

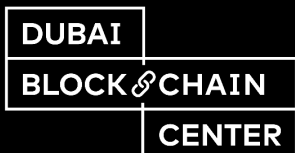


MENA FINTECH
ASSOCIATION

REGULATIONS SIMPLIFIED

A REPORT ON THE REGULATORY FRAMEWORK
OF CRYPTO ASSET ACTIVITIES IN ADGM

Powered by:



LETTER FROM THE AUTHORS

More often than not, what decides the fate of the ones being 'regulated' is not the law or the regulation itself but a regulator who chooses to listen, grow, and even change when needed; we are pleased that ADGM has done just that. Following through, we have extensively analysed the existing OCAB framework that emerged as a result of ADGM's thorough consultations and reVisions of the rules and regulations.

Under this framework, ADGM classified digital assets into Digital Securities, Crypto Assets, Fiat Tokens, derivatives/funds of digital assets, and digital assets.

This report illustrates the regulatory approach of the OCAB framework towards the nature and purpose of digital assets, as well as explains the process of setting up and Operating a crypto asset business, including licensing structures and regulatory compliance, especially regarding new digital asset initiatives in the MENA region.

The report also addresses the regulators' approach to technology governance and disclosure. We aim to simplify regulations so that both the regulated and the regulator may converge in making the world a more tech-driven place.

We hope you find the report to be a pleasant read!

KARM Legal Consultants

Kokila Alagh

Founder
kokila@karmadv.com

Soumya George

Principal Associate
soumya@karmadv.com

Akshata Namjoshi

Senior Associate
akshata@karmadv.com

Dr. Marwan Alzarouni


Founder, Accelliance Consultancy LTD
marwan.alzarouni@accelliance.com

This report is a copyright of KARM Legal Consultants. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of KARM Legal Consultants. For any assistance or clarification, please connect with us at admin@karmadv.com or hello@mena-fintech.org, or visit our website at www.karmadv.com or <https://www.mena-fintech.org>



FOREWORD

FROM THE CHAIRMAN



When we first introduced a policy and governance vertical in the Mena Fintech Association, our aim was to create a gateway between the history and Vision of policy and governance. We intend to continue deep-diving into nuances of tech policy to find the right synergy for conducive regulation of frontier technologies.

With multiple blockchain initiatives sprouting across the MENA region, it is only natural that the community paces fast towards blockchain adoption. One of the first regulators in the region, ADGM, has been the new-age regulator that opted to listen, grow and, adapt when needed.

In the same stride, this report analyses and simplifies the OCAB framework introduced by ADGM so that both the regulated and the regulator can come together and create a more tech-driven world.

Nameer Khan

Chairman

MENA Fintech Association

nameer@mena-fintech.org

INTRO- DUCTION

Digital Assets based on blockchain and DLT technologies, like Bitcoin and Ether, have revolutionised the world of payments, fund-raising, and asset ownership.

ADGM has been one of the first regional regulators to issue extensive regulations to address matters relating to digital assets. The Financial Services Regulatory Authority (FSRA), the financial regulator in ADGM, was the first in the MENA region to publicly support the development of certain digital assets through the amendments to its rules and regulations, further explained through the 'Guidance on Regulation of Crypto Asset Activities' in ADGM (as amended and updated on 14 May 2019 — 'Crypto Asset Guidance') and the 'Guidance on Regulation of Initial Coin/Token Offerings and Virtual Currencies' (as amended and updated on 5 May 2019).

The 'Crypto Asset Guidance,' read in conjunction with other ADGM rules and regulations governing digital assets and related activities, is being Referred to as the 'OCAB framework.'

The OCAB framework was issued and overlooked by the Financial Services Regulatory Authority (FSRA), which is the regulatory arm of ADGM. The FSRA is the regulator that issues Licenses and regulates entities Operating a crypto asset business within and from ADGM.

THE REGULATORY APPROACH

As a cognizant regulator, ADGM hosted a consultation with private and industry players prior to implementing an extensive regulatory regime (vide amendments to the existing rules and issuance of explanatory guidance note) on the varied types of digital assets.

