Questions on Notice – response from the ADC Forum

At the hearing we were asked to present further information on the following:

- exchanges
- custody
- DAOs
- token mapping

Attached are a number of documents relating to these topics provided by our experts, who have played key roles in many of these projects.

1. Benchmarking Exercise: Regulatory Sandbox in other international financial centres
2. Financial Service Commission Mauritius: Consultation Paper on Custody of Digital Assets, November 2018
3. Financial Service Commission Mauritius: Guidance Note on Recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors
4. Bermuda Companies (Initial Coin Offering) Regulations 2018
5. Bermuda Monetary Authority: Consultation Paper on the Digital Asset Business Amendment Act 2020
6. Dr Jane Thomason, DAO Governance Post – LinkedIn
7. Dr Jane Thomason, 'DeFi - Who, what and how to regulate in a borderless, code governed world?'
8. Financial Service Commission Mauritius: Guidance Note on Securities Token Offerings (STOs), April 2019
9. Bermuda Monetary Authority: Consultation Paper on the Digital Asset Business Accounts Rules 2020
10. Financial Service Commission Mauritius: Digital Asset Market Place guidelines May 2021
11. Information on Serbia's Digital Asset Act 2021

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

BENCHMARKING EXERCISE: REGULATORY SANDBOX IN OTHER INTERNATIONAL FINANCIAL CENTRES

Differing approaches to the sandbox

1. The benchmarking exercise undertaken by the Committee was focussed on the sandbox frameworks in five (5) IFCs, namely Abu Dhabi, Australia, Dubai, Singapore and United Kingdom. In all these centres, the regulatory or supervisory sandboxes, all of which were dedicated to financial services, while having their specificities, shared common features including the aim to provide for a contained and controlled landscape in which firms conduct pilot of financial services and products involving emerging technology or innovative application of existing technology in a cost-effective and timely manner before being made available to the whole market.

2. The table below highlights the main features of the respective sandbox in the IFCs surveyed.

General Information		Name of Sandbox	Date launched	Type of Applicant		Benefits		Duration	Safeguards		
IFC	Regulator			Existing Licensees	New Applicants	Relaxed licensing obligations	Relaxed regulatory framework		Limitation on customer base/value	Additional reporting duties	Consumer Protection/ Risk Mediation
Abu Dhabi	Abu Dhabi Global Market	Regulatory Laboratory	2 November 2016	✓	✓	X	✓	2 years	✓	✓	✓
Australia	Australian Securities & Investments Commission	Regulatory Sandbox	December 2016	✓	✓	X	✓	12 months	X	X	✓
Dubai	Dubai Financial Services Authority	Innovation Testing License	06 March 2017	✓	✓	X	✓	6 to 12 months	✓	✓	✓
Singapore	Monetary Authority of Singapore	Regulatory Sandbox	June 2016	✓	✓	X	✓	12 months	✓	✓	✓
United Kingdom	Financial Conduct Authority	Regulatory Sandbox	9 May 2016	✓	✓	✓	✓	3 to 6 months	✓	✓	✓

Objectives of the sandboxes

3. In terms of the objectives of the sandboxes in the IFCs surveyed, it has been noted that these tend to vary based on the mandate of the regulator administering it. A common trait of all sandboxes was that they were attempting to strike the balance between promoting innovation, maintaining financial stability and protecting consumers of financial services. This was being done through the lowering of barriers to enable innovative financial services and products to be tested without the full cost of compliance with the licensing and regulatory requirements and while minimising the time taken for these innovative financial products and services to reach financial markets. Simultaneously adequate safeguards were being set up to mitigate related risks and protect customers.

Eligibility for participating in the sandbox

4. In all five sandboxes, to be admitted to the sandbox, the fundamental requirement is for proposed financial product or service to involve innovation through either the use of new or emerging technologies or existing technologies in an innovative manner to address existing problems or bring benefits to the industry. In addition, the applicant was required having adequate resources to develop its product or service, a detailed and feasible business plan and a product or service which was ready to be tested in the sandbox.

Safeguards

5. Across all IFCs sampled, it has been observed that appropriate safeguards have been put in place to mitigate the risks associated with the sandboxed product or service and to contain the possible consequences of live testing. These safeguards have taken the form of limitations of the scope of the live testing in terms of number and type of customers, duration and total value of the product or service. In some sandboxes, those safeguards extended to key risk management controls, for instance against cyberattacks and system disruptions as well as monitoring and reporting requirements. Other sandboxes placed more emphasis on customer protection measures by requiring dispute resolution and redress mechanisms, compensation arrangements and specific disclosure and consent requirements.

Key finding and conclusion

6. The key finding of this benchmarking exercise is that sandboxes are systematically under the administration of the financial services regulators.

7. In this respect, going forward, Vanuatu may consider whether the RSL should be transferred to the FSC and the BOV or whether both regulators should be statutorily empowered to set up their respective RSL framework while maintaining enhanced collaboration to ensure that there is no regulatory gap between their respective frameworks.

8. However, in the interim, the Committee's proposal for enhanced collaboration between the regulators in relation to sandboxed fintech activities may be considered for implementation.

BENCHMARKING EXERCISE: CRYPTOCURRENCIES ACROSS JURISDICTIONS

The table below regroups the divergent approaches of the countries surveyed[1] regarding treatment of virtual currencies from AML/CFT, taxation and licensing perspectives.

Country	AML/CFT	Taxation	Consumers: Advice or Warning	Intermediaries: Licensing or Registration	Financial Sector Warning or Bans	Bans on Issuance or Use
Australia	-	Clarified tax treatment	Consumer Warning	Plans on introducing new regulations	-	-
Canada	Amendment to existing regulations	Clarified tax treatment	Consumer Warning	-	-	-
China	-	-	-	-	Ban	-
France	Applying existing regulations	Clarified tax treatment	Consumer Warning	-	-	-
Japan	Plans on introducing new regulations	-	Consumer Warning	Plans on introducing new regulations	-	-
Singapore	Plans on introducing new regulations	Clarified tax treatment	Consumer Warning	-	-	-
South Africa	-	-	-	Plans on introducing new regulations	-	-
UK	Applying existing regulations	Clarified tax treatment	-	-	-	-

[1] Information collected from public sources on the internet is not necessarily indicative of all actions taken by each country. Source: Bloomberg (https://www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules)

Annex 1 – International Benchmark

In terms of international benchmark, the Malta, Singapore and Switzerland have been surveyed for their approaches to the treatment given to digital token offerings. As detailed below, Malta is in the process of creating a specific regulatory framework for ICOs and Virtual Currencies which Singapore and Switzerland have opted to apply their existing legislations.

A. Malta

Malta has been very proactive in setting up the legal framework for blockchain. The Malta Financial Services Authority (MFSA) floated a discussion paper[2] on Initial Coin Offerings, Virtual Currencies and related Service Providers on 30 November 2017. Thereafter, on 16 February 2018, the Office of the Prime Minister, issued a Consultation Paper in relation to the establishment of a Malta Digital Innovation Authority (MDIA) and the framework for the certification of Distributed Ledger Technology Platforms and related service providers[3]. The Consultation paper proposes three pieces of legislation, namely:

1. **The Malta Digital Innovation Authority Bill** which seeks to establish the MDIA the Joint Co-ordination Board (JCB) and its scope will be to ensure effective cooperation between MDIA and other National Competent Authorities (NCAs) in the area of technology uses. This Bill also seeks to establish the National Technology Ethics Committee (NTEC) which will ensure that the proper standards of ethics are reflected in the use of relevant Technology Arrangements and to guide other NCAs in Malta;

2. **Technology Arrangements and Service Providers Bill** setting out the set out the regime for the registration of Technology Service Providers (auditors and administrators of Technology Arrangements) and the certification of Technology Arrangements (DLT platforms and related smart contracts).; and

3. **Virtual Currencies Bill** which will provide the regulatory regime and framework for ICOs and for the provision of certain services related to virtual currencies. This regime will cover brokers, exchanges, wallet providers, advisors, wealth managers and market makers dealing in virtual currencies. This proposed legislation proposes to apply a "Financial Instrument Test" to issuers and/or persons offering ICOs conducted in or from Malta to determine whether an ICO is classified as a financial instrument in terms of existing investment services legislation such as the Markets in Financial Instruments Directive (MiFID). This "Financial Instrument Test" will have two stages. The first one being to determine whether a particular VC falls under European Union or Maltese existing legislation. The second stage would then determine whether the VC qualifies as an asset under this Bill. An affirmative determination during the first stage would not require the person undertaking the test to proceed to the second stage.

[2] The Discussion Paper may be accessed at: https://www.mfsa.com.mt/20171130_DiscussionPaperVCs
[3] The Consultation Paper may be accessed at: https://meae.gov.mt/en/Public_Consultations/OPM

B. Singapore

The approach taken by the Monetary Authority of Singapore[4] (MAS) has been the application of existing Securities Laws on Offers or Issues of Digital Tokens issued through ITOs. In this respect, MAS defines "digital tokens that constitute capital market products" as digital tokens representing equity in a corporation, a debenture of the issuer, or a unit in a CIS.

Any such digital tokens are required to comply with the applicable securities laws including, where appropriate, the filing of a prospectus prior to the token issue. The current exemptions to the prospectus requirements relate to small offer or personal offer not exceeding $5 million in any 12-month period, private placements to a maximum 50 persons within any 12-month period, an offer to institutional investors only and an offer to accredited investors. In addition, offers of units in a CIS are subject to authorisation or recognition requirements and to compliance with investment restrictions and business conduct requirements.

Regarding intermediaries facilitating the offer or issue of digital tokens, MAS has classified the following types which would need to be licensed unless otherwise exempted:

1. **Primary platform** operated by a person whereby one or more offerors of digital tokens may make primary offers or issues of digital tokens;

2. **Financial Adviser** providing financial advice in respect of any digital tokens which are investment products; and

3. **Trading Platform** operated by a person where digital tokens are traded. A person who operates a primary platform in Singapore in relation to digital tokens which constitute any type of capital markets products, may be carrying on business in one or more regulated activities under the SFA. Where the person is carrying on business in any regulated activity, or holds himself out as carrying on such business, he has to obtain a capital markets services licence for that regulated activity under the SFA, unless otherwise exempted.

MAS has also clarified that its AML/CFT regime is applicable to digital tokens and as such persons involved have to report suspicious transactions and ensure that they do not deal with or provide financial services to persons who are designated individuals or entities under the Terrorism (Suppression of Financing) Act.

MAS encourages persons who wish to offer digital tokens in Singapore or operate a platform involving digital tokens in Singapore to seek professional advice from qualified legal practitioners to ensure that their proposed activities are in compliance with all applicable laws, rules and regulations in Singapore.

It has been noted that a new payments services framework will be developed with rules dealing with money laundering and terrorism financing risks in the exchange and dealing of crypto currencies for fiat or other virtual currencies. Under the new framework, intermediaries involved in the payment and remittance process will be obliged to implement appropriate policies and control measures to adequately address such risks. These include customer due

[4] Monetary Authority of Singapore, A Guide to Digital Token Offerings, 14 November 2017

diligence; keeping good records; monitoring and screening transactions and reporting suspicious transactions.

C. Switzerland

The Swiss Financial Market Supervisory Authority (FINMA) released guidance (Guidance 04/2017)[5] on the regulatory treatment of Initial Coin Offerings (ICOs) and followed up with its ICO Guidelines[6] published on 16 February 2018. According to the Guidance, compliance with Swiss financial market laws is mandatory for ICOs and foreign financial market regulations should be considered when conducting an ICO from Switzerland.

Based on the definition used by FINMA, an ICO refers to events where a number of investors transfer funds, usually in the form of cryptocurrencies, to an ICO organizer, in return for a quantity of blockchain-based tokens, which are created and stored in a decentralized form, either on a blockchain specifically created for the ICO or through a smart contract on a pre-existing blockchain.

Given that there is no generally recognized classification of ICOs and resulting tokens, FINMA has based its own categorization on the underlying economic function of the token and distinguishes the following three categories as well as hybrid tokens:

- **Payment tokens**, synonymous with Cryptocurrencies, which are intended to be used as a means of payment for acquiring goods or services or as a means of money or value transfer. These tokens give rise to no claims against their issuer.
- **Utility tokens** are intended to provide access to an application or service by means of a blockchain-based infrastructure.
- **Asset tokens** represent assets such as a debt or equity claim against the issuer. These tokens entail a promise for instance a share in future earnings of a company or a project. In terms of their economic function, these tokens are comparable to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain (*tokenized assets*) also fall into this category.
- **Hybrid Tokens**: The individual token categorisation not being mutually exclusive, hybrid tokens may cumulate the features of tokens in different categories. For instance, asset and utility tokens can also be classified as payment tokens.

