approach – The analysis begins with a description of cryptocurrencies, focusing specifically on how the supporting technologies and applications increase vulnerabilities. The information will lay the foundation for examining the vulnerabilities existing in the architecture of cryptocurrency technology, as well as potential targets for regulations. The second part of the analysis will then shift focus to defining the scope of the money laundering problem associated with cryptocurrencies. An in-depth understanding of the problem is necessary to inform tailored AML legislation and regulations. The third part of the analysis will explore emerging AML regulations that govern cryptocurrencies, focusing specifically on those being developed and implemented in the United Arab Emirates (UAE). The UAE regulations will then be compared to those of the USA and European Union (EU) for comparative analysis and best practices.

Findings – The UAE has a robust legal system aimed at bolstering AML efforts while supporting widespread integration of crypto assets into business and government operations. A review of the UAE's legislative framework reveals critical issues. First, the current regulations do not cover decentralized finance (DeFi) and non-fungible tokens (NFTs). The absence of clear regulations for DeFi and NFT protocols has created a leeway for money laundering and related criminal activities. Second, there is a high level of fragmentation in the UAE's legislative landscape. The UAE does not have uniform, national laws that apply to all the Emirates. Fragmentation is not unique to the UAE but a major global problem that affects the USA and EU. Therefore, it is necessary to adopt a tailored approach where standard rules and regulations are responsive to the diverse aspects of cryptocurrencies. The strategy is vital, as it will be impractical to create a single legislation or law that will cover all the crypto assets, including their diverse applications. Furthermore, the Financial Action Task Force (FATF) should develop a global standard that will support a unified/harmonized application of AML/counter-terrorist financing (CTF) laws and regulations related to cryptocurrencies and the blockchain technology.

Originality/value – The borderless nature of digital currency and exchanges means that the existing laws and regulations are inadequate to address cross-border money laundering activities. Thus, there is an urgent need of harmonizing global regulations to ensure uniformity in applications. The quest for harmonization should be a priority as the FATF works towards developing a global standard. The global standard will support a uniform application of AML/CTF laws and regulations related to cryptocurrencies and the blockchain technology.

Keywords Money laundering, Cryptocurrency, Blockchain technology, Cybercriminals

Paper type Research paper

Journal of Money Laundering Control
Vol. 26 No. 6, 2023
pp. 1150-1164

1368-5201
DOI 10.1108/JMLC-07-2022-0109

Introduction

Blockchain technology is one of the revolutionary technological developments of the 21st century. Blockchain is a distributed database or ledger that records a continuous growing list of ordered records, known as blocks (Dyntu and Dykyi, 2019). Blockchain technology provides the infrastructure for cryptocurrencies and other applications. Cryptocurrency is a digital currency that operates on a blockchain technology to record, store and secure transactions. Bitcoin was the first major blockchain innovation that emerged in 2009 following the global financial recession. Although Bitcoin is the pioneer and most popular cryptocurrency, blockchain technology has supported the development of other cryptocurrencies, such as Ether, Litecoin, Ripple and many others (Dyntu and Dykyi, 2019). Blockchain technology and cryptocurrencies continue to grow drastically and revolutionize business transactions beyond the traditional financial sector. The unprecedented development of blockchain technology and increased adoption of cryptocurrencies have paralleled concerns over money laundering and related crimes (Brown, 2016).

The link between cryptocurrency and money laundering has ignited debates over the need of regulating the industry. The question of regulation is critical considering that Satoshi Nakamoto launched Bitcoin in early 2009 with the goal of restricting the interference of governments, financial institutions (FIs) and other third parties in financial transactions (Bartoletti *et al.*, 2021). Governments and regulatory agencies did not indeed pay much attention to the silent cryptocurrency revolution considering that the sector was relatively small. However, the cryptocurrency market has expanded beyond the initial projection to become a billion dollar industry. The development of altcoins has further strengthened the market value of cryptocurrencies. Consider the case where tokenized assets on the crypto market exceeded US$2.5tn (Bartoletti *et al.*, 2021). The main concern is about the pseudonymity features of cryptocurrencies that have emboldened cybercriminals. A pertinent question is how to regulate the industry without stifling the nascent innovation.

The purpose of paper is to provide a high-level analysis of the intersection emerging cryptocurrency sector with anti-money laundering (AML) regulations and risk-based AML diligence systems maintained by FIs. The analysis begins with a description of cryptocurrencies, focusing specifically on how the supporting technologies and applications increase vulnerabilities. The information will lay the foundation for examining the vulnerabilities existing in the architecture of cryptocurrency technology, as well as potential targets for regulations. The second part of the analysis will then shift focus to defining the scope of the money laundering problem associated with cryptocurrencies. An in-depth understanding of the problem is necessary to inform tailored AML legislation and regulations. The third part of the analysis will explore emerging AML regulations that govern cryptocurrencies, focusing specifically on those being developed and implemented in the United Arab Emirates (UAE). The UAE regulations will then be compared to those of the USA and European Union (EU) for comparative analysis and best practices.

Cryptocurrencies: supporting technology, applications and vulnerabilities

The second section of the paper explores the features that characterize cryptocurrencies and their technologies. The section presents an explanatory framework that will lay the foundation for assessing the dangers of cryptocurrencies for AML and counter-terrorist financing (CTF) efforts. Cryptocurrency is a burgeoning market defined primarily by virtual currencies (VCs). VCs have two important features. First, VCs constitute an unregulated digital currency. Second the central bank neither controls nor issues VCs. The two features are not only central to the functioning of VCs, but they also increase their security vulnerabilities. VCs do not have an intrinsic value compared to the traditional regulated currencies (Bartoletti *et al.*, 2021). As mentioned earlier, central authorities control government-issued currencies and back them with either fiat currency/sovereign debt or hard assets, such as gold. In contrast, the unregulated nature of VCs often leads to extensive price fluctuations. Bitcoin is a notable VC that has been recording significant variations in pricing since its introduction to the VC market (Brown, 2016).