The effective consultation process ensured that the key risks associated with this industry, including issues surrounding consumer protection, safe custody, technology governance, disclosure, and transparency have been extensively addressed under the OCAB framework.

As such, it is pertinent to note that most regulators around the world, who have taken a regulatory stance on the subject, have responded by the creation of one or a combination of the following:

A

Application of Existing Regulations:

Many regulators worldwide have, prior to taking a definitive stance on regulation, tried to bring it under the umbrella of existing laws e.g. Australia's Information sheet (INFO 225) on ICOs and Cryptocurrency.

B

Retrofitted Regulation:

Jurisdictions have also committed amendments to existing laws to cover the requirements of regulating digital assets. E.g. Estonia's Amendment to Money Laundering Act and Terrorism Financing Prevention Act, and Bahrain Central Bank's addition of a 'Crypto Assets' Module in the Capital Markets volume of its rulebook.

C

New Regulation/Regime:

Some jurisdictions have come out with new laws or regulations enacted specifically to regulate digital asset activities. E.g. Malta enacted the Virtual Financial Assets Act in 2018.

In comparison to other jurisdictions, ADGM has taken a safe yet counterintuitive approach. Though it may not have necessarily enacted new legislation to address digital asset activities, they made a **retrofitted approach** to regulate the issuance of digital assets and associated activities in its existing framework. They also introduced a new activity of Operating a crypto asset business. Nonetheless, through their Guidance Notes, regulators further provided guidance on how certain digital assets may be regulated, clarifying that some of them are already part of their existing framework.

Source: Blandin, Apolline, et al. "GLOBAL CRYPTOASSET REGULATORY LANDSCAPE STUDY." Cambridge Centre for Alternative Finance.

www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf



FRAME- WORK ON DIGITAL ASSETS

The advent of Bitcoin and its related uses also brought to the fore, benefits and risks associated with the new-age tokens.

The nature and purpose of these tokens or digital assets are also varied and hence, it is often difficult to regulate them the same way. While analyzing the nature of the digital assets, the question is often whether such token is a 'Security Token', and the Howey Test adopted by the US, appears to be the most commonly discussed test.

However, at a regulatory level, the credit largely goes to Switzerland's FINMA for being the first to come up with their own nomenclature of tokens i.e. Payment tokens/cryptocurrencies, utility tokens, and asset tokens. Many other jurisdictions from around the world have established their own classifications, with nomenclatures ranging from – virtual assets, Crypto Assets, digital assets, and so on.

Under the OCAB framework the Digital Assets have been classified into :

(i) Digital Securities; (ii) Crypto Assets; (iii) Fiat Tokens; (iv) Derivatives/ Funds of Digital Assets; and (v) Other Digital Assets.

1. DIGITAL SECURITIES NÉ SECURITY TOKENS

Unlike the Howey-Test adopted by the US SEC, ADGM does not currently have a test to determine whether or not a token qualifies as a Security. The FSRA deems that if digital or virtual tokens are considered a Security under the Financial Services and Markets Regulations 2015 (FSMR), they may be referred to as Digital Securities. Generally, for a token to be deemed a Security, it should exhibit the characteristics or features of a Share, Debenture, or Units in a Fund.

Deemed as Securities under the law, the issuance of Digital Securities would be required to comply with all requirements for Offers of Securities to the Public under Chapter 4 of the Markets Rules, which would, among others, include the obligation to publish a prospectus unless such an offer may be categorised as an 'Exempt Offer.'

Since Digital Securities or Security Tokens are treated as Securities, they will have to be traded in Recognized Investment Exchanges. The technological infrastructure of an exchange that permits the trading of Digital Securities would have to resemble an exchange that allows for the trading of Crypto Assets/cryptocurrencies.

In accordance thereof, the OCAB framework recognises that a Licensed Crypto Asset Exchange may also operate as a recognised investment exchange after relinquishing its financial services permission (FSP) to act as a Crypto Asset Exchange (unless the recognition order includes a stipulation that it may also operate as a Crypto Asset Exchange).