Pre-financing and Pre-sale

In some ICOs, tokens are already available at fundraising stage. This takes place on a pre-existing blockchain. Another possibility is "pre-financing" whereby investors are only offered the prospect to receive tokens at some point in the future. In such cases, the tokens or the underlying blockchain are to be developed at a later stage. It is also possible that there is a token pre-sale to investors whereby they acquire tokens entitling them to acquire different tokens at a later date.

---

[5] FINMA Guidance 04/2017 may be accessed at: https://www.finma.ch/en/documentation/finma-guidance/#Order=4

[6] The FINMA ICO Guidelines may be accessed at: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

Overview of the Swiss Financial Market Laws

Though Switzerland has a relatively fintech-friendly regulatory framework, ICOs founders, operators and issuers are required to consider the applicability of a number of financial market laws including the banking, financial market infrastructure, federal intermediated securities, stock exchange, anti-money laundering and collective investment schemes legislations as well as the Code of Obligations. In addition, ICOs must ensure that foreign regulations are factored-in, especially, securities law in force in the United States of America where tokens are offered to US persons.

Banking Act

An entity conducting an ICO that accepts or publicly advertises to accept more than 20 deposits from the public may trigger banking requirements relating to deposit taking especially in cases where participants receive their invested capital back, whether or not with a guaranteed return, by handing over the tokens. This may entail an obligation for the ICO issuer to obtain a prior banking licence as only a bank would be permitted to issue such tokens. Where, the tokens are not associated with claims for repayment on the ICO organizer, such tokens do not generally fall within the definition of a deposit.

Legal Qualification of Token as a Security

Swiss laws recognise four types of tradeable securities if they are unified and suited to mass trading, namely:

i. certified securities;
ii. uncertificated securities;
iii. derivatives; and
iv. intermediated securities.

The criterion "*unified and suitable for mass trading*" applies if the securities are offered to the public in the same structure and denomination or are placed with more than 20 clients. It is likely that ICOs will meet this criterion on a regular basis with the effect of being categorised as one of the four security types set out above. But given that a token, being immaterial by its nature, will not qualify as a (physically) certificated security under Swiss law, the other three types of securities need to be considered.

If tokens of an ICO constitute securities, they fall within the scope of securities regulation. Also, if the assets collected as part of an ICO are managed externally, there may be points of contact with the collective investment schemes regulation. In addition, if equity or debt securities are registered on a blockchain and issued in token form for public subscription, a prospectus must be published.

Know Your Customer (KYC) Duties and Responsibilities

The Swiss anti-money-laundering legislations aim at protecting the financial system from money laundering and the financing of terrorism. It extends all prudentially supervised financial intermediaries (banks, securities dealers, fund management companies, insurance companies, central counterparties, casinos, etc.) as well as individuals or legal entities that professionally store, transfer, accept or invest third-party assets. As such these intermediaries are obliged to conduct KYC to identify the parties involved in a transaction as well as the actual beneficial owner. In addition, they must ensure that appropriate documentation is provided to enable subsequent tracking of the transaction for criminal prosecution purposes. If a substantiated suspicion of money laundering or terrorist financing exists, the financial

intermediary must issue a report to the Money Laundering Reporting Office Switzerland and block the corresponding accounts.

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

REGULATORY FRAMEWORK FOR THE

CUSTODIAN SERVICES (DIGITAL ASSET) LICENCE:

CONSULTATION PAPER[1]

05 November 2018

1 The views expressed and proposals contained in this document are not final and subject to changes following feedback received from the industry, stakeholders and the public.

Table of Contents

Introduction **4**

Background and Context **5**

Purpose of this Consultation Paper **6**

Approach **6**

Technical Requirements **7**

Part I. Operational and Governance Standards **7**

1. Objective of the business 7
2. Minimum Stated Capital 8
3. Governance 8
4. Representative in Mauritius 8
5. Staffing 8
6. Outsourcing 9
7. Redundancy strategy for equipment procurement 10
8. Insurance 10
9. Efficiency and Performance 10
10. Anti-Money Laundering and Counter-Terrorist Financing ("AMLCFT") Systems and Controls 10
11. Statutory Reporting 11
12. Disclosure to clients 11
13. Qualified licence to be issued based on value of Digital Assets under custody 11
14. Minimum assets to be maintained as reserve 12
15. Management of operational risks 12
16. Custody processes and systems testing 12
17. Incident Reporting 13
18. External Audit of policies and procedures 13
19. Use of Automation 13
20. Record keeping 14
21. Business Continuity 14
22. Statutory Compliance 15

Part II: Custody Safekeeping Standards **15**

1. Key and Seed Generation 15
2. Key and Seed Storage 16
3. Security infrastructure for on-site cold storage of Digital Assets 18
4. Asset Agnostic systems and procedures 19

Part III: Custody Transaction Handling Standards **19**
1. Multi-Signature Authorisation 19
2. Selection of signatories 19
3. Justification for approval/rejection of a transaction by a signatory 20
4. Detection of suspicious or fraudulent transactions 20
5. Valuation of the Digital Asset under custody and evidence thereof 20

Conclusion **20**

Introduction

Mauritius has, over the past three decades, been consolidating its good repute as an International Financial Centre with a diversified product portfolio.

With the transformative incidence of financial technology ("fintech") on the global financial services industry, one landmark development in the fintech landscape has been the emergence of Digital Assets[2] and their use as a medium of exchange for transactions over the internet. The recent years have also witnessed significant strides in evolution of the technologies underpinning these Digital Assets, including blockchain[3].

At present, "Initial Token Offering[4]" ("ITO"), the process whereby investors transfer funds, generally in the form of cryptocurrencies[5], to the ITO organiser, in return for blockchain-based tokens[6], in electronic/binary form, has significantly grown as an alternative means of raising capital[7] for project funding.

As a forward-looking regulator, the Financial Services Commission, Mauritius (the "FSC") has embarked on setting up an enabling framework for fintech. Following the issue of the FSC Guidance Note on the Recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors (the "Guidance Note") on 17 September 2018, the FSC is now establishing the regulatory framework in relation to the Custodian Services (Digital Asset) Licence which will enable its holder to provide safe-keeping services in relation to Digital Assets.

2 A Digital Asset is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status. Digital Asset is considered as encompassing a "Virtual Asset" as defined by the Financial Action Task Force (FATF) in the FATF Recommendations as updated in October 2018

3 This term refers to a decentralised digital ledger or database of transactions relating to digital assets which are recorded chronologically.

4 The terms ITO and Initial Coin Offerings, used indistinctively, refer to an offer by a company to the public or specific investors to purchase or otherwise acquire Digital Assets or tokens as a means of raising funds.

5 Cryptocurrencies, a category of digital assets, are a math-based, decentralised convertible virtual currency, protected by cryptography, a medium of exchange and/or a unit of account and/or a store of value and do not have legal tender status. The term "Cryptocurrency" is defined by the FATF in its publication entitled Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014

6 The FSC considers a "token", commonly referred to as a "coin", as an electronic/digital representation of access rights to a service or ownership rights of an asset.

7 ITOs have been considered as analogous to initial public offerings with tokens issued being comparable to traditional shares in a company.

Background and Context

Regulation 21 of the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 (the "CIS Regulations") requires every Collective Investment Scheme ("CIS") to appoint and have, at all times, a custodian. The function of the custodian will be to take the assets of the CIS into its custody for safe-keeping and to deal with those assets in accordance with the written agreement with the CIS.

With Digital Assets now being a recognised asset-class for investment by specific investors and CIS, the Digital Assets of a CIS must also be held for sake-keeping by a custodian.

The FSC however acknowledges that while fintech activities have been developing exponentially in complexity, one major growth limiting factor has been the lack of appropriate custody services for the safekeeping of Digital Assets.

In traditional financial services, a custodian fulfils three (3) key functions relating to assets, namely validation, security and trust. Currently, in the absence of licensed custodians specialised in holding Digital Assets, first-party custodianship remains the main option to safeguard clients' Digital Assets.

This creates a fundamental security concern for Digital Assets given that the loss of a private key equates to losing the ownership rights to the Digital Asset.

Under the existing regulatory framework administered by the FSC, the two (2) following types of custodian licences are being issued:

- Custodian licence under section 100 of the Securities Act 2005 (the "SA");
- Custodian (Non-CIS) pursuant to section 14 of the Financial Services Act 2007 (the "FSA").

In line with the requirements of section 100 of the SA, the holder of the first type of Custodian licence must mandatorily be a bank or a trust company which is a subsidiary of a bank. The holder of this licence is authorised to hold the assets of CIS in custody.

The second type of licence, namely the Custodian (Non-CIS) licence, issued by the FSC under section 14 of the FSA, enables the provision of custody services to clients other than CIS. Despite there being no statutory restriction, as a matter of practice, the FSC has also been issuing the Custodian (Non-CIS) licence solely to banks or bank subsidiaries owing to their financial strength, infrastructure to store physical assets, traceability of assets, speed of execution of orders, global money transfer services and reliability of records.

Yet, the existing regulatory framework applicable to the two custodian licences relate primarily to securities[8] or physical assets and are not appropriate for the safekeeping of Digital Assets.

8 The term "securities" is defined under section 2 of the SA.

To bridge this gap and provide a solution for the custody of Digital Assets to the fintech ecosystem, in line with the Budget 2018/19, the FSA has been amended to empower the FSC to issue the Custodian Services (Digital Asset) Licence under which an entity will be licensed to hold for safekeeping, the Digital Assets of its clients.

The holder of the Custodian Services (Digital Asset) Licence, which is issued under section 14 of the FSA, will be a licensee of the FSC and will be required to ensure strict compliance with the relevant Acts[9] under the administration of the FSC as well as other applicable enactments. Simultaneously the holder of the Custodian Services (Digital Asset) Licence will also be considered as a "financial institution" under the Financial Intelligence and Anti-Money Laundering Act 2002 (the "FIAMLA") and will be required to adhere to the Anti-Money Laundering and Counter-Terrorist Financing ("AMLCFT") related laws, regulations and codes AMLCFT in Mauritius including the FSC Code on the Prevention of Money Laundering and Terrorist Financing, the FIAMLA and regulations made thereunder.

Purpose of this Consultation Paper

In line with its collaborative approach, through this Consultation Paper, the FSC is pleased to present, for the comments and views of the industry, its stakeholders and the public, its perspective on the essential components of the regulatory framework for the Custodian Services (Digital Asset) Licence.

As opposed to the custody of traditional physical assets where the asset itself or its proxy is held by the custodian, blockchain-based Digital Assets are not physically held. With such inherently digitized assets, having appropriate standards for the custody of Digital Assets becomes crucial given that the transaction information pertaining to the asset is public, distributed and immutable.

This Consultation Paper sets down the proposed operational, governance and technical requirements for the Custodian Services (Digital Asset) Licence as envisioned by the FSC.

Approach

In line with section 18 of the FSA, the FSC solely issues a licence upon being satisfied that the applicant, amongst other factors, has adequate resources, infrastructure, and staff with the appropriate competence, experience and proficiency to carry out the activity for which the licence is sought.

In assessing the capacity of an entity to provide custody services for Digital Assets, the approach contemplated by the FSC will focus on three core areas for this activity, namely:

9 "Relevant Acts" is defined under section 2 of the FSA.

1. *Operational and Governance Protocols* – The policies and protocols as well as operational risk management, including fraud prevention, in relation to the custody of Digital Assets.

2. *Safekeeping of Digital Assets* – The generation and securing of seeds and keys as well as management of addresses and wallets relating to Digital Assets. This area also extends to recovery processes regarding seeds and keys which have either been corrupted or otherwise compromised.

3. *Transaction Management* – The procedures for the facilitation of incoming and outgoing transactions in relation to a Digital Asset being held in custody to ensure that appropriate Know Your Client ("KYC") and Customer Due Diligence ("CDD") measures are applied prior to any transactions being authorised.

In respect of the three aforementioned focus areas, the holder of the Custodian Services (Digital Asset) Licence will be required to comply with best standards and practices established by the industry.

The approach proposed by the FSC in some parts of this Consultation Paper is explicit and prescriptive, while in other parts, "standards" and "industry practices" have been mentioned in view of setting the minima criteria while keeping the requirements voluntarily wide. In so doing, the FSC expects that as industry expertise develops in this field of activity, these best practices and standards may then be considered to develop guidelines for specific functions of the custody of Digital Assets.

Technical Requirements

Part I. Operational and Governance Standards

1. Objective of the business

1.1. The objectives of the applicant for the Custodian Services (Digital Asset) Licence shall be limited to the safe-keeping of Digital Assets and operations arising directly from it as stated in the application. For the avoidance of doubt, a single entity applicant will not be permitted to undertake any other financial business activities[10] along with the custody of Digital Assets. Such other financial business activities will have been undertaken under by a separate entity holding the relevant licence from the FSC.