Blockchain technology or distributed ledger is the key feature of cryptocurrencies. In fact, Barone and Masciandaro (2019) have described blockchain technology as the engine that powers cryptocurrency networks. Blockchain is a cryptographically secured ledger that uses a decentralized network to track transactions (Shapiro, 2018). VCs are primarily categorized as being centralized or decentralized. Decentralized VCs, also known as cryptocurrencies, "are distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight" (Dyntu and Dykyi, 2019). A noteworthy observation is the absence of a third-party repository or central administrator for the decentralized VCs. Instead, cryptocurrencies rely on a distributed system to authenticate transactions involving decentralized VCs. Comparatively, centralized VCs have a repository or central administrator that issues the virtual currency. The central administrator or repository performs the same function as that of the central bank in regulating the currency system (Barone and Masciandaro, 2019).

Blockchain networks, such as Bitcoin, Ethereum and Litecoin, provide the supporting technology for many decentralized VCs. The purpose of the blockchain network is to link a series of records, also known as blocks, with cryptography. The network has multiple nodes or computers that receive and broadcast requests for a transaction (Brown, 2016). The network verifies the transaction and then adds an unchangeable and permanent block to the blockchain by creating a distributed ledger technology (DLT). The DLT plays an instrumental role in ensuring the integrity and safety of the financial transactions (Dupuis and Gleason, 2021). Furthermore, the DLT has a proof-of-work system that sustains the crypto ecosystem and validates transactions. The DLT also holds a public chronological record for monitoring transactions and linking them to specific Bitcoin addresses that serve as stores of value (Brown, 2016). The DLT infrastructure is increasingly facilitating micro-financing by monetizing low-cost services and goods. FIs are also using the technology to promote financial empowerment for unbanked and poor populations.

In principle, decentralized cryptocurrencies allow transacting parties to interact directly in secure, cost-efficient, fast and private ways without the need of intermediaries, such FIs and banks. The exclusion of a central administrator in the decentralized peer-to-peer network prevents the possibility of a centralized security failure. The exclusion also lowers transaction costs and enhances transparency between the transacting parties (Bartoletti *et al.*, 2021). Nevertheless, the absence of intermediaries or a central authority raises pertinent regulatory concerns. Specifically, the decentralized system creates a convenient network for money laundering, terrorist financing and other illegal financial transactions. The absence of a central oversight is a major security concern because it makes it hard to apportion accountability in cases of fraud/scams, money laundering and other illegal financial transactions (Bartoletti *et al.*, 2021; Shapiro, 2018).

In summary, VAs have numerous potential benefits for businesses and individuals. Notable advantages of VAs include lower cost, greater speed and increased efficiency in completing financial transfers and payments. The potential of facilitating financial inclusion has now supported the proliferation of VCs beyond the financial sector. On the other hand, the DLT systems offers massive benefits that go beyond those accrued from VCs. Businesses and business institutions are increasingly findings mechanisms for integrating the blockchain technology in their respective operations (Dupuis and Gleason, 2021). Nonetheless, the unregulated nature of VCs makes them highly vulnerable to criminality. The anonymity or pseudonymity of VCs constitute a significant security risk. Criminals are exploiting the unique features of VCs to promote acts of money laundering, terrorist financing, theft and fraud. Consequently, VCs potentially pose a considerable danger to the integrity of global financial systems in the absence of strong regulatory frameworks (Dupuis and Gleason, 2021).

Money laundering in the cryptocurrency system

Money laundering entails the process of concealing the sources of illegally acquired money using multiple transactions before integrating the funds into a legitimate financial system (Dyntu and Dykyi, 2019). The defining feature of money laundering is "cleaning" money from dirty sources, such as drug and human trafficking, terrorism, kidnappings, cybercrimes, corruption, gambling, embezzlement and related illegal activities. Money laundering follows three successive stages: placement, layering and integration. Placement introducing the proceeds of crime into the financial system using different approaches, such as shell companies, offshore banking and deposit structuration. The second step is to disguise the trail of the money to foil paper trail to the sources. Notable strategies used at this stage include using false invoices, loaning to a company, transferring money to a company account. The third step is making the "cleaned" money available to the criminal(s) using legitimate sources (Bartoletti *et al.*, 2021). Money laundering does not necessarily involve all the three steps nor follow the steps in a sequence. On the contrary, some of the stages could be combined while other repeated on multiple occasions.

The explicit steps of the money laundering process are central to the effectiveness of AML strategies. The clearly defined steps make it practical for regulatory and law-enforcement agencies to trace criminal proceeds to their illegitimate sources. FIs usually look for red flags at each of these stages (Brown, 2016). The use of red flags is a risk-based approach (RBA) under the framework of the Financial Action Task Force (FATF). FATF is an international authority that develops global standards for combating money laundering and terrorist financing. The inter-governmental organization proposes the use of risk categories or red flags to identify the risk of money laundering and terrorist financing (Dyntu and Dykyi, 2019; Jones, 2022). The most common red flags include transactions that involve geographic/country risk, customer risk and product/service risk. The presence of the risk categories informs decisions about whether to record the transaction through a suspicious activity report, prompting further investigations or ignoring the same (Barone and Masciandaro, 2019). Unfortunately, the decentralized nature of cryptocurrencies makes it challenging to apply FATF RBA regulations and red flags.

Cryptocurrencies present momentous challenges to global AML/CTF regulatory frameworks. FATF RBA best practices include due diligence, monitoring of transactions and know your customer (KYC). These strategies have been effective in tracking the flow and integration of criminal proceeds into the legitimate financial systems. However, they cannot be successfully integrated in the cryptocurrency landscape because of the practical difficulties. The main problem lies with the absence of a third-party repository or central administrator in the decentralized VC system (Boggiano, 2021). A pertinent question that emerges is whether the VC ecosystem requires robust and extensive regulations. An answer to this question is necessary because it will lay the foundation for assessing the strengths and limitations of the existing regulations in the UAE and across the globe. Thus, it is imperative to examine the rationale for regulating cryptocurrencies, including the scope and extent of these regulations. The achievement of this goal is critical in finding out if cryptocurrencies should have the same level of AML regulations like those applied to the traditional banking system.