2.

CRYPTO ASSETS & ACCEPTED CRYPTO-ASSETS

Under the OCAB framework, a crypto asset is defined as a digital representation of value that can be digitally traded, and functions as: (a) a medium of exchange; and/or b) a unit of account; and/or c) a store of value, but does not have legal tender status in any jurisdiction. A Crypto Asset is: (a) neither issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and (b) distinguished from Fiat Currency and E-money.

The subject of cryptocurrencies and virtual currencies has been scrutinised by various policymakers and regulators, each of whom has touched upon the subject in different ways. To illustrate:

(i) European Central Bank Approach: The ECB, in its 2015 report titled 'Virtual Currency Scheme,' defined virtual currencies as digital representations of value, not issued by a central bank, credit institution, or e-money institution, which in some circumstances can be used as an alternative to money.

(ii) International Monetary Fund (IMF) approach: The IMF recognised virtual currencies as digital representations of value, issued by private developers and denominated in their own unit of account. It recognises that virtual currencies are digital representations of value but differ from other digital currencies, such as e-money, which is a digital payment mechanism for and denominated in fiat currency.

(iii) World Bank approach: The World Bank classified cryptocurrencies as a subset of digital currencies, which it defines as digital representations of value that are denominated in their own unit of account distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money.

Contrary to most other policymakers, the World Bank has also defined cryptocurrencies as digital currencies that rely on cryptographic techniques to achieve consensus

(iv) Financial Action Task Force (FATF)

Approach: The FATF regards cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but do not have legal tender status (i.e. when tendered to a creditor, are a valid and legal offer of payment) in any jurisdiction.

It further states that virtual currency is distinguished from fiat currency, which is the

coin and paper money of a country that is designated as its legal tender, and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency, i.e. electronically transfers money that has legal tender status.

As is evident from the above, the definition of crypto asset under the OCAB framework is strongly influenced by the FATF definition.

However, one of the most path-breaking approaches of ADGM in this regard has been the introduction of the Accepted Crypto Assets concept, on par with Mexico and Thailand. Accepted Crypto Assets are those that have been accepted and approved by the regulator in ADGM. Unlike the Thai SEC, which has announced that only Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum Classic (ETC), Ethereum (ETH), Litecoin (LTC), Ripple (XRP), and Stellar (XLM) will fall under the category of accepted Crypto Assets, ADGM has not released a public list of accepted Crypto Assets.

Applicants applying to undertake any of the regulated activities will need to have the details of each accepted crypto asset that is proposed to be used for the conduct of their regulated activities. Each crypto asset must satisfy various determining factors to be approved, which include Security features, traceability, exchange connectivity, efficiency, type of distributed ledger, functionality etc. It is important to note that an accepted crypto asset for one License Holder may not be approved for another Licensee.

3.

FIAT TOKENS OR STABLE COINS

Although the term has been extensively utilised by market players since 2018, there was no legislative clarity on the interpretation of sTablecoins. Despite being a revolutionary concept, cryptocurrencies are still not being widely accepted. One of the key reasons for this is the high level of price fluctuation surrounding Crypto Assets; sTablecoins are expected to address this issue. sTablecoins are cryptocurrencies whose value is usually pegged to a currency or exchange-traded commodities such as precious metals or industrial metals. To elaborate, sTablecoins may be of any of the following types:

- (a) Fiat-Backed sTablecoins** - Backed by a fiat currency and the most widespread example of this is Tether.
- (b) Commodity-Backed sTablecoins** - This category of sTablecoins is backed by commodities like gold, precious metals, agricultural produce, oil, etc.
- (c) Cryptocurrency-Backed sTablecoins** - Crypto-Backed sTablecoins are coins backed by other digital currencies, usually top-ranked cryptocurrencies with large market capitalisation such as Bitcoin (BTC) or Ether (ETH).
- (d) Non-Collateralised sTablecoins** - This category of digital currency is not backed by any real-world or Cryptocurrency asset. Instead, price stability is achieved algorithmically by expanding and contracting the coin's circulating supply in response to market behaviour. If the price of the sTablecoin begins falling beneath its peg, the system will reduce the supply of coins in circulation, thereby increasing demand – and value – for the remaining coins. On the other hand, if the price of the sTablecoin climbs above its peg, the algorithm will release more coins into circulation, effectively devaluing each individual coin.