1.2. In addition, for ring-fencing purposes, a single entity will not be allowed to act as custodian for both traditional assets (securities or physical assets) and Digital Assets. An entity wishing to offer both types of custodian services shall be required to do so under separate legal entities and with appropriate licences.

10 The term "financial business activities" is defined under section 2 of the FSA.

2. Minimum Stated Capital

2.1. The custodian of Digital Assets shall, at all times, have and maintain a minimum stated unimpaired capital of not less than MUR 500,000 or such higher amount as the FSC may determine.

3. Governance

3.1. An applicant for the Custodian Services (Digital Asset) Licence shall –

3.1.1. Ensure that its governance structure provides effective oversight of its activities, taking into consideration the nature, scale and complexity of its business;

3.1.2. Establish adequate internal controls and adopt strategies, policies, processes and procedures in accordance with principles of sound corporate governance and risk management;

3.1.3. Maintain its registered office and place of business in Mauritius; and

3.1.4. Have a board of directors composed of not less than 3 directors, at least one of whom shall be resident in Mauritius.

4. Representative in Mauritius

4.1. The applicant must also have, at all times, a representative in Mauritius who shall be responsible for –

4.1.1. Filing with the FSC such document as may be required under the relevant Acts and any other enactment;

4.1.2. Acting as liaison with the FSC for any correspondence, notice or summons; and

4.1.3. Maintaining records of the custodian in line with the applicable statutory requirements.

5. Staffing

5.1. The applicant will have to ensure that it is adequately staffed with the appropriate competence, experience and proficiency to properly perform its functions. It will also be required to have properly defined and documented duties and responsibilities amongst its staff regarding safe-keeping, transaction management and custody related operations.

5.2. Such staffing details and responsibility allocation plans, in line with its business needs will have to be submitted to the FSC as part of its procedure manuals at the time of the application for the Custodian Services (Digital Asset) Licence.

Background screening of personnel

5.3. The applicant will be required to subject all staff performing core custody-related tasks to prior vetting and clearance through appropriate background screenings or other appropriate tests in accordance with best industry-related standards.

5.4. Such screening may have to be conducted on a recurrent basis, depending on business needs, following the issue of the Custodian Services (Digital Asset) Licence and relevant records evidencing these personnel checks must be maintained and made available for inspection by the FSC upon request.

Manual execution of core functions

5.5. The applicant must have documented procedures such that non-automated core functions related to the custody of Digital Assets are performed only by personnel who have been subject to the abovementioned background screening.

Access to Keys, Seeds and related information

5.6. The applicant must also have appropriately documented systems to restrict access to keys, seeds and information relating to Digital Assets being held under custody solely authorised personnel on a demonstrated business needs basis.

5.7. An updated list of authorised personnel having such access must be maintained along with clearly defined procedures to enable or revoke access rights. In addition, access rights to keys, seeds and related information must be adequately logged to evidence access rights management.

6. Outsourcing

6.1. In its application, full disclosure must be made to the FSC regarding functions which the applicant proposes to outsource to any external third party and the rationale for the proposed outsourcing.

6.2. The applicant must have appropriate protocols so that the third party is subject to adequate due diligence both in terms of the fitness and propriety as well as its capacity to fulfil the outsourced function in accordance with the prescribed regulatory requirements for the custody of Digital Assets. Details of such due diligence conducted must be kept on record by the applicant.

6.3. It is to be however pointed out that the applicant shall retain full responsibility vis-à-vis the FSC for the failure by the third party to fulfil the outsourced function.

7. Redundancy strategy for equipment procurement

7.1. The applicant will have to maintain a documented redundancy strategy for the procurement of equipment used to perform core functions of the custody function from alternative suppliers in case of failure by the main supplier(s) to comply with contracts for delivery of such equipment. At any point in time, the applicant must have in place the appropriate infrastructure to ensure that the core tasks relating to its activities are fully functional at all times.

8. Insurance

8.1. Subject to availability, the applicant shall be required to subscribe to adequate insurance protection in relation to the Digital Assets being kept in custody.

8.2. At application stage, evidence that such arrangements for insurance subscription have been initiated, must be submitted to the FSC.

9. Efficiency and Performance

9.1. The applicant must demonstrate that it has, in place, appropriate systems and procedures so that it operates in an efficient manner and completes transactions in a timely manner as per industry best practices and standards.

10. AMLCFT Systems and Controls

10.1. As part of its application document pack, the applicant will be required to submit a detailed report containing an in-depth assessment of the potential money laundering and terrorist financing ("ML/TF") risks posed by its operations as well as the measures, systems, controls and protocols which will be established in relation to those ML/TF risks. Once licensed, prior to starting its operations, the licensee will be required to have those ML/TF systems and controls in place.

10.2. For the sake of clarity, the FSC wishes to point out that the Custodian Services (Digital Asset) Licence will be issued under section 14 of the FSA and as such the holder of this licence, while being a licensee of the FSC, will simultaneously be considered as a "financial institution" under the FIAMLA.

10.3. Consequently, the holder of the Custodian Services (Digital Asset) Licence will be required to ensure strict adherence to the appropriate laws, regulations and codes relating to AMLCFT in Mauritius including the FSC Code on the Prevention of Money Laundering and Terrorist Financing, the FIAMLA and regulations made thereunder.

10.4. As part of its systems and controls to prevent ML/TF, the applicant must have in place procedures to conduct CDD and KYC as well as to ascertain the source of funds/wealth of potential clients prior to on-boarding.

11. Statutory Reporting

11.1. The applicant must have in place a system to ensure that it complies with its statutory reporting requirements as prescribed under the applicable laws.

12. Disclosure to clients

12.1. The documented procedures of the applicant must, in addition, include systems for appropriate disclosures to be made to each client, on a regular basis or alternatively at the latter's request, on transactions relating to his account(s) such as an account statement containing at a minimum, the activity period, transaction dates and amount, account balance and valuation of Digital Assets in the account, where appropriate, to enable the client to identify any unauthorized or erroneous transactions and ascertain the account's integrity.

12.2. The FSC considers that the protocols of the applicant must also cater for the following disclosures:

12.2.1. Each client to be provided with an original of the signed agreement regarding the custody of his Digital Assets at the time of on-boarding;

12.2.2. Thereafter, client to be informed of any action which is likely to impact on the signed agreement; and

12.2.3. Any occurrence which may have an incidence on the Digital Assets belonging to the client being held in custody;

12.3. In the event that such disclosures are being made to the client through a web-based service, the applicant will need to have in place a user multi-factor authentication system in line with the best industry practices.

13. Qualified licence to be issued based on value of Digital Assets under custody

13.1. If the application is successful, the applicant, will initially be issued with a qualified licence allowing it to start its operations and develop its activities. Once it is fully operational and after having held Digital Assets under custody valued at least at USD 30 million for a consecutive period of three (3) months, it will be required to inform the FSC and submit evidence thereof to the FSC. Upon being satisfied with the operations of the holder of the qualified licence, this licence will then be converted into the full Custodian Services (Digital Asset) Licence. The holder of the qualified licence shall endeavour, on a best effort basis, to be fully operational and meet the threshold of USD 30 million worth of Digital Assets under custody within six (6) months from having been issued with the qualified licence.

14. Minimum assets to be maintained as reserve

14.1. After having started its operations under the qualified licence and at all times thereafter, the applicant will also be required to maintain a minimum quantum of assets in reserve to ensure that it has sufficient liquidity to continue its operations in the event that all its clients have withdrawn their Digital Assets. The amount of this minimum reserve, which is to be notified to the FSC, will have to be maintained by the applicant in line with its operational needs.

14.2. As a general rule, the applicant will not be permitted to prevent the withdrawal by a client of its Digital Assets in line with the contract, in order to maintain the minimum reserve requirement.

15. Management of operational risks

15.1. The applicant's procedures must include a comprehensively documented operational risk management programme (ORMP) which shall include all current industry risks and be audited on an on-going basis to cater for emerging risks to its business. This ORMP, to be applied in the operations of the applicant and communicated to all relevant personnel, will need to include, at a minimum:

15.1.1. Strategies developed to identify, assess, monitor and control/mitigate operational risks;

15.1.2. Policies and protocols relating to operational risk management and controls;

15.1.3. Methodology to assess operational risks; and

15.1.4. Operational risk reporting system.

16. Custody processes and systems testing

16.1. Once it has been licensed by the FSC, the custody processes and systems in place must be tested on a scheduled recurrent basis with evidence of such tests and findings thereof being appropriately documented. Such findings must be made available to the FSC for inspection, upon request. The schedule for system testing must be included in its protocols to be submitted to the FSC at the time of application.

16.2. The recurrent testing schedule must mandatorily take into consideration procedural risks as well as high impact financial risks and may also extend to:

16.2.1. Penetration testing and vulnerability scans;

16.2.2. Wallet integrity audits;

16.2.3. Key and seed generation procedures;

16.2.4. Completed transaction audit to ensure compliance with protocols;

16.2.5. Suspicious transaction handling;

16.2.6. Migration of storage devices (cold to hot storage and vice versa); and

16.2.7. Proof of reserves audits.

16.3. Systems testing must be undertaken in line with the industry's best standards and practices and may be conducted by the licensee, independent third parties or both. The participation of external parties will be highly relevant in defining risks and tests which may have been overlooked by the licensee.

17. Incident Reporting

17.1. The applicant must have in place appropriate protocols to ensure that any incident, which results in an interruption of its operations, is properly logged and documented with details of the cause of the incident, impact, method used to resolve the incident and timeframe for doing so. The procedures of the applicant will have to provide for such a report to be periodically escalated to the applicant's management and board of directors for their information. The report may also be used to update the existing custody processes and systems in view of plugging any identified gaps.

18. External Audit of policies and procedures

18.1. The applicant must have in place appropriate arrangements for its policies and procedures to be externally audited. The external audit findings must be used to address any shortcomings identified. Records of the audit findings along with documentation of any remedial actions implemented must be kept and made available for inspection by the FSC upon request. The FSC recommends that the first external audit be conducted within the first year of operation and thereafter on a recurrent basis, in line with industry best standards and practices.

19. Use of Automation

19.1. The applicant may have recourse to the use of automation in relation to its functions. The proposed automation of its functions will have to be disclosed in its procedures submitted at the time of application along with appropriate justifications.

19.2. For any use of automation to perform core and other operational functions relating to the custody of Digital Assets, the ORMP is to be duly updated to provide for scenarios to be followed in the event that the automation fails.

20. Record keeping

20.1. The systems of the applicant must have properly documented procedures relating to record keeping on its clients, including their respective identity as well as information on the Digital Assets kept under custody, including detailed transactional information. Such records must be in line with the appropriate statutory requirements and must be available for inspection upon request by the FSC.

20.2. Transactional information to be maintained on record to include:

20.2.1. Transaction time stamp;

20.2.2. Transaction type;

20.2.3. KYC/CDD on parties to the transaction;

20.2.4. Relevant signatories and transaction approval/rejection evidence;

20.2.5. Account balances; and

20.2.6. Transaction value.

20.3. The applicant may consider keeping its records and data using blockchain technology for immutability.

21. Business Continuity

Personnel Redundancy

21.1. For the purposes of business continuity, the applicants will be required to have:

21.1.1. As part of its protocols, a personnel redundancy system to ensure the continuity of its operations in the event that the primary personnel assigned to perform a non-automated core function is unavailable. This may include having back-up staff with appropriate expertise to perform the applicable function.

21.1.2. A suitable alternate site which will allow it to continue its operations uninterrupted, in the event that the primary custody location is compromised.

Disaster Recovery

21.2. The FSC will require that the applicant maintains appropriate disaster recovery facilities, with appropriate geographic segregation and equivalent security installations as the main place of business, in view of ensuring business continuity and client asset protection.

22. Statutory Compliance

22.1. The applicant, once licensed, must ensure that it complies, at all times, with all applicable laws in Mauritius, and where applicable, the relevant laws in the jurisdictions in which it operates.

Part II: Custody Safekeeping Standards

1. Key and Seed Generation

1.1. As part of its documented protocols to be submitted to the FSC at application stage, the applicant will be required to demonstrate that appropriate safeguards have been embedded in the seed creation and subsequent key generation process so that seeds and keys are sufficiently resistant to speculation or collusion.

1.2. In this respect, the applicant will be required to establish that the method to be employed for the generation of asymmetric private-public key combinations adhere to best industry standards and practices in terms of entropy, to ensure unpredictability and randomness for resilience to supposition. The method may also include an additional security measure such as a back-up mnemonic pass-phrase generated as part of the seed which may be utilized to regenerate the seed if need be.

1.3. Ideally, the applicant must have at least two distinct individuals from its personnel, involved in the process of generating entropy during seed creation. The protocols of the applicant must provide for measures ensuring that no single person ever comes into possession of all facts or knowledge of the entirety of the seed or back-up mnemonic passphrase. As a general rule, the applicant's protocols must include proper safeguards to prevent individuals who have been involved in seed creation from getting access to the systems and processes enabling the initiation of transactions through cryptographic signature.