The claim that cryptocurrencies have contributed to the increasing cases of money laundering and terrorist financing is a controversial issue. Two phenomena have bolstered claims about the safety risks associated with cryptocurrency. First, Silk Road, a digital black-market platform that evolved with the inception of Bitcoin hosted illegal drug transactions and money laundering activities. Although the FBI shut down the Silk Road in 2013, the incident exposed the securing vulnerabilities of cryptocurrencies. Bitcoin has continued to be a site for money laundering, with an exponential increase in cases (Dyntu and Dykyi, 2019). Second, Zaif, a Japanese cryptocurrency exchange, has sued Binance for having weak KYC requirements that facilitated the laundering of $60m that cybercriminals stole from the exchange in 2018 (Shevchenko, 2022). The two examples have emboldened claims that cryptocurrency is a threat to the security of global financial systems by making it easier for criminals to launder illegal funds. Recent data from Chainalysis, a blockchain analysis company that specializes in analyzing crypto and blockchain, report a 30% increase in laundered cryptocurrency in 2021 (Chainalysis Team, 2022a).

A deeper analysis of the crypto money laundering is central to determining the level of regulation needed. The media and critics continue to paint a gloomy picture about crypto money laundering and other illegal activities. The reports have raised apprehension and an ambivalent attitude about cryptocurrencies across countries and central banks. Some governments, such as Russia, China, India, Iran, Turkey and others have either restricted cryptocurrencies or consider Bitcoin and altcoins as illegal forms of currency. Moreover, there has been a sustained increase in security crackdown against cryptocurrency wallets owned and controlled by malware operators, ransomware attackers, human traffickers, scammers, terrorist groups and dark net market operators. The concerns are indeed valid considering the unregulated and decentralized features of cryptocurrencies. A critical question is whether the crypto money laundering figures being released are a true reflection of the problem and worser than those associated with the traditional banking system. Therefore, first step is comparing the rates of money laundering through cryptocurrency versus traditional banking.

The United Nations (UN) estimates that $800bn to $2tn or 2%–5% of fiat currency is associated with criminal activity, including money laundering and terrorist financing. According to the UN estimates, more than 90% of money laundering in fiat currency remains undetected (United Nations Office on Drugs and Crime, 2022). Concurrently, Chainalysis reports that only 0.15% of all cryptocurrency transactions were associated with some form of illegal activity in 2021 (Chainalysis Team, 2022a). The data demonstrates that cryptocurrencies only accounts for the smallest portion of money laundering and terrorist financing activities. The latest report of the Financial Crimes Enforcement Network ("FinCEN"), an agency within the US Treasury Department, offers more insights into this issue. Specifically, the FinCEN reports that profits from corruption activities in developing countries, drug trafficking, human trafficking and Ponzi schemes continue to flow through FIs unabated despite being flagged by bank employees. FinCEN cites the most trusted global banks as being enablers of money laundering and terrorist financing activities across the globe.

Cryptocurrencies can reach the same threshold of money laundering through the traditional banking system if they meet two specific conditions. The first one is high transaction speeds to facilitate efficient and swift borderless transfer of proceeds of crime. The second one is completing illegal financial transactions in decentralized, fully contained VC environments (Barone and Masciandaro, 2019). Opponents of cryptocurrency often cite the anonymity or pseudonymity of the system as a key feature that supports the propagation of money laundering. People transact in VCs using codes or alphanumerical pseudonyms, which makes it hard to link the pseudonym to a real person, providing a veil of anonymity. Anonymity is not a guarantee considering that law enforcement agencies have been successful in tracing criminal activities being perpetrated through cryptocurrencies. For example, the FBI uncovered the Silk Road syndicate because the criminals had used Bitcoin to transact. On the other hand, there is a relatively small number of VCs that are truly decentralized. Most crypto users also remain connected to the traditional financial system, which makes it practical to monitor suspicious activities (Dupuis and Gleason, 2021).

Cryptocurrencies pose a low risk to AML and CTF efforts, but the VC system still affords an efficient system for money laundering activities. Cases of money laundering through Bitcoin continue to increase. Thus, it is of the essence to established local, regional and international policies and regulations are effective in tackling the dangers that VCs pose to AML and CTF. The current AML/CTF regimes depends primarily on FATF's RBA to money laundering and terrorist financing. The RBA system is inefficient, as discussed previously, because decentralization makes it challenging to identify and act upon red flags. Consider the case where global authorities spend up to $8bn annually on combating money laundering and terrorist financing but only seize less than 1% of illicit financial flows through the established financial system (United Nations Office on Drugs and Crime, 2022). Both the UN and FinCEN have also admitted that more than 90% crime proceeds pass through the established financial system without being detected. Consequently, it is counterproductive to apply regulations and practices that have been ineffective in tackling money laundering in the financial system.

The meteoric rise of VCs and related technologies arguably pose a considerable challenge to the existing AML/CTF regime. The conventional principle of "bank secrecy" has had a profound influence on the architecture of the current AML/CTF regulations. The secrecy principle mandates FIs to act as gatekeepers as their primary responsibility. The role entails monitoring financial transactions and reporting to public authorities on a case-by-case basis. The secrecy principle cannot be applied to decentralized cryptocurrencies because of the absence of gatekeepers. Thus, the technology that supports VCs has effectively rendered conventional AML/CTF regulations as outdated (Naheem, 2020). A notable example is where international regulations developed by the UE and FATF emphasize the intersection of fiat money and cryptocurrencies. The approach leaves many of the cryptocurrency transactions unregulated. Hence, it is now imperative to explore emerging regulations being adopted in the UAE and globally. The author proposes a tailored approach to cryptocurrencies because existing AML measures are incompatible with cryptocurrencies and do not address the blockchain.