ADGM is the first regulator to have recognised the concept of sTablecoins through crypto asset guidance. However, though, the guidance recognises the multiple types of sTablecoins prevalent in the market, FSRA has confirmed that it will only permit a fully backed 1:1 fiat token, i.e backed only by the same fiat currency it purports to be tokenising. Thus, Fiat Tokens are to be treated as a mechanism for storing value (e.g. e-money) and is to be treated as a digital representation of a fiat currency

Considering the sTablecoins that are approved by FSRA are limited to fiat-backed sTablecoins (aka Fiat Tokens), the OCAB framework has clarified that:

- (a)** The Issuer of a Fiat Token would be required to obtain a Financial Services Permission (FSP) for conducting Money Transmission Services
- (b)** Custodian of Fiat Token would be required to obtain an FSP for acting as a Fiat Custodian. To clarify further, such entities do not require a License to undertake a crypto asset activity. Interestingly, a crypto custodian, which may provide custody services over both Fiat Tokens and Crypto Assets requires an FSP to act as crypto custodian only. An exchange which utilises:
 - (i)** its own Fiat Tokens as a payment/transaction mechanism solely within its own platform/ecosystem; or
 - (ii)** uses third-party-issued Fiat Tokens as a payment/transaction mechanism that is required to be Licensed as Crypto Exchange only.

However, in all cases, the Fiat Token must be able to demonstrate that it fulfils the same requirements of an Accepted Crypto Asset under the OCAB framework.

OTHER CATEGORIES OF DIGITAL ASSETS

Under the OCAB framework, any Derivative and Collective Investment Funds of Crypto Assets, Digital Securities, and Utility Tokens would be regulated under the FSMR as a Specified Investment. To the extent necessary, the regulations applicable to a fund would also apply in such cases.

Accordingly, any market operators or market intermediaries dealing or managing investments in Derivative and Collective Investment Funds of Crypto Assets, Digital Securities, and Utility Tokens will be subject to the appropriate regulations and rules applicable under FSMR and may need to be approved by FSRA as FSP Holders, Recognised Investment Exchanges, or Recognised Clearing Houses, as applicable.

Lastly, the OCAB framework recognises Utility Tokens as tokens that may be redeemed for access to a specific product or service, typically provided using a DLT platform, do not exhibit the features and characteristics of a regulated investment/instrument under the FSMR. To the extent that these tokens do not constitute Accepted Crypto Assets, these tokens, are not regulated by the FSRA.



OPERATING A CRYPTO ASSET BUSINESS

Licensed Activities:

The OCAB framework introduced a new regulated activity – Operating a Crypto Asset Business (OCAB) – and any person who proposes to carry out such activity requires an FSP from the FSRA. An OCAB licence Holder (‘OCAB Holder’) is permitted to engage in activities relating to Accepted Crypto Assets only. The following Table enumerates the activities which require and are excluded from the need to obtain an OCAB licence.

Table 1

Activities Requiring the OCAB License	Activities Excluded from the OCAB License
<ul style="list-style-type: none"> Buying, Selling, or exercising any right in accepted Crypto Assets (whETHER as principal or agent); 	<ul style="list-style-type: none"> The creation or administration of Crypto Assets that are not accepted Crypto Assets;
<ul style="list-style-type: none"> Managing accepted Crypto Assets belonging to another person; 	<ul style="list-style-type: none"> The development, dissemination, or use of software for the purpose of creating or mining a crypto asset
<ul style="list-style-type: none"> Making arrangements with a view to another person (whETHER as principal or agent). Buying, Selling, or providing custody of Accepted Crypto Assets; 	<ul style="list-style-type: none"> The transmission of Crypto Assets
<ul style="list-style-type: none"> Marketing of accepted Crypto Assets; 	<ul style="list-style-type: none"> A loyalty points scheme denominated in crypto assets; or
<ul style="list-style-type: none"> Advising on the merits of Buying or Selling of accepted Crypto Assets or any rights conferred by such Buying or Selling; and 	<ul style="list-style-type: none"> Any other activity or arrangement that is deemed by the FSRA to not constitute Operating a crypto asset business.
<ul style="list-style-type: none"> Operating as a Crypto Asset Exchange; or as a Crypto Asset Custodian 	