1.4. The protocols of the applicant must also cater for seed creation and key generation to be carried out on an Air Gap Machine in physical space which is, as per industry best practices, secured to be resilient against malicious attacks, whether over the network or physically.

1.5. In the event that a single seed is produced for a signatory, the applicant's procedures must ensure that the signatory is involved in the production of the associated key. Moreover, as soon as the seed has been generated, the applicant must have systems in place to make sure that it is to be stored on an encrypted, password-secured device.

1.6. Furthermore, the applicant must demonstrate that it has in place an appropriate process according to which all digital data post seed creation and key generation, including entropy procedures, seeds, private keys, or any other sensitive wallet information created during the seed-key generation process is securely deleted using an industry

accepted deletion process for electronic media. Any such information in hard copy is also to be appropriately destroyed using pulping, cross-cut shredding or incineration.

2. Key and Seed Storage

Primary Key and Seed Storage

2.1. Regarding primary key and seed storage, the applicant must demonstrate that its protocols provide for keys and seeds which are not in use, to be stored by means of strong encryption and password-secured device, in accordance with industry best standards and practices.

2.2. In addition, at any point in time, the applicant is to have systems and procedures to ensure that:

2.2.1. Fewer than the number of keys required to initiate a transaction are stored together whether online or at a single physical location; and

2.2.2. It is impossible to initiate transactions solely using signatures stored online or at the physical address.

Back-up Storage

2.3. In terms of back-up storage, once the mnemonic back-up phrase has been generated, the applicant's protocols will have to provide for it to be broken in two or more parts with each part being kept separately in distinct tamper-proof containers stored in different physically secure locations. The protocols, must not, under any circumstances, allow a sufficient number of parts of the back-up phrase required to regenerate the seed, to be stored in a single location.

2.4. Back-up seed storage must, in accordance with industry best practices, be off-site from the place where transactions are managed and operations are conducted. Off-site physical seed storage must, at least, be maintained by a third party which is adequately equipped with safe deposit boxes enabling dual key access.

2.5. The procedures of the applicant must incorporate measures to ensure that the access to off-site back-up seed storage is restricted solely to the authorised personnel of the applicant. Prior to allowing access to the back-up seed storage, the identity of the authorised personnel will have to be verified and confirmed by the third party through multifactor identity verification and audit consistent with industry best practices.

2.6. All back-up seed storage facilities must be equipped with appropriate vaults, 24/7 video monitoring and adequate security systems for protection against forcible attacks, flood, fire, cyclone and other climatic conditions.

2.7. The applicant must also have in place systems to ensure that an internal audit of the back-up seeds is conducted, at a minimum, on a quarterly basis to assess whether they

have been tampered with or removed from secured storage. The audit results must be properly recorded with details of any incidents observed as well as any remedial actions taken, if any, and are to be provided to the FSC for inspection upon request.

Impaired Key

2.8. As part of its systems and protocols, the applicant will be required to have documented procedure to be actioned in the event that a key, seed or a part thereof is suspected to have been compromised, including but not limited to new wallet creation and migration of the relevant Digital Asset thereto.

2.9. Its protocols must also provide for the applicant to duly investigate any suspicion that a key, seed or a part thereof has been compromised. The investigation findings must be properly documented and made available for inspection by the FSC upon request.

Uninterrupted Access

2.10. The applicant must also have written procedures demonstrating that it will be able to provide its clients with uninterrupted access to their respective Digital Assets being kept under its custody in the event that it is no longer able to abide by the custody agreement or it ceases to operate. These procedures may have to extend to transferring the Digital Assets according to the instructions of the client or such other mutually agreeable arrangements.

Segregation of client assets

2.11. The FSC will require that the applicant maintains systems and controls ensuring that an address or wallet is ascribed to one single client and that the Digital Assets belonging to that client is kept in his designated address/wallet. Adequate procedures must also be in place to ensure that at no point in time, the Digital Assets belonging to different clients are pooled or kept together at a single address or common wallet.

Address use strategy

2.12. The FSC considers that the use of a new address for every transaction relating to a client ensures the latter's privacy and the confidentiality of his personal information. Thus, using the same client address for numerous transactions may arguably lead to more information being revealed on the client, for instance his identity or commercial investment data with resulting safety concerns. Accordingly, the protocols of the applicant must include appropriate address use strategy which justifies when a new address will be used and when recurrent use of the same client address will be made for multiple transactions.

3. Security infrastructure for on-site cold storage of Digital Assets

3.1. Regarding on-site cold storage, the applicant will have to demonstrate to the FSC that it will have in place, an adequately secured physical infrastructure, which will include but shall not be limited to, guarded access to the facilities with restricted admittance to authorised personnel only, vault/safe storage with dual key requirements and 24/7 closed-circuit television system. Access procedures will have to be adequately documented and must be made available for inspection by the FSC upon request.

Storage Strategy for Digital Assets

3.2. The procedures of the applicant must include a strategy for choosing the suiting storage for a Digital Asset being brought in custody factoring, amongst other circumstances, the volume of transactions relating thereto, the speed at which those transactions are to be executed and risk appetite of the client. This strategy for choosing the appropriate storage medium will have to be in accordance with industry best standards and practices.

Security Breaches

3.3. The protocols of the applicant will need to clearly spell out the procedures, which are to be periodically audited, to be actioned in the event, or suspicion thereof, that a security breach has occurred including hacking, attack, theft or any situation whereby a Digital Asset being kept in custody has been compromised. The systems of the applicant will have to incorporate appropriate actions specifically designed to protect the Digital Assets being held in custody in the event of security breaches. The policies of the applicant will have to extend to duly notifying the relevant client of the security incident.

Revocation of a signatory's access key to a back-up seed

3.4. Additionally, the FSC expects the applicant's protocols to include measures for the immediate revocation of the key(s) held by a signatory. Such revocation must spontaneously prevent the signatory from accessing the back-up seed or any information relation to the mnemonic phrase used in the seed creation. A revoked signatory must also not be able to recover the seed.

3.5. In practice, the FSC expects that the revocation of a signatory will only entail the removal of the latter's access to a back-up seed without the need to create a new wallet or migrate the Digital Asset in custody to another wallet. Such procedure for revocation of access must be periodically audited and user access logs must be monitored for unauthorized access by revoked signatories.

4. Asset Agnostic systems and procedures

4.1. The systems and procedures of the applicant will be expected by the FSC to be asset agnostic and ensure the same level of regulatory compliance relating to the safekeeping, transaction management and custody operations with respect to every Digital Assets type irrespective of wallet functionality protocol.

4.2. However, the applicant may choose to have the systems and protocols supporting one specific type of Digital Asset, instead of multiple types. In such a situation, the licence issued to the applicant will be restricted to the custody of the specific Digital Asset type. This licence may thereafter be extended as the systems and protocols evolves to support other types of Digital Assets.

Part III: Custody Transaction Handling Standards

1. Multi-Signature Authorisation

1.1. The protocols of the applicant must ensure that at any point in time, no single party is able to initiate and complete a transaction pertaining to a Digital Asset being held in custody. Furthermore, the applicant will mandatorily be required to mitigate the risk of collusion between the signatories in view of initiating unauthorized transactions relating to a Digital Asset under custody.

1.2. A possible consideration is for the applicant to use an M-of-N multi-signature standard, in line with the best industry practices, requiring a minimum number of signatures to have quorum for the purpose of initiating and completing a transaction. In case this approach is chosen by the applicant, the set minimum number of signatures for quorum will have to be documented by the applicant.

2. Selection of signatories

2.1. To curtail the risks of collusion or malicious acts by signatories, the applicant will be required to have an established procedure in view of designating the signatories for transactions relating to Digital Assets under custody. Such risks of collusion and other acts of bad faith by signatories must be catered for in the applicant's ORMP.

2.2. Methods which may be contemplated by an applicant to mitigate the risk of collusion amongst designated signatories may include:

2.2.1. Identities of signatories being unknown to each other; and

2.2.2. Signatories having differing incentives (for instance, the client or his representative, the applicant and other possible third parties such as a bank or law firm).

3. Justification for approval/rejection of a transaction by a signatory

3.1. The applicant will have to demonstrate that as part of its protocols, each signatory will be required to document the rationale to approve or reject a transaction in relation to a Digital Asset under custody. The rationale under which a transaction may be approved or rejected by a signatory, the evidence to be kept on record as well as the time frame to validate or reject the transaction, may be contractually agreed between the client, the custodian and the signatories. Any transaction approval/rejection and supporting justifications must be properly logged and made available to the FSC for inspection upon request.

3.2. The applicant will also be required to maintain a detailed log for any change in the chain of access to a Digital Asset.

3.3. Records of transaction approval/rejection and supporting justifications as well as any change in the change of access to a Digital Asset, may also be made available, upon request, for review by the owner of the Digital Asset subject to the transaction.

4. Detection of suspicious or fraudulent transactions

4.1. The applicant must have a documented system for detection of suspicious or fraudulent transactions as well as the procedure for reviewing suspicious transactions with clear actions to be implemented based on the findings of the review, in line with the requirements of the relevant enactments.

5. Valuation of the Digital Asset under custody and evidence thereof

5.1. In the event that the current market value is amongst the underpinning reasons for a transaction involving a Digital Asset being kept in custody, prior to the transaction, the protocols of the applicant must provide for disclosure, to the client and signatories, of the source of the valuation and the methodology used for such valuation. This valuation methodology will have to be in accordance with the industry best standards and practices for the calculation of the real-time valuation of Digital Assets at the time of transaction.

Conclusion

This Consultation Paper contains the FSC's perspective on the regulatory framework for the Custodian Services (Digital Asset) Licence, on which, in line with its collaborative approach, the FSC is seeking feedback from the industry, its stakeholders and the public.

The consultation period will span from 05 November 2018 to 30 November 2018. Interested parties are invited to send their comments, feedback and suggestions in relation to the regulatory framework proposed in this Paper during the consultation period by email on csda@fscmauritius.org.

Glossary of Terms

Air Gap Machine	A computer specifically designed so that it is impossible for it to connect to the internet. The computer is designed without a microphone, network card, hardwired network connectivity and Bluetooth.
Cold Storage	A method of storing Digital Asset or information whereby the device used for storage is not connected to the Internet.
Custodian	The entity entrusted with the custody of Digital Assets.
Custody	The safekeeping of Digital Assets being held or transacted.
Digital Assets	Any token, in electronic/binary form, which is representative of either the holder's access rights to a service or ownership of an asset. A Digital Asset, in this respect, includes a digital representation of value which: • is used as a medium of exchange, unit of account, or store of value but which is not legal tender, even if it is denominated in legal tender; • represents assets such as debt or equity in the promoter; or • provides access to a blockchain-based application, service or product. A Digital Asset, however, exclude: • any transaction in which a business, as part of an affinity or reward programme, grants value which cannot be exchanged for legal tender, bank credit or any Digital Asset; or • a digital representation of value issued for use within an online gaming platform.
Entropy	Unpredictability or randomness within the source code which is used to generate a cryptographic seed which ensures that a seed cannot be simply recreated.
Multi-Signature	The requirement for a minimum of number of signatures (M) out of the total number of available signatures (N) for a wallet in order for a transaction to be initiated. Also referred to as "multi-sig" or M-of-N transacting method.
Signatory	An individual providing one of the signatures in an M-of-N multi-signature transacting method.
Signature	An authorization protected by cryptography which is applied by a designated signatory to initiate a transaction.
Safekeeping	The contractual obligation according to which a custodian is required to secure and preserve Digital Assets kept being held in custody.

Seed	An alphanumeric phrase generated through the process of entropy. The alphanumeric phrase is a list of words from a specific word set which are used to create a mnemonic. This mnemonic stores all required information to use a key or apply a signature.
Transaction	An exchange or operation specific to a Digital Asset being held in custody.
Transaction Type	Classification of a transaction according to its specific purpose. Transaction types will include deposit and withdrawal.

Financial Services Commission
Mauritius

Fintech Series

Guidance Note

Recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors

1. Background

1.1. The Financial Services Commission, Mauritius (FSC), the integrated regulator for non-banking financial services and global business sectors, is highly supportive of Fintech-related initiatives in the Mauritius International Financial Centre.

1.2. In light of the developments in Fintech activities, the FSC has been receiving numerous queries from its licensees and stakeholders regarding the possibility for them to invest in Cryptocurrencies[1].

1.3. Through this Guidance Note, the first in the Fintech Series, issued under section 7(1)(a) of the Financial Services Act 2007, the FSC seeks to provide clarifications to its licensees and stakeholders on its position regarding investment in Digital Assets, including Cryptocurrencies.