Anti-money laundering regulations: the United Arab Emirates perspective

The UAE has a highly regulated business environment. A brief overview of the governance structures in the UAE lays the foundation for understanding the application of the existing AML laws and regulations. The UAE is a federal government made up of seven Emiratis. Each Emirati has their own free zones. The free zones have limited independence from both the Emirate and federal law applicable to customs and restrictions on foreign investment. Nevertheless, the UAE has two autonomous financial free zones: the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM). The DIFC and ADGM are independent jurisdictions created under the UAE Constitution and federal law, and they are regulated by the Dubai Financial Services Authority (DFSA) and the Financial Services Regulatory Authority (FSRA), respectively. The two are autonomous because their regime of civil, financial and commercial laws are distinct from the reminder of the UAE. The next step is to review the UAE's legal system before narrowing to AML regulations.

The UAE legal system has rapidly modernized in response to its position as a global trading and financial hub. The UAE espouses the civil law system that included both legal codes and Islamic/Shariah law. The major legal codes include the Civil Transactions Law, the Penal Code, the Commercial Transactions Law and the Commercial Companies Code. Each of the seven Emirates also have their own laws and regulations in addition to the federal law. The laws and regulations apply in each of the Emirati where federal law is nonexistent. The UAE Central Bank and the Securities and Commodities Authority (SCA) are the primary federal regulators in the realm of financial and capital markets (Elrifai, 2021). On the other hand, the DIFC uses the common law system that draws influence from the English common law, whereas the ADGM wholesomely uses the English common law. However, it is important to point out that the UAE federal criminal law, including the federal AML laws, are enforceable in both the DIFC and ADMG. The next task now is to examine AML laws and regulations in the UAE having explored how the legal system works (Elrifai, 2021).

Regulation of blockchain and cryptocurrencies in the United Arab Emirates

The UAE Government has prioritized both DLT and blockchain technology. The UAE's quest for digitization has influenced the decision by both local and federal governments to explore, adopt and integrate blockchain technology across government operations. Notable initiatives include the Emirates Blockchain Strategy 2021 and Dubai Blockchain Strategy 2020 (Naheem, 2020). Investment into the blockchain and crypto technology has allowed the UAE to diversify its economic potential beyond oil production. The efforts have laid the groundwork for the UAE to become the global hub for blockchain and crypto technology. The achievement of this goal has been the primary motivator for the UAE's rapid legal modernization (El Maknouzi and Sadok, 2021). The UAE has adopted and continues to work on new laws and legislations that will propel it to the global status of the largest hub for blockchain and crypto technology. Therefore, the UAE has not banned crypto currencies, but it has established a robust legal framework to protect crypto assets from financial criminals (Elrifai, 2021). Regulation of cryptocurrencies in the UAE falls under three categories: the ADGM, the DIFC and Onshore UAE.

First, the ADGM has assumed an active and leading role in regulating cryptocurrencies through the FSRA, Abu Dhabi's competent regulator. The FSRA amended the Financial Services and Markets Regulations of 2015 by releasing a far-reaching framework to regulate crypto asset businesses in June 2018 (Kerr and England, 2022). The FSRA describes crypto assets as commodities under this law. The framework, dubbed the Crypto Asset Legislative Framework, requires all operators in the virtual asset (VA) market, including custodians or intermediaries, to seek approval from the FSRA. The FSRA has been regularly updating the framework to keep abreast with global developments in cryptocurrencies (Naheem, 2020). Thus, anyone transacting in the virtual or crypto assets must comply with the same regulations as those that govern derivatives, securities and funds in the ADGM. The approval allows the operators to operate as financial service permission holders. The last amendment was in February 2020, and it included the crypto regulatory guidelines, the Regulation of Crypto Asset Activities. The guidelines include security measures that govern AML/CTF requirements and crypto assets exchanges (Elrifai, 2021).

Second, the DIFC has always taken a wait-and-see approach when it comes to the regulation of crypto assets, including their issuance, issuers and sponsors. Consider the case where the DFSA warned investors about cryptocurrencies, clarifying that the regulator was not actively regulating crypto assets, license farms and product offerings in the DIFC. However, the DIFC introduced a new regulatory framework for VAs in October 2021 through the Consultation Paper 138 issued in March 2021 (El Maknouzi and Sadok, 2021). The regulations, operationalized by the DFSA, apply to investment tokens. The rights and duties of the holders determine whether the tokens will be a derivative or security. The new regulations allow individuals to engage in activities related to investment tokens either from or in DFIC (Gump, 2022). Nonetheless, DFSA approval is mandatory prior to carrying out these activities. The DFIC continuously amends and enacts new laws aimed at regulating crypto assets and utility tokens. For example, the DFIC is currently keen on adopting investment tokens that are missing in the new regulations. They include utility and exchange tokens, as well as stablecoins (El Maknouzi and Sadok, 2021).

Third, the SCA released Decision No. 23 of 2020 in November 2020, named the Crypto Assets Activities Regulation (CARR). The CARR outlines general operational rules businesses involving crypto assets, including individuals taking part in these activities. The CARR also has additional AML/CTF provisions. The CARR provisions underscore the need of instituting a solid compliance network, including AML monitoring practices and KYC. One of the requirements is to only withdraw and deposit crypto assets to and from a designated bank account in the name of the holder. The designated bank account should also be with an authorized financial institution, whether domiciled in the UAE or a foreign country (Naheem, 2020). According to the CARR regulations, foreign FIs must have an explicit approval from the SCA. The traceability of the crypto asset is another element of the CARR provisions. Specifically, the CARR does not allow FIs open funding accounts for a crypto asset that cannot be adequately traced. The funding accounts do not qualify to transact through a licensed person (Elrifai, 2021).

Finally, the Dubai Multi Commodities Centre (DMCC) has signed memorandum of understanding (MoU) with the SCA. The MoU came into effect in March 2021. The DMCC, a new free zone and a Dubai Governmental Authority, regulates commodities trade and enterprise. The purpose of the MoU is to create a regulatory framework that will govern all crypto assets being listed and traded in the DMCC (Kerr and England, 2022). DMCC's onboarding teams will collaborate with the SCA to approve crypto-related businesses intending to establish base in the DMCC. The SCA will also regulate crypto-related activities in line with the policies promulgated in October 2020. The aim of the alignment is to develop an integrated ecosystem that will support blockchain and crypto industries. The MoU will also create an environment for spurring growth within the sector, as well as supporting the application of blockchain technologies in Dubai (El Maknouzi and Sadok, 2021). The DMCC has been licensing and regulating proprietary trading involving crypto commodities since 2017. The DMCC labels crypto assets as commodities, subsequently allowing them in the jurisdiction (Elrifai, 2021).