Licence Application:

Crypto Asset Guidance has clarified that applicants for the OCAB licence must be prepared to engage extensively with the FSRA, both during the application process and thereafter. Hence, the guidance recommends that the applicants appoint compliance advisers, with the appropriate skills, knowledge, and experience to provide the requisite assistance throughout the application process.

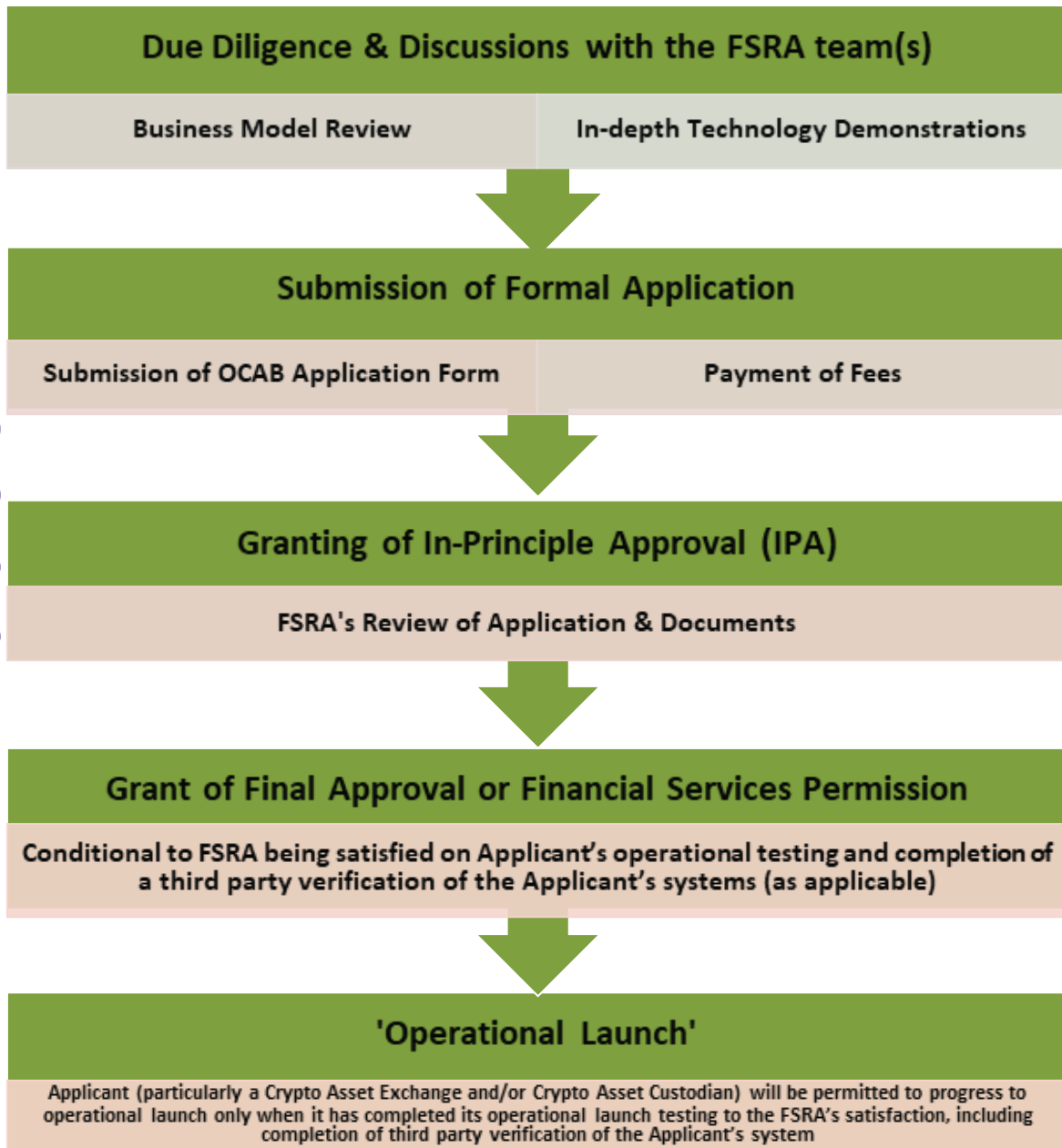
The fees for the application and the ongoing annual superVision varies based on the activity proposed to be undertaken (Refer to Table 2). Additionally, a Crypto Asset Exchange