2. Digital Assets

2.1. The FSC considers as a Digital Asset, any token[2], in electronic/binary form, which is representative of either the holder's access rights to a service or ownership of an asset. A Digital Asset, in this respect, includes a digital representation of value which:

[1] The FSC has adopted the definition of the term "Cryptocurrency" provided by the Financial Action Task Force (FATF) in its publication entitled Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014. According to the FATF, Cryptocurrencies, a category of Digital Assets, are a math-based, decentralised convertible virtual currency which are protected by cryptography and are used as a medium of exchange and/or a unit of account and/or a store of value but do not have legal tender status.

2.1.1. is used as a medium of exchange, unit of account, or store of value but which is not legal tender, even if it is denominated in legal tender;

2.1.2. represents assets such as debt or equity in the promoter; or

2.1.3. provides access to a blockchain-based application, service or product.

2.2. A Digital Asset will, however, exclude:

2.2.1. any transaction in which a business, as part of an affinity or reward programme, grants value which cannot be exchanged for legal tender, bank credit or any Digital Asset; or

2.2.2. a digital representation of value issued for use within an online gaming platform.

2.3. The FSC considers Cryptocurrencies as being a sub-category of Digital Assets.

3. Cryptocurrencies are not legal tender in Mauritius

3.1. Cryptocurrencies, unlike fiat currencies, are not legal tender in Mauritius. Nonetheless, the FSC acknowledges that, albeit reliant upon market demand and supply, Cryptocurrencies have "value" since they are exchangeable for other things having value, thereby showing characteristics akin to physical commodities such as grain or precious metals.

3.2. The FSC thus considers a Digital Asset including a Cryptocurrency as being a store of value.

4. Digital Assets and Cryptocurrencies as an asset-class

4.1. Since transactions in Cryptocurrencies are unregulated and their prices are extremely volatile in their exchange rates to fiat money, investments in Cryptocurrencies tend to be of a high-risk nature.

[2] The FSC considers a "token", commonly referred to as a "coin", as an electronic/digital representation of access rights to a service or ownership rights of an asset.

4.2. The FSC, nonetheless, recognises that Digital Assets including Cryptocurrencies may constitute an asset-class for investment by the following:

4.2.1. Sophisticated[3] investors;

4.2.2. Expert[4] Investors;

4.2.3. Expert Funds[5];

4.2.4. Specialised Collective Investment Schemes[6]; and

4.2.5. Professional Collective Investment Schemes[7].

5. Investments in Digital Assets and Cryptocurrencies not protected by any statutory compensation arrangements in Mauritius

5.1. Given the high-risk nature of investments in Digital Assets and Cryptocurrencies, the FSC considers that they may not be suitable for investment by retail investors.

5.2. The FSC thus urges all prospective investors to fully ascertain the related risks prior to committing any funds for investment in Digital Assets and Cryptocurrencies.

5.3. In addition, the FSC hereby informs the public and other investors that any investment in Digital Assets and Cryptocurrencies is at their own risks and that they are not protected by any statutory compensation arrangements in Mauritius.

Financial Services Commission
17 September 2018

FSC House, 54 Cybercity, Ebene 72201, Republic of Mauritius
Tel: (230) 403 7000 Fax: (230) 467 7172
E-mail: fscmauritius@intnet.mu, Website: www fscmauritius.org

[3] The term "Sophisticated Investor" is defined in section 2 of the Securities Act 2005.
[4] The term "Expert Investor" is defined in regulation 78(a) of the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 (CIS Regulations 2008).
[5] The term "Expert Fund" is defined in regulation 2 of the CIS Regulations 2008.
[6] The term "Specialised Collective Investment Scheme" is defined in regulation 77 of the CIS Regulations 2008.
[7] The term "Professional Collective Investment Schemes" is defined in regulation 75 of the CIS Regulations 2008

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

BERMUDA

COMPANIES (INITIAL COIN OFFERING) REGULATIONS 2018

BR 65 / 2018

TABLE OF CONTENTS

PART 1
PRELIMINARY

1 Citation
2 Interpretation

PART 2
MINIMUM REQUIRED INFORMATION FOR INITIAL COIN OFFERING

3 Application for consent
4 Minimum required information regarding the proposed project
5 Minimum required information describing the project
6 Minimum required information regarding digital asset issue
7 Minimum required information regarding any proposed transfer following digital asset issue
8 Minimum required information regarding compliance issues

PART 3
COMPLIANCE MEASURES

9 Meaning of "appropriate measures"
10 Verification of identity and timing of verification
11 Requirement to cease transactions, etc.
12 Enhanced due diligence
13 Reliance on third parties
14 Record-keeping
15 Audit of ICO

PART 4
MISCELLANEOUS

16 Class of digital assets
17 Meaning of "promoter"
18 Security of digital assets, etc.

The Minister responsible for companies, in exercise of the power conferred by section 34M and section 287A of the Companies Act 1981, makes the following Regulations:

PART 1

PRELIMINARY

Citation

1 These Regulations may be cited as the Companies (Initial Coin Offering) Regulations 2018.

Interpretation

2 In these Regulations—

"Act" means the Companies Act 1981;

"AML/ATF regulated financial institution" has the meaning given in regulation 2(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008;

"applicant" means the company that submits an application for consent;

"application for consent" means an application to the Minister under section 4A of the Act for consent to an ICO;

"appropriate measures" has the meaning given in regulation 9;

"independent professional" means a professional legal adviser or accountant being a firm or sole practitioner in independent practice who by way of business provides legal or accountancy services to other persons;

"Initial Coin Offering" or "ICO" has the meaning given in section 34A of the Act;

"participant" means a person who purchases or otherwise acquires digital assets pursuant to the Initial Coin Offering;

"project" has the meaning given in section 34A of the Act;

"proposed participant" means a person who makes an application to purchase or otherwise acquire digital assets pursuant to the Initial Coin Offering.

PART 2

MINIMUM REQUIRED INFORMATION FOR INITIAL COIN OFFERING

Application for consent

3 An application for consent shall be submitted to the Minister in such form as the Minister may direct and shall include the minimum required information set forth in this Part and the ICO offer document.

Minimum required information regarding the proposed project

4 An application for consent shall include the following minimum information relating to the Initial Coin Offering project including—

(a) the name of the project and the names of the project managers;

(b) the name of the applicant, including addresses, email addresses and websites and any other jurisdiction in which the applicant is registered;

(c) the details of all persons involved with the ICO including the digital asset issuer, the owner of the platform, ICO organisers and other such information; and

(d) confirmation as to whether any one or more of the persons referred to in paragraph (a), (b), or (c) have applied for or been granted a licence, permission or other authority under any law relating to the proposed ICO or otherwise relating to financial markets in any other country or countries and, if so, the relevant details.

Minimum required information describing the project

5 An applicant shall submit the following minimum information describing the ICO project—

(a) information about the project organisation and project planning including the project phases and milestones and estimated time for delivery;

(b) key features of the product or service to be developed;

(c) the proposed market participants that the ICO seeks to target and the proposed jurisdiction or jurisdictions;

(d) whether there are any restrictions regarding participants;

(e) information regarding the technologies to be used and including whether distributed ledger technology or other new or existing technologies will be used (and whether this is an open source project);

(f) the means by which the ICO will be financed;

(g) the amount of money equivalent (in Bermuda dollars) that the ICO is intended to raise by reference to the number of digital assets;

(h) whether such funds have already been allocated to a specific project and how any surplus funds would be handled.

Minimum required information regarding digital asset issue

6 An applicant shall provide the following minimum information describing the digital asset issue—

(a) whether a digital asset has been created, or will be created in the course of the ICO; and if the latter, the steps for the creation of the digital asset by reference to the technical standards;

(b) the amount or proportion of the digital assets that will be retained by the project operator and project development team and whether there is a vesting period and, if so, details of the timeline;

(c) the point at which, by whom and the manner in which the digital asset will be transferred to the participants;

(d) a detailed description of the functionalities that are planned for the digital asset and a description of the point or points when the planned functionalities will apply or become active;

(e) the rights that the participant would acquire and any obligations to be imposed on the participant and how they will be documented (specifics regarding participation and issuing conditions are required);

(f) whether a financial institution that is subject to anti-money-laundering and anti-terrorist financing laws in Bermuda or any other jurisdiction will be engaged to meet due diligence requirements under Bermuda laws and, if so, detailed information about the relevant processes and the relevant financial institution must be provided;

(g) whether the applicant or any other persons involved in the ICO have previously completed or attempted to complete an ICO in Bermuda, or any other jurisdiction, and if so the status of the ICO and any other project funded thereby;

(h) whether the digital asset has been marketed by the applicant or any other party identified in regulation 4 as an investment.

Minimum required information regarding any proposed transfer following digital asset issue

7 An applicant shall include with his application the following minimum information—

(a) whether the digital asset can be traded or transferred between persons with or without an intermediary or other third party custodian and information about compatible wallets and technical standards;

(b) whether the digital asset will already be functional at the time of transfer and, if so, to what extent;

(c) whether it is intended that the digital asset may be used in exchange for goods or services of the applicant or third parties;

(d) whether there are plans for the project operator or issuer to buy back the digital assets and the terms of the repurchase.

Minimum required information regarding compliance issues

8 An applicant for consent shall submit the following minimum required information regarding compliance features which it intends to include in its systems—

(a) a description of the technical standards or software, blockchain or other distributed ledger technology that will be used to identify participants in the ICO;

(b) a description of the procedures or protocol that will be used to confirm the identities of the participants in the ICO; and

(c) a description of the measures that will be established to enable an audit and production of a compliance statement at the close of the Initial Coin Offering confirming compliance with these Regulations and other relevant provisions of Part IIIA of the Act.

PART 3

COMPLIANCE MEASURES

Meaning of "appropriate measures"

9 For the purposes of these Regulations, appropriate measures include the following—

(a) identifying any participant and verifying the participant's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) in the case of a legal entity or legal arrangement, identifying the participant and verifying the identity of the relevant natural person carrying out the transaction or proposed transaction;

(c) in the case of a person purporting to act on behalf of a participant, verifying that the person is in fact so authorised and identifying and verifying the identity of that person; and

(d) conducting enhanced due diligence whenever necessary in accordance with regulation 12.

Verification of identity and timing of verification

10 (1) A company shall, in relation to an Initial Coin Offering, ensure that it applies appropriate measures relating to identification and verification of the participants in the Initial Coin Offering.

(2) Subject to paragraph (3), a company must verify the identity of a participant before the issuance of a digital asset to the participant with respect to the ICO.

(3) Such verification may be completed after the issue of a digital asset if—

(a) the rights and functionalities are such that the digital asset can only be used for services and products provided by the ICO issuer;

(b) this is necessary not to interrupt the normal conduct of business;

(c) there is little risk of money laundering or terrorist financing occurring, provided that the verification is completed as soon as practicable after the digital asset is issued;

(d) any money laundering or terrorist financing risks that may arise are effectively managed; and

(e) it appears that a participant, or any person purporting to act on behalf of the participant, is not or does not appear to be anonymous or fictitious.

Requirement to cease transactions, etc.

11 (1) Where in relation to any participant or proposed participant in an ICO, a company is unable to apply appropriate measures in accordance with the provisions of these Regulations, the company—

(a) shall not open any account or carry out a transaction for the person;

(b) shall not issue a digital asset to the person;

(c) in the case of a participant in an ICO, shall not permit that participant to undertake any further transactions of any nature, until such time as the company has been able to apply the measures; and

(d) shall terminate any existing business relationship with the person.

(2) In the event that an existing business relationship is terminated in accordance with paragraph (1)(d), details regarding the termination shall be included in any final audit or other compliance report required by the Registrar.

Enhanced due diligence

12 (1) A company must apply on a risk-sensitive basis enhanced due diligence to business relationships with existing participants or proposed participants in its ICO—

(a) in accordance with paragraph (2);

(b) in instances where a person or a transaction is from or in a country that has been identified as having a higher risk by the Financial Action Task Force;

(c) in instances where a person or a transaction is from or in a country that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions;

(d) in any other situation which by its nature may present a higher risk of money laundering or terrorist financing;

(e) in instances where the company suspects money laundering or terrorist financing; or

(f) in instances where the company doubts the veracity or adequacy of documents, data or information previously obtained for the purpose of identification or verification.

(2) Where any of the circumstances in paragraph (1) exist, a company must take specific and adequate measures to compensate for the potential risk, for example by applying one or more of the following measures—

(a) ensuring that the participant's identity is established by additional documents, data or information;

(b) employing supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an AML/ATF regulated financial institution (or equivalent institution) which is subject to equivalent regulations;

(c) ensuring that the first payment is carried out through an account opened in the participant's name with a banking institution;

(d) monitoring the participant's activity.