Critical analysis of the United Arab Emirates laws and regulations

The UAE has robust legal framework for regulating crypto assets. In a nutshell, the current cryptocurrency regulations introduced from the fourth quarter of 2020 compel providers to incorporate crypto assets and services onshore or in the existing financial freezones. The providers must also seek licensure from the SCA. The ADGM was first to introduce a comprehensive VA framework in the UAE (Naheem, 2020). As such, ADGM's regulations have not only garnered considerable international attention but they have also attracted some centralized crypto asset exchanges to operate out of the ADGM. The ADGM regulations will continue to attract investors if the VA framework remains agile and service-oriented. The regulations will particularly continue to attract traditional centralized entities whose supporting technology aligns with ADGM's current framework (Hadef and Partners, 2021). The same case also applies to the DMCC new regulations. DMCC's has significant international collaborations that continues to attract considerable talent.

Moving forward, the effectiveness of the UAE legislative frameworks will depend on their ability to attract talent. The FATF had added the UAE to the "grey" watchlist of money laundering countries. The FATF identified the UAE as having inherent vulnerabilities to money laundering because of its position as a global financial and trade hub. Thus, the UAE could use the partnership between DMCC and SCA, as well as DMCC's international collaboration to attract talent. The SCA VA Regulation has also made it certain for crypto businesses to operate onshore, in addition to helping the UAE to attain some of the projected blockchain ambitions (Naheem, 2020). The growth and safety of the cryptocurrency landscape in the UAE depends on the ability to attract technical talent, beyond attracting only business and marketing functions. Technical talent will set the stage for blockchain and cryptocurrency innovations to thrive in the UAE (Elrifai, 2021). However, there are notable concerns that will more likely derail the achievement of this objective, as well as retain the UAE on FATF's grey watchlist of money laundering countries.

First, the regulations have largely bypassed the growing decentralized finance (DeFi) industry. DeFi is central to the growth and development of the global blockchain and crypto ecosystem. DeFi is an emerging financial technology that uses secure distributed ledgers such as those used by cryptocurrencies (El Maknouzi and Sadok, 2021). Conversely, DeFi is increasingly evolving to become the most preferred avenue for propagating money laundering and related criminal activities. For instance, Chainalysis has reported a significant increase in the use of DeFi to launder money. According to Chainalysis, there was a 1,964% year-over-year increase in the total value of cryptocurrency laundered through DeFi protocols, reaching a total of $900m in 2021 (Chainalysis Team, 2022b). The cited figures only account for funds generated through cryptocurrency-based crime, such as darknet market sales and ransomware attacks. The true figure for DeFi money laundering activity is more likely to be much higher after incorporating profits accrued from 'offline' crimes, such as drug trafficking, where criminals convert the illegal proceeds into cryptocurrency (Elrifai, 2021; Moss, 2021). Thus, DeFi is a grey area that needs comprehensive laws and regulations.

The UAE will attain the goal of being the global leader in cryptocurrencies by making DeFi regulations a policy priority. The main concern is that both the ADGM and Onshore UAE regulations do not incentivize the development of DeFi and permissionless peer-to-peer systems, as the regulations are unclear in these areas. The initial draft of the SCA VA Regulation included some provisions that would have regulated DeFi activities (El Maknouzi and Sadok, 2021). Unfortunately, the final and implemented regulation ultimately omitted the provisions. Similarly, consultations that led to the DIFC regulations did not support DeFi because of the low-risk appetite in relation to security tokens. Comparatively, FSRA released a discussion paper in May 2022 to broaden understanding of the potential opportunities and risks associated with DeFi protocols. Abu Dhabi is the only Emirate that seems to be actively seeking to develop a legislative framework that will govern DeFi (Kerr and England, 2022). There is still a lack of clarity and direction in Dubai and from both the Central Bank and SCA. The increasing pace of DeFi adoption exemplifies the danger of not addressing the current legislative gap.

Global legislative efforts are acknowledging the need of regulating DeFi protocols for security reasons. For instance, the FATF updated its recommendations in November 2021 to encompass DeFi. The new draft guidance has clarified the definition of DeFi protocols, including the designation of DeFi providers as VA service providers (VASPs). If implemented, the new recommendation could demand that DeFi platforms find the means of implementing KYC rules. A notable issue that has emerged from the FATF guidance is that decentralized governance does not necessarily imply immunity from regulatory scrutiny.

Thus, both decentralized and centralized crypt projects will be under immense pressure to comply with the same AML/CTF requirements applicable to traditional FIs (Naheem, 2020). Therefore, the UAE should now direct attention to the development of DeFi regulatory frameworks that will be consistent with the FATF guidance. However, the FTFT guidance has provides a broader definition of VASPs, which will ultimately create legislative challenges. DeFi controllers are more likely to push back against legislative efforts instead of embracing regulations that may come out (Elrifai, 2021).

Second, non-fungible tokens (NFTs) represent another area of legislative uncertainty in the UAE. The current UAE regulations are both unclear and uncertain about the status of NFTs, including their characterization in either the existing or new regulatory frameworks. Although NFTs have multiple applications, they are considered the digital answer to collectibles (El Maknouzi and Sadok, 2021). Unlike Bitcoin and cryptocurrencies, NFTs are specific to artwork rather than digital shares or currencies. A key question is whether NFTs should be subject to the same regulations applicable to other crypto assets. The question is crucial because NFTs are increasingly contravening consumer protection laws and intellectual property law. Concerns are mounting over the possibility of using NFTs as a gateway for money laundering considering the exorbitant amounts flowing through the NFT market (Kerr and England, 2022). The regulation of the NFT market is imminent given the possibility that criminals could be using NFT transactions to circumvent AML/CTF regulations. However, legal implications are murky for NFT ownership, and it could take time to develop a coherent policy framework.