Table 2

Activity	Application Fees	Annual SuperVision Fee
Non-Custody OCAB intermediary activities only	\$20,000	\$15,000
Crypto asset custodian and non-custody OCAB intermediary activities	\$40,000	\$30,000
Crypto asset exchange	\$125,000	\$60,000
Crypto asset exchange and crypto asset custodian	\$145,000	\$75,000

As elaborated, the application comprises a five-stage process. Refer to Table 3 for clarity on the process flow.

Table 3





REGULATORY COMPLIANCE FOR OCAB HOLDERS

In addition to the regulatory capital requirements, the OCAB framework mandates that an OCAB Holder should have a robust technological set-up as well as mechanisms and measures to comply with the FSRA's rules and regulations on Anti Money Laundering and countering financing of terrorism.

1. Anti-money laundering:

FSRA has been closely monitoring international developments surrounding Anti-money Laundering laws, including the recent statements by the FATF relating to the risks associated with digital asset activities. Under FSRA regulations, OCAB Holders are mandated to adopt a risk-based approach. In order to implement the risk-based approach, OCAB Holders are expected to have processes in place to identify, assess, monitor, manage, and mitigate money-laundering risks. Sufficient resources are expected to be allocated for this purpose and periodic risk assessments are to be undertaken by OCAB Holders.

The OCAB Holder should have a Money Laundering Reporting Officer who is responsible for its compliance with AML Rules. However, the knowledge and awareness of the managerial personnel with respect to the business and technical risks arising out of a crypto business, including the possible use of Crypto Assets in illegal and criminal activities is crucial. The framework notes that one of the key risks that must be addressed is the risk associated with the on-boarding of a customer.

FSRA has strictly advised OCAB Holders to refrain from following a simplified Customer Due- Diligence.

In this respect, OCAB Holders are expected to have in place Customer Risk Assessment and Customer Due Diligence (CDD) policies and procedures. Also, for non-face-to-face on-boarding, OCAB Holders must have means to ascertain the correct identification of a Client as a natural person, including the obtaining of a joint selfie with two currently valid forms of the client's facial ID, one of which must be the passport and the second a copy of an official government-issued document. OCAB Holders shall obtain signed self-certifications from the clients identifying the details of all passports issued and held in their name(s). The self-certification may also be used to capture tax-related obligations of the customer. In this respect, it is important to highlight that since OCAB Holders would be collecting information relating to private individuals, an OCAB Holder must comply with ADGM Data Protection Regulations 2015.

In addition to the measures associated with customer on-boarding, it is expected that the transactions of a customer also be closely monitored. Therefore, OCAB Holders are expected to develop, implement, and maintain effective systems to monitor a transaction undertaken by a customer.

The OCAB Holder should have systems in place to determine the origin of a crypto asset and monitor its destination as well as apply strong 'know your transaction' measures. Consequently, strong internal processes are required to be implemented that may assist in identifying the illegal use of accepted Crypto Assets.

OCAB Holders may seek to utilise their own or third-party technologies and solutions available in the market to meet their regulatory obligations (e.g. those associated with customer risk assessment, detection of fraud as well as transaction identification, monitoring, and reporting) and risk management requirements (e.g. margin limits and large exposure monitoring).