Reliance on third parties

13 (1) A company may rely on a person who falls within paragraph (2) to apply any measures required by these Regulations, provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the company's reliance on the other person, the company—

(i) must obtain information sufficient to identify participants;

(ii) must satisfy itself that reliance is appropriate given the level of risk for the jurisdiction in which the party to be relied upon is usually resident; and

(iii) will remain liable for any failure to apply such measures.

(2) The persons are—

(a) an AML/ATF regulated financial institution;

(b) an independent professional supervised for the purposes of these Regulations by a designated professional body in accordance with section 4 of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008;

(c) a person who carries on business in a country or territory other than Bermuda who is—

(i) an institution that carries on business corresponding to the business of an AML/ATF regulated financial institution or independent professional;

(ii) in the case of an independent professional, subject to mandatory professional registration recognised by law;

(iii) subject to requirements equivalent to those laid down in these Regulations; and

(iv) supervised for compliance with requirements equivalent to supervision by his supervisory authority.

Record-keeping

14 (1) A company must keep the records specified in paragraph (2) for at least the period specified in paragraph (3).

(2) In respect of a business relationship or an occasional transaction, the records are—

(a) a copy of, or the references to, the evidence of the person's identity obtained pursuant to these Regulations, together with the results of any analysis or enhanced due diligence undertaken in relation to that person; and

(b) the records of transactions, provided that such records must be sufficient to permit the reconstruction of individual transactions.

(3) In this regulation, the period is—

(a) in the case of records in paragraph 2(a), for the duration of the business relationship and five years beginning on the date on which the business relationship ends or five years beginning on the date the occasional transaction is completed;

(b) in the case of records in paragraph 2(b), five years beginning on the date the transaction is completed.

(4) A company who is relied on by another person must keep the records specified in paragraph (2)(a) for five years beginning on the date on which he is relied on for the purposes of these Regulations in relation to any business relationship or occasional transaction.

(5) But in any case where a company has been notified in writing by a police officer that particular records are or may be relevant to an investigation which is being carried out, the company must keep the records pending the outcome of the investigation.

(6) For the avoidance of doubt, all documents and findings related to the investigations of—

(a) complex transactions;

(b) unusually large transactions; or

(c) unusual patterns of transactions,

must be recorded and kept for a minimum period of five years and shall be made available to competent authorities upon request.

(7) A person referred to in regulation 13(2)(a) or (b) who is relied on must, if requested by the person relying on him within the period referred to in paragraph (4)—

(a) make available to the person who is relying on him as soon as reasonably practicable after the request but not later than five business days thereafter any information about the participant which he obtained when applying appropriate due diligence measures; and

(b) without delay forward to the person who is relying on him, copies of any identification and verification data and other relevant documents on the identity of the participant which he obtained when applying those measures.

(8) A company who relies on a person referred to in regulation 13(2)(c) (a "third party") to apply appropriate measures must take steps to ensure that the third party will, if requested by the company, within the period referred to in paragraph (4)—

(a) as soon as reasonably practicable make available to him any information about the participant; and

(b) as soon as reasonably practicable forward to him copies of any identification and verification data and other relevant documents on the identity of the participant,

which the third party obtained when applying those measures.

(9) For the purposes of this regulation, a person relies on another person where he does so in accordance with regulation 13(1).

Audit of ICO

15 A company must—

(a) carry out an internal compliance review with respect to the conduct of its ICO and financial operations (including financial expenditures, if any) connected therewith and prepare a compliance report; and

(b) file with the compliance report with the Registrar in such form as the Registrar may determine,

within 90 days of completion of the ICO.

PART 4

MISCELLANEOUS

Class of digital assets

16 For the purposes of an ICO, "class" means digital assets having the same rights, features and attributes.

Meaning of "promoter"

17 A person is not a promoter for purposes of an ICO solely by virtue of his provision of professional services to the company in relation to the ICO.

Security of digital assets, etc.

18 The company shall ensure that appropriate mechanisms are in place in respect of the security of digital assets issued to recipients, confidentiality, disclosure of information and connected matters and that applicable Bermuda laws are complied with in these respects.

Made this 6th day of July 2018

Acting Minister of Finance

[Operative Date: 10 July 2018]

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY
AND FINANCIAL CENTRE

BERMUDA MONETARY AUTHORITY

CONSULTATION PAPER

DIGITAL ASSET BUSINESS AMENDMENT ACT 2020

7 AUGUST 2020

TABLE OF CONTENTS

I. INTRODUCTION 3

II. ENHANCEMENTS TO THE DIGITAL ASSET REGULATORY FRAMEWORK 3

Other proposed changes 5

Housekeeping changes 7

The digital asset industry and other interested persons are invited to share their views on the proposals set out in this paper and Bill. Comments should be sent to the Authority digitally, via the below survey link or QR code, no later than **07 September 2020**.

https://www.surveymonkey.com/r/3XP5DRN

I. INTRODUCTION

1. The Digital Asset Business (DAB) environment is a new and rapidly evolving space. As such, it is important that Bermuda's regulatory and supervisory framework keeps pace with the rapid rate of change so as to remain fit for purpose. The Bermuda Monetary Authority (Authority) has undertaken to enhance its oversight of DABs as part of the ongoing development of Bermuda's digital asset regulatory framework.

2. The Authority is proposing to amend the *Digital Asset Business Act 2018* (DABA or Act) to give greater clarity to certain sections and to make other changes that are intended to facilitate the development of the FinTech sector in Bermuda and a more effective administration of the Act.

3. The amendments to the Act (Bill) will cover, among other things, the following areas:
    (a) Amending some definitions to clarify the Authority's intent in certain sections
    (b) Insert a requirement to notify the Authority regarding changes to exemption conditions
    (c) Extending the Authority's ability to modify applicable fees
    (d) Establishing a new testing licence to be called a Class T licence

II. ENHANCEMENTS TO THE DIGITAL ASSET REGULATORY FRAMEWORK

4. The Authority develops risk-based financial regulations that it applies to the supervision of all of Bermuda's financial sectors, including banks, trust companies, investment businesses, insurance companies and DABs. The following proposed changes are intended to improve on the overall administration of the Act.

5. The Authority is proposing the following changes:

- Amending the definition of "digital asset exchange" to '"digital asset exchange" means a centralized or decentralized electronic marketplace used for digital asset issuances, distributions, conversions and trades, including primary and secondary distributions, with or without payment; provided that digital asset conversions and trades may also be entered into by the electronic marketplace as principal or agent'
- "Digital asset derivative exchange" means a centralized or decentralized marketplace used for digital asset derivatives issuances, distributions and trades with or without payment; provided that digital asset derivatives trades may also be entered into by the marketplace as principal or agent

- In the definition of "digital asset services vendor" replace the word 'means' with 'includes'

6. The Authority is proposing to introduce a requirement for companies that seek an exemption order under section 11 of the Act to file an application for such exemption and for such companies to be required to declare annually that they continue to qualify for exemption. This proposal will improve the oversight regime for this sector. This proposal will require the Minister of Finance to amend the existing exemption Order process to provide for persons to notify the Authority of their exempted status and to re-notify annually. Further, section 11 will also be amended with the exemption in 11(5) (a) deleted. The wording here has been interpreted differently from its intended use and, in order to avoid any further confusion, is to be removed.

7. Additionally, the Authority is clarifying a power introduced last year that would allow it to modify a fee in cases where companies would require other licences in addition to a DAB licence, particularly where a business activity crosses between legislative Acts such as investing in digital assets. Presently, a company may need both an investment business licence and a DAB licence, potentially requiring two fees for a single activity. The Authority is of the view that in these particular cases it may be appropriate for the Authority to offer a flexible fee structure. The Authority is proposing to amend section 16 of the Act to add the following:

   The Authority may, where it has made a determination –

   (a) Exempt a registered person from the requirement to pay any fee under this section, as may be prescribed under the Bermuda Monetary Authority Act 1969
   (b) Reduce any fee required to be paid by a registered person under this section by such amount as it considers appropriate, as may be prescribed under the Bermuda Monetary Authority Act 1969
   (c) In granting an exemption from, or reduction of, any fee payment under section (16), the Authority may impose any condition on such exemption or reduction, as it may determine appropriate
   (d) The Authority shall not grant an exemption from, or reduction of, any fee payment under section (16) unless it is satisfied that it is appropriate to do so having regard to the nature, scale and complexity of the business carried on by the registered person

8. It should be noted that the proposals in paragraphs 6 and 7 have previously been consulted on in a consultation paper titled *Digital Asset Business Amendment Act 2019* in May 2019. However, the requisite changes were omitted from the Act. As such, their inclusion in this consultation paper is intended primarily as a reminder to industry stakeholders of the Authority's previously planned amendments to the Act.

Other proposed changes

9. After its first complete year of FinTech operation, the Authority undertook a reflection upon the lessons learned from its licensing process, as well as from its interactions with market participants. In an effort to maintain the appropriate regulatory framework and to ensure that it continues to support financial innovation that may benefit the jurisdiction, the Authority considered whether the current set of classes under DABA were fit for purpose. In particular, consideration was given as to whether the present M (modified) and the F (full) licences were appropriate to support all stages of innovation of the evolving DAB environment.

10. Based on its research and analysis, the Authority considers it may be appropriate to enhance the FinTech regulatory framework to support all stages of innovation by giving additional consideration to the fact that innovation requires rapid testing and piloting. As such, it may be necessary for the Authority to enhance its regulatory framework to support that objective.

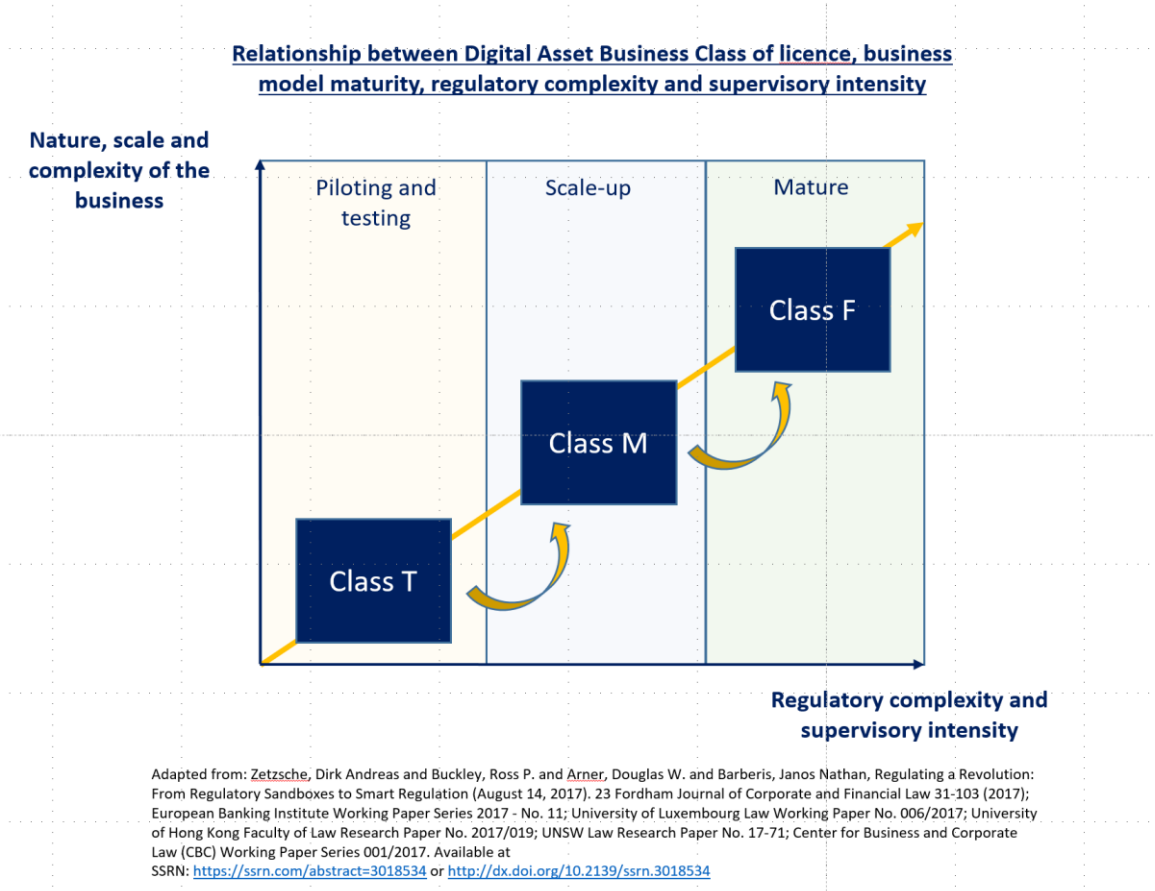
11. Further, the Authority is of the view that the best way to adapt the present framework is by the addition of a new "test" or Class T licence. The purpose of this licence class is for the testing of a minimum viable product/service via beta testing or piloting. Applicants must; (1) develop a success criterion for the test within their business plan, (2) list their pre-identified or targeted customers or counterparties, (3) hold capital of at least BD$10,000 equivalent and (4) ensure that appropriate risk disclosures for potential counterparties are in place.