The 2021 FATF guidance also covers NFTs. The FATF 2021 guidance does not consider NFTs to be VAs under its definition. Furthermore, the new guidance does not identify issuers of NFTs as VASPs. However, the FATF encourages regulators to "consider the nature of the NFT and its function in practice and not what terminology or marketing terms are used" like in the case DeFi (Hadef and Partners, 2021). FATF's recommendations toward NFTs are seemingly not as comprehensive as the guidance for DeFi and stablecoins. People buy NFTs for two different reasons: the intrinsic connection to an artwork or artist and investment purposes because of the potential increase in their future prices. The lack of an expansive approach to NFTs creates a regulatory challenge, especially for people who buy NFTs because of the connection with the artist or artistic work (Elrifai, 2021). The purchase of NFTs for investment purposes presents a potential area for possible regulations. Thus, the language of "investment purposes" rather than that of "collectibles" will likely influence stricter regulations. The UAE must now more to provide legal clarity o NFTs as soon as it is feasible because of the growing focus on luxury art and goods.

Third, fragmentation of laws and regulations that govern crypto assets is a prominent problem in the UAE. Cryptocurrency regulations in the UAE fall into three categories: Onshore UAE, DIFC and ADGM. Of the three, ADGM is the only jurisdiction that has issued far-reaching regulatory framework for regulating cryptocurrencies and related assets. The DIFC started to regulate cryptocurrencies as recent as 2021. Comparatively, regulations that cover Onshore UAE are still in their infancy stages. Thus, Abu Dhabi is the only Emirate with a robust legislative framework, although these regulations cannot be applied nationally. The situation creates a legislative gap characterized by high levels of fragmentation and piecemeal application of the law. Consider the case where Dubai and Abu Dhabi usually have competing and overlapping laws, which undermines enforcement and effectiveness. The issue is concerning because Dubai and Abu Dhabi are autonomous Emiratis with distinct civil, financial and commercial legal regimes.

The Federal Decree-law No. 20 of 2018 and the Cabinet Resolution No. 10 of 2019 are two important legislative instruments that could offer the needed harmonization. The Federal

Decree-law No. 20 of 2018 on Anti Money Laundering, Combating the Financing of Terrorism and Financing of Illegal Organizations (or the AML Law) was amended in September 2021. The amendment created a new group of institutions, specifically VASPs, that need to be compliant with the AML Law. The amended AML Law also prohibits legal or natural persons from engaging in the activities of VASPs or any other financial activities without a valid license, registration, or entry. The authorization should be from competent regulatory authorities (El Maknouzi and Sadok, 2021; Hadef and Partners, 2021). The amendment AML Law is essential because VASPs and crypto exchanges have been operating with significantly less regulatory scrutiny. Despite the progress being made, the amended AML Law is not complete considering that the pace of crypto development and adoption often outrun that of legislative reforms (Elrifai, 2021).

The problem of fragmentation is a global one. The regulatory regime is not only fragmented in the UAE, but it is also a global phenomenon. Consider the case where the UAE does not have a formal framework but rather a patch work of regulations across the seven Emirates. Similarly, there is no uniform regulations that govern cryptocurrencies and crypto assets across the globe. For example, some countries have outrightly banned trading in cryptocurrencies while others are open to and supporting the adoption of blockchain and crypto assets. Complete/total restriction is no longer a feasible approach since cryptocurrencies and blockchain technology continues to evolve at a high speed, with crypto markets successfully navigating the stringent regulations in some jurisdictions. The greatest challenge facing regulators is developing clear rules to regulate the complex word of cryptos while keeping pace with the speed of evolution. Hence, a global comparison of regulations may set the stage for ultimate harmonization of AML/CTF laws related to cryptocurrencies.

Cryptocurrency regulations: a global perspective

The USA has the largest share of cryptocurrencies, which makes it an ideal jurisdiction for global comparisons. Specifically, the USA is home to the highest number of crypto exchanges and investors, trading platforms, investment funds and crypto mining firms. Regulations covering cryptocurrencies are diverse and overlapping in the USA. The Treasurer's Financial Crimes Enforcement Network (FinCEN) has legalized cryptocurrency exchanges although the regulator does not consider cryptocurrencies to be a legal tender in the country (Naheem, 2020). The USA regulates cryptocurrencies under the regulatory scope of the Bank Secrecy Act, with legislation varying across states. The regulations require the providers of cryptocurrency exchange to register with FinCEN, keep the right records, implement an AML/CTF program and submit required reports to the relevant authorities. The FATF guidelines have a profound influence on the regulation of crypto assets in the USA. Specifically, the Treasury's FinCEN demands that all crypto exchanges comply with FATF's Travel Rule (United States Government Accountability Office, 2014).

The USA shares the same fragmentation problem with the UAE when it comes to the regulation of crypto assets. The Securities and Exchange Commission (SEC) is perhaps the most powerful regulator in the USA. However, the Treasury's FinCEN, the Commodity Futures Trading Commission (CFTC) and the Federal Reserve Board have oversight over crypto exchanges in the USA. The interpretation and guidance differ across the organizations. For instance, the SEC often views cryptos as securities; the CFTC defines Bitcoin as a commodity and the Treasury calls Bitcoin a currency (Haar, 2022). The variations in definition and guidance have inadvertently created a muddied regulatory framework. States also have their own regulations and law although they are neither visible nor clear. As such, a consistent legal framework is difficult to find at the state level. The

Justice Department has instead assumed a leadership role in developing cryptocurrency regulations of the future through coordination with both the SEC and CFTC. The Congress has also been setting new laws and rules that reinforce compliance with AML/CTF reporting and record-keeping obligations (Haar, 2022).