Cash transactions pose a significant risk due to the difficulty in determining their source. Hence, OCAB Holders wishing to conduct cash transactions will be required to implement enhanced controls to mitigate the inherent risks of such transactions. Such controls include setting appropriate limits on cash deposits (e.g. daily, monthly, or yearly limits), a prohibition on receiving direct cash or the receipt of cash other than from bank accounts, and prohibitions on receiving funds from third parties.

Further, the FSRA does not consider it appropriate for OCAB Holders to accept deposits by way of credit cards or credit facilities/credit lines.

OCAB Holders are required to have processes in place that enable them to disclose, prior to entering into an initial transaction, all material risks to their clients in a manner that is clear, fair, and not misleading. An OCAB Holder is required to develop, implement, and adhere to a Crypto Asset Compliance Policy, tailored to meet specific crypto asset business compliance requirements, and reflecting a clear comprehension of the OCAB Holder's understanding of its compliance responsibilities.

Prior to commencing operations, OCAB Holders are expected to establish online connectivity with the UAE's Financial Intelligence Unit for the purposes of submitting Suspicious Activity Reports (SAR)

2. Technology Governance

OCAB Holders are obligated to implement robust measures for technology governance and controls. Specifically, OCAB Holders would be required to have technology governance and controls with

a focus on crypto asset wallets, private keys, origin and destination of crypto asset funds, Security, and risk management.

From a technical perspective, due attention should be given to maintenance and development of systems and architecture, Security measures, procedures for safe storage and transmission of data, processes specifying management of personnel and decision making and procedures for the creation and management of services, interfaces, and channels provided by or to third parties. With respect to each of these aspects, detailed policies and procedures are required to be put in place and implemented.

System/software updates/upgrades are also expected to be tested for technical, operational, and Security vulnerabilities, including but not limited to functional, penetration and stress testing. The outcome of such testing should be well-structured and -documented and signed off by technology-focused executives of the OCAB Holder.

Third-party verifications/audits of core systems being used are to be conducted annually at the least.

Such audits should verify the custody arrangements and the amount of their purported holdings of Crypto Assets and Client Money. Crypto asset custodians and Crypto Asset Exchanges would also be required to have an annual review of their infrastructure, undertaken by reputable third-party, cybersecurity consultants.

Everyone in the crypto community is aware of the sudden passing of a Canadian exchange platform CEO that resulted in the permanent loss of approximately \$145 million worth of Crypto Assets in customer funds, due to the deceased being the only person with the passwords required to access the company's wallets. This incident highlighted the risks posed by concentrating the access of privileged or sensitive information to a single person. Without limiting this obligation, specifically, the IT infrastructures of Crypto Asset Exchange and Crypto Asset Custodian are expected to provide strong-layered Security and seek the elimination of single points of failure. The infrastructure is expected to be strong enough to prevent accidental destruction or breach of data, collusion or leakage of information by employees/former employees, successful hack of a cryptographic and hardware Security module or server, or access by hackers of any single set of encryption/decryption keys that could

result in a complete system breach. As such ADGM has left no stone unturned to ensure that in case of such unforeseen events, there is a mechanism in place to ensure that investors remain protected.

An OCAB Holder is required to comply with the following:

- (a)** Have in place clear, well-documented, and transparent rules and procedures governing the use of open source software and detailing the software's stability, Security, and fitness for purpose
- (b)** Have robust procedures and protective measures to ensure the secure offline generation of keys, storage, backup, and destruction of both public and private keys for their own wallet operations and where they offer wallet services to clients.
- (c)** Consider the use of multi-signature wallets – or similar mechanism or procedures where the same may be not be possible.
- (d)** Implement procedures to cover due diligence on the deposits and withdrawals by legal persons that represent further multiple deposit Holders or withdrawal recipients of Crypto Assets. For such deposits and withdrawals, OCAB Holders should be able to assess the ultimate beneficiaries' wallet addresses and their source or destination of funds as appropriate.