12. The T licence will have an initial duration of 12 months or less and appropriate regulatory requirements based on proportionality. The business models in this class should be a DABA licensable activity and licensing fee would be limited to BD$1,000.

13. The three licences available under the Act are meant to provide a progression of regulatory complexity and supervisory intensity that is commensurate with the nature, scale and complexity of the business and that supports prudent industry development. The focus of the Authority is always to be risk-based, proportional and to provide clear expectations to the industry. We expect that the introduction of a specific testing class reduces the ex-ante costs of understanding the regulatory requirements for entities seeking to run contained pilots or tests.

14. In addition, it clarifies, with a view to protecting the public, which companies are in testing or piloting phases and that, as such, may represent a higher risk of failure. In return, customers of financial services may be better equipped to make an informed decision.

15. The graph below illustrates the relationship between the proposed class of licences.



Adapted from: Zetzsche, Dirk Andreas and Buckley, Ross P. and Arner, Douglas W. and Barberis, Janos Nathan, Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation (August 14, 2017). 23 Fordham Journal of Corporate and Financial Law 31-103 (2017); European Banking Institute Working Paper Series 2017 - No. 11; University of Luxembourg Law Working Paper No. 006/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/019; UNSW Law Research Paper No. 17-71; Center for Business and Corporate Law (CBC) Working Paper Series 001/2017. Available at SSRN: https://ssrn.com/abstract=3018534 or http://dx.doi.org/10.2139/ssrn.3018534

16. For clarity as to the expectation for each of these classes and without prejudice to the powers of the Authority to impose additional conditions, please find a summary table of some of the key features below:

Licence class	**Class T (test)**	**Class M (modified)**	**Class F (full)**
Business model maturity	Testing and piloting a business model, a product or a service which is still unproven generally or in a specific context	Scaling up a business model that has previously been tested and building full compliance programme	Proven business model at scale with fully developed compliance programme
Limitations on licence	Very limited scale, pre-set number or category of participants	Limited scale or volume of business	Usually none

Supervision	Limited reporting, important emphasis on disclosure of risks and limitations of test to prospective customers	Monthly supervisory meeting and returns with pre-determined key performance indicators	Yearly annual returns with on-site supervision
Minimum net assets	$10,000	$100,000	$100,000+
Insurance requirements	No	Yes	Yes
Head office requirements under DABA[1]	Local incorporation only	Proportional expectations as the company grows in scale and complexity	Full obligations
Duration	Three to 12 months with the potential to extend	12-24 months with the potential to extend	No pre-determined duration
Application filing costs	Reduced to $1,000	$2,266	$2,266
Annual (or for the pre-determined period) licence costs	Reduced to $1,000	Regular fee structure applies	Regular fee structure applies

17. Related to the addition of the new T Licence, the Authority is proposing to amend section (15) (1) by adding after the words "licensed undertaking" the words "except Class T licence holders"; and in section 19 (3) after the word "Bermuda" add the words "except in the case of a T licence where the Authority has granted an exemption to this provision". Section 21 (Head Office) will carry a similar exemption as the Authority recognizes that this is a very early stage of business development.

18. In section 66 Certificates of Compliance, the Authority is proposing to add a sentence to state that in cases where a licence expires before the financial year-end then a company should submit its certificate within 30 days of licence expiration.

Housekeeping changes

19. Housekeeping changes generally include a mix of minor technical changes, errors and/or omissions and consequential amendments.

[1]Notwithstanding any other potential legal obligations, including economic substance.

20. A consequential amendment is being made as a result of the passing of the *Digital Asset Issuance Act* (DAIA) which amends section 7(1) of the DABA 2018 (prudential and other returns), after paragraph (f) by inserting (g) “accreditation of digital asset business;”.

****

BERMUDA

DIGITAL ASSET BUSINESS AMENDMENT ACT 2020

BR / 2020

TABLE OF CONTENTS

1. Citation
2. Amends section 2
3. Amends section 11
4. Amends section 12
5. Amends section 15
6. Amends section 16
7. Amends section 19
8. Amends section 21
9. Amends Schedule 1
10. Consequential amendment

DIGITAL ASSET BUSINESS AMENDMENT ACT 2020

WHEREAS it is expedient to amend the Digital Asset Business Act 2018 to, amongst other measures, introduce a new class of licence; revise the definitions of digital asset exchange, digital asset derivative exchange and digital asset services vendor and to revise the power of the Authority to exempt any undertaking from the payment of any fee imposed under the Bermuda Monetary Authoriy Act 1969; or to reduce such fees; and for purposes connected with and incidental to those matters;

Be it enacted by The Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda, and by the authority of the same, as follows:—

Citation

1 This Act which amends the Digital Asset Business Act 2018 (the "principal Act"), may be cited as the Digital Asset Business Amendment Act 2020.

Amends section 2

2 Section 2 (1) of the principal Act is amended—

(a) by repealing and replacing the definition of "digital asset exchange" as follows—

"digital asset exchange" means a centralized or decentralized electronic marketplace used for digital asset issuances, distributions, conversions and trades, including primary and secondary distributions, with or without payment; provided that digital asset conversions and trades may also be entered into by the electronic marketplace as principal or agent";

(b) by repealing and replacing the definition of "digital asset derivative exchange" as follows-

"digital asset derivative exchange" means a centralized or decentralized marketplace used for digital asset derivatives issuances, distributions and trades with or without payment; provided that digital asset derivatives trades may also be entered into by the marketplace as principal or agent;";

(c) in the definition of "digital asset services vendor" by deleting the word "means" an substituting "includes".

Amends section 11

3 Section 11 of the principal Act shall be amended by —

(a) deleting subparagraph (5) (a)

Amends section 12

4 Section 12 of the principal Act shall be amended —

(a) by inserting the following after subparaph (3) "(b)" —

"(c)" class T licence, under which a person shall be licensed to provide any digital asset business activity under the definition of digital asset business, for a defined period determined by the Authority and for the purpose of carrying

out pilot or beta testing in relation to such activity.";

(b) in subparagraph (4) by inserting after "licence" the words "or class T licence";

(c) in subparagraph (5) by inserting after "licence" the words "or class T licence".

Amends section 15

5 Section 15 of the principal Act is amended —

(a) in subsection (1), by inserting after "undertaking", the words "other than a licensed undertaking granted a class T licence pursuant to section 13,";

(b) inserting the following new subsection after subsection (1) —

"(1A) A licensed undertaking granted a class T license shall —

(i) not be required to keep its licence on display at its principal place of business in Bermuda; and

(ii) publish a statement on its website for the duration of its licence, that it has a been issued a class T licence by the Authority to carry out pilot or beta testing in relation to the digital asset business activity.

Amends section 16

6 The principal Act is amended in section 16 by deleting the word "licensed" in subsections (1), (5) (a) and (b) and (7) where it appears.

Amends section 19

7 The principal Act is amended in section 19 (3) by inserting after "Bermuda", the words "except where such representative has been approved by the Authority to be appointed to a licensed undertaking granted a class T licence pursuant to section 13.".

Amends section 21

8 The principal Act is amended in section 21(1) by inserting after "undertaking", the words "other than a licensed undertaking granted a class T licence pursuant to section 13,".

Schedule 1 Amended

9 Schedule 1 to the principle Act is amended in paragraph 2 —

(a) in subparagraph (3) by inserting after "A licensed undertaking" the words, "other than an undertaking granted a class T licence";

(b) by inserting the following after subparagraph (3) —

"(3A) An undertaking granted a class T licence shall not be regarded as conducting its business in a prudent manner unless it maintains or, as the case may be, will maintain minimum net assets of $10,000 or such amount as the Authority may direct

taking into consideration the nature, size and complexity of the licensed undertaking;"

(c) in subparagraph (6) by inserting after "A licensed undertaking" the words, "other than an undertaking granted a Class T licence".

Consequential Amendment

10 The consequential amendments set forth in the Schedule have effect.

DIGITAL ASSET BUSINESS AMENDMENT ACT 2020
EXPLANATORY MEMORANDUM

This Bill seeks to, amongst other measure; introduce a new class of DABA licence; repeal and replace the definitions of "digital asset exchange", "digital asset derivative exchange" and revise the definition of "digital asset services vendor"; scope all new Class T licensees from the requirements to display a licence and maintain an office and head office in Bermuda; and to revise the power of the Authority to exempt any undertaking from the payment of any fee imposed under the Bermuda Monetary Authoriy Act 1969; or to reduce such fees:

Clause 1 provides for citation of the Bill.

Clause 2 provides for the repealing and replacing of the defined terms digital asset exchange, digital asset derivative exchange and a revision to the term digital asset services vendor.

Clause 3 proposes to amend section 11 by deleting subparagraph 5(a) in order to avoid misinterpretation of this activity in the market.

Clause 4 makes provision for a new limited duration test licence, the "Class T licence". Licensees in this class will have an opportunity (likely for not more than 12 months), to carry out pilot or beta testing in relation to a digital asset business activity, while under the supervision and direction of the Authorty and shall be required to obtain a "higher" M or "F" licence once the period of licensing has expired (where

such licensee wishes to progress to the next phase). The Fees, supervision and matters such as the appointment of a senior representative have been taken into account in respect of the limited duration of the class. The Authority may impose any conditions it deems fit in the licensing of any person in this class. Once an undertaking has satisfied the Authority of the fitness of the digital asset business activity, it may surrender its licence and submit an application to be licensed by the Authority in either the "M" or "F" licensing classes as a next or final phase of licensing.

Clause 5 makes provision for section 15 to be amended to require a Class T licensee to publish the fact that it has attained a T license on its website for the duration it holds the licence to carry out pilot or beta testing in relation to the digital asset business activity, as due to the limited nature of the class, the Authority has determined that such entity will not have the opportunity to display such license in its registered office.

Clause 6 proposes to amend section 16 by amending subsections (1), (5) (a) and (b) and (7), by deleting the word "*licensed*", which shall enable the Authority to exempt any undertaking from any fee imposed under the Bermuda Monetary Authority Act 1969; or allow for the Authority to reduce such fees as it sees fit. Previously, section 16 only allowed the Authority the power to exempt licensed undertakings from the requirement to pay any fee under section 16 (or to reduce said fees). The limitations of the Authority's powers under this section to "licensed" undertakings was not aligned with the original consultation conducted with the market, whereby the intent of the Authority was noted as allowing it to exercise such powers in relation to *any* undertaking subject to fees under section 16. The Authority shall not grant such exemption unless it is satisfied with the matters set out under subsection (7) of section 16;

Clause 7 provides amendment to section 19 to be revised to allow for a Class T licensed undertaking's senior

representative to not have to maintain an office in Bermuda; The rationale for this amendment is that the T licence is an early stage developmental licence which allows limited business and as such the senior representative will often be an executive ot the company. The office requirement would be amended as the business scales up.

Clause 8 proposes amendment to section 21 to scope out Class T licensees from the requirement to maintain an office in Bermuda; the point of this class of licence is to encourage the growth of testing and development in Bermuda. Considering the limited scope of the licence (testing) the intent is to expedite the process and ensure it makes financial sense.

Clause 9 proposes to amend the minimum criteria for licensing under Schedule 1 paragraph 2, to allow for a class T licensee to only have to hold assets equivalent to the amount of $10,000 and to not have to comply with the obligations of a Class M or F licensee relating to obtaining an insurance policy in respect of its operations. Such lower barriers to entry have been carefully considered by the Authority with respect to the nature, scale and complexity of the digital asset business to be conducted by an undertaking in this licensing class.

Clause 10 proposes consequential amendments to be made to the Fourth Schedule to the Bermuda Monetary Authority Act 1969, under the heading “Digital Asset Business Act 2018” to introduce new fee payments in respect of the new licencing class.

SCHEDULE

(Section 8)

Amends Bermuda Monetary Authority Act 1969

The Bermuda Monetary Authority Act 1969 is amended in the Fourth Schedule under "**PART C- 2021 "Digital Asset Business Act 2018**" by—

(a) inserting the following new paragraph after paragraph 2 "(h)" —

"(i) the fee payable by an undertaking carrying digital asset business in accordance with a Class T licence pursuant to section 12 (3) shall be $1000";

(b) inserting the following new paragraph after paragraph 3 "(h)" —

"(i) the fee payable by an undertaking carrying digital asset business in accordance with a Class T licence pursuant to section 12 (3) shall be $1000".

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

DAO GOVERNANCE POST - LINKEDIN

Dr Jane Thomason

While DeFi has demonstrated extraordinary innovation, it is still a very new industry and risks abound. About $120 million worth of assets were stolen from DeFi platforms in 2020. In this post, we look at DeFi governance. We take a look at Decentralised Autonomous Organisations (DAOs), the infamous DAO hack, explain how DAO governance is commonly executed and some of the vulnerabilities, and look at some of the improvements that projects are working on.