Unlike the UAE, the regulation of cryptocurrencies is under the influence of the legislature in the USA. Both the US Government agencies and lawmakers have taken a keen interest in the founding principles of cryptocurrencies: decentralized and unregulated. The direction of the legislation depends on the administration in power. For instance, the Biden Administration has proposed sweeping legislations that will increase the scope of regulating cryptocurrencies (Haar, 2022). Nonetheless, the USA suffers from high levels of political polarization and radicalization that often derail progressive efforts. Consider the case where lawmakers prefer decentralization and limited government involvement. Nevertheless, legislators are also keen on developing regulatory guidance to protect investors in the wake of high cases of criminal activity involving cryptocurrencies. Despite these challenges, the end game of the US regulations is to make it extremely hard for criminals to use cryptocurrencies to perpetrate tax evasion and illicit activities. The achievement of this objective is indeed critical although lawmakers continue to send mixed messages about the cryptocurrency regulations (United States Government Accountability Office, 2014).

The EU classifies crypto assets and cryptocurrencies as qualified financial instruments (QFis). The EU does not have a uniform AML/CTF regulatory framework for crypto assets and cryptocurrencies. On the contrary, AML/CTF regulations may vary across member states. Crypto is generally legal across the EU although the level of adoption and compliance depends on the regulations of the member states. Compliance with the regulations that govern cryptocurrency exchanges may also vary with the European Commission, European Banking Authority, European Central Bank, European Supervisory Authority for Securities and European Insurance and Pension (European Parliament, 2022). Cryptocurrency exchanges dealing in QFis operate under regulations enacted at the regional levels. Firms can use the existing QFis licenses to provide cryptocurrency-related products and services. However, these firms must comply with a raft of EU cryptocurrency rules and regulations, such as AML/CTF, AML Directives (AMLD), the Second Electronic Money Directive, Central Registration Depository/Capital Requirements Regulation and others.

Some countries in the EU have independent regulators that provide registration requirements for exchanges. For instance, Germany has the Financial Supervisory Authority (BaFin), France has Autorité des Marchés Financiers, and Italy has the Ministry of Finance as their primary regulators. The three regulators grant authorizations and licenses that can be used as passport exchanges, allowing the license holders to operate under a single legislative regime across the entire EU bloc. AMLD are central to the EU legislative framework. The European Parliament periodically issues the AMLDs with the goal of preventing money laundering and terrorist financing. The other important objective of the AMLDs is to create a consistent regulatory environment in the EU (Covolo, 2020). Fragmentation of laws across EU member states has created AML compliance gaps that are hindering efforts to addressing emerging money laundering and terrorist financing activities. Thus, the AMLDs have set the stage for harmonization, which remains elusive in the UAE and the USA.

Members of the European Parliament (MEPs) drawn from the Committee on Civil Liberties and Committee on Economic and Monetary Affairs unanimously agreed to strengthen AML/CTF efforts through by issuing a draft legislation in March 2022. The MEPs drafted the legislation in response to the absence of rules and guidance for tracing the transfer of crypto assets. Thus, the aim of the draft legislation is to enhance the traceability of crypto assets like in the case of traditional money transfers (European Parliament, 2022). If implemented, it will be mandatory to disclose information about the source and beneficiary of transactions during the exchange of crypto assets. The information should be forwarded to the competent authorities. The goal of the new regulations is to trace and block suspicious transactions. The proposed rules are critical, as there is no EU rules or regulations that allow the tracing of crypto-asset transfers (European Parliament, 2022). Thus, the new proposal, if enacted, will strengthen AML/CTF regulations in the EU. Conversely, the law is unclear about the specific crypto assets that will be covered, including DeFi and NFTs.

Conclusion and future directions

The regulation of crypto assets and cryptocurrencies is a murky are in the field of AML and CTF. Blockchain and cryptocurrency are novel technologies that continue to evolve at unprecedented speeds. Regulators face the challenge of developing robust legislative frameworks that will keep up with the pace of technological developments. The UAE has assumed a leading role in regulating crypto assets to bolster AML/CTF efforts. However, the existing legislative frameworks are fragmented with no possibility of harmonization in sight. The problem of fragmentation also pervades regulations being implemented in the USA and across the EU. A key observation from the analysis is the existence of multiple autonomous entities responsible for regulating crypto assets in the UAE, USA and EU. Although FATF guidance is an international standard for AML/CTF regulations, the approach differs significantly across the countries. The UAE is keen about complying with the FATF regulations to avoid being blacklisted, but the current laws are either ineffective or inadequate to address all the security threats posed by the exchange of crypto assets.

The existing limitations call for a tailored approach to regulations instead of relying on general laws that lack clarity. Crypto assets are not static, but they instead evolve with emerging technology. Additionally, blockchain is a new technology that is largely still unexploited. A combination if these issues underscore the value of tailoring AML/CTF regulations to specific blockchain and cryptocurrency technologies. Each class of crypto assets offers unique benefits, complexities and challenges. As such, it will be impractical to create a single legislation or law that will cover all the crypto assets, including their diverse applications. As such, it is imperative to development a robust regulatory framework that will target the specific uses of crypto assets, such as investments, payments, derivatives and tax status. The achievement of this goal is essential given that the existing regulations emphasize the intersections of cryptocurrencies and fiat currency. The approach is commendable, but the application of cryptocurrencies is not restricted to the conversion of crypto assets into fiat currency. There is a growing trend where business entities and even government agencies are accepting cryptos as a mode of payment.

The growing acceptance of cryptocurrencies as a valid form of payment will ultimately see a reduction in the use of fiat currency to buy goods and services. The development will potentially provide a save haven for money laundering, especially if the exchange involves DeFi and NFTs. The borderless nature of digital currency and exchanges means that the existing laws and regulations are inadequate to address cross-border money laundering activities. Thus, there is an urgent need of harmonizing global regulations to ensure uniformity in applications. Consider the case where criminals living in countries with stringent laws may take advantage of the laxity in other countries to perpetrate acts of money laundering. A notable example is the increasing flow of crypto assets from Russia and China into the UAE, as the two countries have criminalized cryptocurrency exchanges. Therefore, it is of the essence to broaden and strengthen the mandate of FATF, which is the *de facto* regulator of money laundering and terrorist financing across the globe. The FATF has been playing an instrumental role in releasing new AML/CTF guidance, but the impact has been insignificant because of the ambivalent attitude of member states, jurisdictions and regional organizations.