(e) Have a programme of planned systems outages to provide for adequate opportunities to perform updates and tests and notifying clients of such outages.

(f) Maintain clear audit logs of decision making. Staff with decision-making responsibilities should have the adequate expertise, particularly from a technological standpoint, to make such decisions.

(g) Wherever public and private cloud service providers are used, such service providers should be thoroughly screened and a clear roles and responsibilities matrix must be implemented.

Many regulators in the world have not considered the possibility of protecting investors in case of fork. ADGM on the other hand has achieved that feat. As per the OCAB framework, the licence Holders are required to ensure that changes in the underlying protocol of a crypto asset that results in a fork are managed and tested proactively. This obligation includes managing any discrepancy between the balances recorded on the previous version versus the new version. Even in the case of a fork, the clients should be able to deposit and withdraw accepted Crypto Assets in and out of an OCAB Holders' infrastructure.

3. Other Obligations

In addition to what was mentioned, OCAB Holders have certain additional obligations under the OCAB framework, as listed below:

OCAB Holders should have processes to disclose to a Client all material risks associated with crypto transactions in a fair, clear, and not misleading manner. This is an ongoing obligation and should be undertaken not just at the time of on-boarding a Client but during the entire duration that the Client avails the services. The risk disclosures must be continually updated.

All communications, including advertising or investment materials or other publications, made by an authorised person, including an OCAB Holder, should be made in an appropriate manner and that an authorised person shall implement suitable policies and procedures to comply with the requirements of the FSMR

OCAB Holders are obligated to operate in substance within ADGM. Accordingly, they must commit resources within ADGM, including, but not limited to, commercial, governance, compliance/surveillance, operations, technical, IT, and HR functions.

(iv) OCAB Holders intending to operate solely as a broker or dealer for clients (including the operation of an OTC broking or dealing desk) are restricted from structuring their brokerage/dealing services or platform in such a way that would have it be considered as Operating a market/Crypto Asset Exchange. It may be highlighted that under the FSMR, a person does not operate a crypto asset exchange if it regards a facility which is merely an order-routing system where orders for Buying and Selling accepted Crypto Assets are merely transmitted but do not interact.

(v) OCAB Holders have also been advised to avoid transactional interaction with any infrastructure or services where a counterparty is unknown or anonymous (e.g. certain peer to peer or decentralised exchanges at any stage of the process within and outside of the OCAB Holders' core operations.

(vi) OCAB Holders as data controllers shall be responsible for determining the purpose for which, and the manner in which, personal data is processed.



SPECIALISED OCAB ACTIVITIES – CRYPTO ASSET EXCHANGE & CRYPTO CUSTODIAN

As per the regulations, Operating a Crypto Asset Exchange means the trading, conversion or exchange of:

(a) a Fiat Currency or other value into Accepted Crypto Assets; (b) an Accepted Crypto Assets into Fiat Currency or other value; or (c) one Accepted Crypto Asset into another Accepted Crypto Asset. However, a person is not deemed to operate a Crypto Asset Exchange if it operates a facility which is merely an order-routing system where orders for Buying and Selling Accepted Crypto Assets are merely transmitted but do not interact.

CONC- LUSION

Though the systems surrounding digital assets is here to stay, globally, the regulators are still analysing the regulatory approach that they wish to adopt. In the midst of this regulatory confusion, ADGM has embraced its position as a torchbearer in the GCC region and implemented robust structures to support the use of digital assets within the ADGM. The framework is designed to address the full range of risks associated with crypto asset activities, including risks relating to money laundering and financial crime, consumer-protection technology governance, custody, and exchange operations.

The FSRA has also addressed issues around technology governance, disclosure/transparency, market abuse, and the regulation of Crypto Asset Exchanges in a manner similar to the regulatory approach taken in relation to global Securities exchanges.

As an early adopter of the crypto asset regulatory framework in the GCC region, ADGM has shown its willingness and a keen interest in supporting this emerging technology. It would be interesting to see the overall impact of these regulatory developments on the crypto asset market in the UAE.