In conclusion, the quest for harmonization should be a priority as the FATF works towards developing a global standard. The global standard will support a uniform application of AML/CTF laws and regulations related to cryptocurrencies and the blockchain technology. However, it is not enough to have a global standard considering the possibility of not being implemented across countries and regions. Instead, the FATF should revise the existing assessment methodologies that evaluate the level of compliance at the national level. the FATF will develop a uniform standard and then allow countries and regions to operationalize the regulations based on their unique circumstances and challenges. For instance, countries can use the FATF guidance and rules as the benchmark for developing national crypto AML/CTF regulations. The FATF should then assess progress and compliance based on the unique situation of each country to tailor corrective measures. The FATF framework should also include provisions for building the capacity of countries to address existing vulnerabilities in international and national financial systems.

References

Barone, R. and Masciandaro, D. (2019), “Cryptocurrency or usury? Crime and alternative money laundering techniques”, *European Journal of Law and Economics*, Vol. 47 No. 2, pp. 233-254, doi: 10.1007/s10657-019-09609-6.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L. and Serusi, S. (2021), “Cryptocurrency scams: analysis and perspectives”, *IEEE Access*, Vol. 9 No. 1, pp. 1-1, doi: 10.1109/ACCESS.2021.3123894.

Boggiano, K. (2021), “FATF guidance of NFT, DeFi and digital assets: void for vagueness?”, 12 April available at: www.law.com/legaltechnews/2021/04/12/fatf-guidance-of-nft-defi-and-digital-assets-void-for-vagueness/?slreturn=20220520051017

Brown, S.D. (2016), “Cryptocurrency and criminality: the bitcoin opportunity”, *The Police Journal: Theory, Practice and Principles*, Vol. 89 No. 4, pp. 327-339, doi: 10.1177/0032258X16658927.

Chainalysis Team (2022a), “Crypto crime trends for 2022: illicit transaction activity reaches all-time high in value, all-time low in share of all cryptocurrency activity”, 6 January, available at: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

Chainalysis Team (2022b), “DeFi takes on bigger role in money laundering but small group of centralized services still dominate”, 26 January, available at: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

Covolo, V. (2020), “The EU response to criminal misuse of cryptocurrencies: the young, already outdated 5th anti-money laundering directive”, *European Journal of Crime, Criminal Law and Criminal Justice*, 29 September, Vol. 28 No. 3, available at: https://brill.com/view/journals/eccl/28/3/article-p217_217.xml

Dupuis, D. and Gleason, K. (2021), “Money laundering with cryptocurrency: open doors and the regulatory dialectic”, *Journal of Financial Crime*, Vol. 28 No. 1, pp. 60-74, doi: 10.1108/JFC-06-2020-0113.

Dyntu, V. and Dykyi, O. (2019), “Cryptocurrency in the system of money laundering”, *Baltic Journal of Economic Studies*, Vol. 4 No. 5, pp. 75-81, doi: 10.30525/2256-0742/2018-4-5-75-81.

El Maknouzi, M.E.H. and Sadok, H. (2021), “Regulation of virtual currencies in the United Arab Emirates: accounting for the emerging public/private distinction”, *Development Studies Research*, Vol. 8 No. 1, pp. 346-355, doi: 10.1080/21665095.2021.1980413.

Elrifai, S.N. (2021), "The virtual currency regulation review: United Arab Emirates", 2 September, available at: https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/united-arab-emirates

European Parliament (2022), "Crypto assets: new rules to stop illicit flows in the EU", 31 March, available at: www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

Gump, A. (2022), "Dubai passes landmark law regulating virtual assets (including cryptocurrencies)", 9 March, available at: www.jdsupra.com/legalnews/dubai-passes-landmark-law-regulating-8666988/

Haar, R. (2022), "U.S. officials send mixed messages on crypto regulation. Here's what it all means for investors", 18 April, available at: https://time.com/nextadvisor/investing/cryptocurrency/crypto-regulation-talks-heat-up/'

Hadef and Partners (2021), "The future of crypto assets regulation in the UAE", 27 October, available at: www.lexology.com/library/detail.aspx?g=88c0f35c-7ea5-439b-90d7-df3fe4f70586%20https://www.coinfirm.com/blog/uae-crypto-regulations/

Jones, B. (2022), "FATF's take on digital assets: updated guidance and recommendations", 25 February, available at: www.jdsupra.com/legalnews/fatf-s-take-on-digital-assets-updated-7477968/

Kerr, S. and England, A. (2022), "UAE steps up anti-dirty money measures to avoid global watchlist", 16 January, available at: www.ft.com/content/cc8242a9-8f11-4b7f-88d9-32dde3a7fbca

Moss, E. (2021), "Fighting money laundering on the new front of decentralized finance", 3 December, available at: https://internationalbanker.com/finance/fighting-money-laundering-on-the-new-front-of-decentralized-finance/

Naheem, M.A. (2020), "Presenting a legal and regulatory analysis of the United Arab Emirates' past, present and future legislation on combating money laundering (ML) and terrorist financing (TF)", *Journal of Money Laundering Control*, Vol. 1, doi: 10.1108/JMLC-08-2017-0038.

Shapiro, D. (2018), "Taxation and regulation in decentralized exchanges", *Journal of Taxation of Investments*, Vol. 36 No. 1, pp. 3-13.

Shevchenko, A. (2022), "Binance sued for allegedly facilitating money laundering with 'lax KYC'", available at: https://cointelegraph.com/news/binance-sued-for-allegedly-facilitating-money-laundering-with-lax-kyc

United Nations Office on Drugs and Crime (2022), "Money laundering", available at: www.unodc.org/unodc/en/money-laundering/overview.html

United States Government Accountability Office (2014), "Virtual currencies: emerging regulatory, enforcement, and consumer protection challenges", 29 May, available at: http://gao.gov/assets/670/663678.pdf

Corresponding author
Tareq Na'el Al-Tawil can be contacted at: dr.tareqaltawil@yahoo.com