Why Does DAO Governance Matter DeFi?

Decentralised Autonomous Organisations (DAOs) are *"non-hierarchical organizations that perform and record routine tasks on a peer-to-peer, cryptographically secure, public network, and rely on the voluntary contributions of their internal stakeholders to operate, manage, and evolve the organization through a democratic consultation process"*. DAOs are in common use for DeFi and conservatively oversee more than $480 million. DeFi DAOs help users transfer cryptocurrencies across different blockchains, and serve popular DeFi use cases such as crypto lending or yield farming.

DAOs are open-source, thus transparent and, in theory, incorruptible but depending on the governance rules, there are different levels of decentralization. While the network might be geographically decentralized, and have many independent but equal network actors, the governance rules written in the smart contract or blockchain protocol will always be a point of centralization and loss of direct autonomy. DAOs can be architecturally decentralized (independent actors run different nodes), and are geographically decentralized (subject to different jurisdictions), but they are logically centralized (the protocol).

DAOs have both internal and external governance components. Internal governance is characterized by non-hierarchical modes of governance and has quasi-democratic features. The external governance is the reliance on clusters of servers and individual nodes for the functioning of the network and decision-making. Notably, those who control nodes and server capacity can exert undue influence on decision-making, and in a stronger way than other actors.

The best known failure of DAO governance demonstrated how formative and vulnerable DAO governance can be. In The DAO Controversy: The Case for a New Species of Corporate Governance?, Robbie Morrison et al. summarise some of the key features of DAOs, that amount to both features and risks. These are (1) there are no trusted human executives since the organization is governed and operated by smart contracts, (2) the smart contracts which form their governance are written and executed as computer code, (3) monitoring and enforcement of smart contracts are likewise by computer algorithms, (4) there are weak or non-existent mechanisms for dispute resolution, since the "code is law," and all participants have agreed in advance to abide by the code of the smart contract(s). In the case of The DAO hack, a smart contract both granted investors voting rights according to their

level of investment and decisions regarding the distribution and management of its $150 million dollar fund, risk, residual claims, voting rights, and voting itself, was achieved through the consensus of the investing community. However, their priorities and values did not align and there were no contingencies to define, manage, or control these conflicts. Since the decision-making structure was implemented and managed solely by the code, the DAO left the entirety of its governance operations to an algorithm which became The DAO's sole governance mechanism. It operated as it was instructed and according to previously-agreed rules. This attack concerned a clever exploitation of TheDAO's blockchain-encoded smart contract.

This experience raises legitimate questions about whether someone should be accountable in DAOs and how details of governance, legalities, ethicalities, and the logic flaws in the code are corrected and the liability for losses. In a DAO IT governance and corporate governance are one and the same.

Rozas et al summarise the key blockchain-based governance tools as:

1. Tokenization: the process of transforming the rights to perform an action on an asset into a transferable data element, a token, on the blockchain.

2. Self-enforcement and formalization of rules: the process of embedding organizational rules in the form of smart contracts.

3. Autonomous automatization: the process of defining complex sets of smart contracts as DAOs, which may enable multiple parties to interact with each other, even without human interaction.

4. Decentralization of power over the infrastructure: the ownership and control of the technological tools employed by the community through the decentralization of the infrastructure they rely on, such as the collaboration platforms (and their servers) employed for coordination.

5. Increasing transparency:the process of opening the organizational processes and the associated data by relying on the persistence and immutability properties of blockchain technologies.

6. Codification of trust: codifying a certain degree of trust into systems which facilitate agreements between agents without requiring a third party..

Some of the issues of governance in decentralized systems can be:

1. Users see tokens as yield, not voting rights, leading to a very individualist approach to collaboration. Protocols started using their governance tokens as “rewards” for users participating in the network.

2. No minimum number of participation in order to kickstart the governance. In order for a system to be considered sufficiently decentralized, there needs to be a high minimum number of token holders/participants.

3. Most of the DAOs raise money in one way or another and in return, investors get back governance tokens. This creates a high degree of centralization at the start of token distribution.

A challenge for DeFi is that the economic incentives of providing liquidity in order to get rewarded with governance tokens, this encourages competitive and speculative behavior which leads back to a centralized governance structure, since tokens slowly concentrate in a few hands. So where can this lead? Projects can become vulnerable to attacks because of excessive centralization and parties with conflict of interest can push through proposals, and activist investors can acquire a significant enough amount of governance tokens to help push through proposals profitable to them.

Vulnerabilities of DAOs also lie in the automation. The organization is governed and operated by smart contracts, the smart contracts which form the governance are written and executed as computer code. The monitoring and enforcement of smart contracts are by computer algorithms, and there are weak or non-existent mechanisms for dispute resolution, since the "code is law," and all participants have agreed in advance to abide by the code of the smart contract.

Wulf Kaal notes more mature voting alternatives are slowly emerging. Some possible improvements to DAO governance have been suggested such as:

- Releasing smart contracts in stages.
- Certification processes and review processes as well as multiple security audits from respected institutions in combination with formal verification programs for smart contracts.
- Designing the DAO such that it can be stopped when it may appear to become too big to fail.
- Barriers to DAO entry can help ensure the success of on-chain governance, such as with permissioned blockchains or community guidelines.

Many DAOs are experimenting with novel governance structures. The legal status of a DAO is also a gray area, as nobody owns the organization, who can be sued and who sues or in the case of liquidating a tangible asset owned by the DAO, what rules are to be followed?

DeFi is still in its infancy as an industry and the concept of DAOs is still relatively young, so we will continue to see a greater number of players entering the market and making improvements. As with all emerging and unregulated technologies, DeFi continues to be a case for "*caveat emptor".*

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

DeFi - Who, what and how to regulate in a borderless, code governed world?

Dr Jane Thomason

Hold onto your hats boys and girls! It's a new world - a financial system without intermediaries, that anyone can access 24 hours a day with only a mobile phone and a wallet! Julien Bouteloup of Stake Capital and a blockchain pioneer explained: *"In DeFi what we are building is fully decentralised technology, fully transparent, run by mathematics, no one can beat that. We are building on research papers, 40 years of research, fundamental research, discrete mathematics being built and put on chain that no one can beat. You cannot beat that, GitHub didn't exist in the 90s. First, the fact that we're going at the speed of light, is because everything is open source, and everyone can participate".*

Novum Insights report that since 2020, the DeFi market has grown by 40 times, with the Total Value Locked standing at $61B. Stablecoins, one of the major pillars of DeFi, almost quadrupled in the first half of 2021 to $112 billion. Massive gains are being made, but at the same time, DeFi investors are also losing money because DeFi is not regulated, moderated, intermediated, hosted or validated by a central authority, only driven by smart contracts. If the smart contract malfunctions, is hacked, or otherwise has a problem, there is no recourse. Loretta Joseph, Global Digital Asset Regulatory Expert explains: *"Regulators protect consumers and investors. In DeFi, you don't have any intermediaries to regulate, So it's totally P2P. The question is how it will be regulated in the future? People are going to get scammed. When people start to get scammed, the first thing they do is complain to the Regulator. "*

Indeed, about $120 million worth of assets were stolen from DeFi platforms in 2020. Cointelegraph report that the majority of hacks are due to developer incompetence and coding mistakes. That's significant, when the sector is entirely reliant on the code.

SEC Commissioner, Hester Peirce, said about DeFi:"*It's going to be challenging to us because most of the way we regulate is through intermediaries and when you really build something that's decentralized, there's no intermediary. It's great for resilience of a system. But it's much harder for us when we're trying to go in and regulate to figure out how to do that*."

Regulatory concerns tend to be around the volatility of crypto markets as contrasted with government-backed fiat currency, the nature of their use in connection with illicit or illegal activities, the unregulated nature of cryptocurrency exchanges and the absence of legal recourse in the event of any financial loss incurred. In the heady NFT markets, there is a lot of activity, confusion, and large crypto transactions, expected to stimulate regulators to create limits for big money moves in NFTs to prevent money laundering. At a macro level, the decentralisation of the financial system and the ability to manage economic stability and protect consumer interests poses a further challenge to regulators.

DeFi DAOs help users transfer cryptocurrencies across different blockchains, and serve popular DeFi use cases such as crypto lending or yield farming. DAOs conservatively oversee more than $543 million. In a DAO IT governance and corporate governance are one and the same. The organization is governed and operated by smart contracts, which are monitored and enforced by algorithms. The code both governs and executes. Should the algorithms fail, who then is responsible?

In Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective, Ellul et all outline some key points to consider; (i) the importance of identifying central points which can be used to apply regulation to, such as miners, core software developers, end users, and even enabling governmental or regulatory players to be potential blockchain participants; (ii) issues of identifying liability, for example that of core software developers; (iii) the challenges that the immutability and lack of update-ability of smart contracts brings; and (iv) the need for quality assurance and technology audit processes.

Exchanges and wallet providers are the most obvious targets for regulation. Decentralized exchanges (DEXes) allow users to trade directly from their wallets in a P2P manner without intermediaries. Global money-laundering watchdog the Financial Action Task Force (FATF) has exchanges in thie sights. Cointelegraph report that the Financial Action Task Force (FATF) proposed guidelines suggest that DApps (DEXs and other DeFi applications) will be responsible for complying with country-specific laws enforcing FATF, AML, and Counter-Terrorism Financing (CTF) standards.

A recent review of 16 leading exchange platforms by LSE , found that just four were subject to a significant level of regulation related to trading, so there is a clear gap. Getting listed on any major exchange now requires a project to have passed auditing, but meaningful security doesn't end there. Toby Lewis, CEO of Novum Insights, made the point , " *Also remember that smart contracts can be attacked. Even if they are audited, it does not give you a guarantee that it will be exploit-free. Do your own research before you start".*

Regulators are on a learning curve, decentralized, disintermediated and borderless blockchain networks challenge regulators. In an open-source environment where projects are developing at an average compound growth rate of 20% per year, finding just the right moment to regulate is a classic problem to solve, whereby people are protected from risk but innovation is not constrained. Some governments have addressed achieving this balance by using regulatory sandboxes (UK, Bermuda, India,South Korea, Mauritius, Australia, Papua New Guinea and Singapore), some have gone straight to legislating (San Marino, Bermuda, Malta, Liechtenstein).

Far from resisting regulation, leading DeFi figures embrace it as part of the maturing of the industry. In an interview with Cointelegraph, Stani Kulechov, the founder of DeFi lending platform Aave, suggests that peer review will be the future. *"Auditors are not here to guarantee the security of a protocol, merely they help to spot something that the team itself wasn't aware of. Eventually it's about peer review and we need to find as a community incentives to empower more security experts into the space."* In the same article, Emeliano Bonassi spoke about ReviewsDAO, a peer review forum for connecting security experts and projects looking for reviews. Bonassi sees potential for this to become a learning opportunity where people with specialized knowledge can branch into other areas and young developers can grow into fully-fledged auditors.

Giving expert opinion on DeFi to Cointelegraph, Brendan Blumer concluded *"The real winners in the digital economy will be those that think long-term and take the time to ensure their products meet jurisdictional and professional service requirements."* It certainly looks like exchanges, and software developers, could be in the sights of regulators. We anticipate regulators will look for ways to improve technology quality assurance processes, and DeFi governance, which this can only be done in conjunction with the industry. Mark Taylor emphases that regulators need to continue to work in partnership with crypto industry players to protect consumers.

Julien Bouteluop explains, *"We are actually building in DeFi everything that traditional finance has, but faster, stronger, more transparent and accessible by everyone that's here, it's really different. It means that anyone in the world can access technology, and doesn't need to ask permission from anyone. I think it's necessary to push for innovation, and to build a better world".*

Who and what gets regulated? It's a global 24/7, borderless market. Regulators need to get their thinking caps on and learn to audit code! This is a whole new ball game.

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

Financial Services Commission MAURITIUS

Fintech Series

Guidance Note 2

Securities Token Offerings (STOs)

1. Background

1.1. The Financial Services Commission, Mauritius (FSC), the integrated regulator for non-banking financial services and global business sectors, remains highly supportive of Fintech-related initiatives in Mauritius.

1.2. Following the Guidance Note on the Recognition of Digital Assets[1] as an asset-class for investment by Sophisticated and Expert Investors, the FSC has been receiving queries from stakeholders regarding the statutory requirements applicable to STOs.

1.3. This Guidance Note, the second in the Fintech Series, issued under section 7(1)(a) of the Financial Services Act 2007, highlights the regulatory approach of the FSC in relation to STOs.

2. Regulatory framework for STOs

2.1. "Securities tokens" are "securities" as defined in the Securities Act 2005, represented in digital format.

2.2. An STO generally means the issue of Securities Tokens, as a method of raising funds from investors, in exchange for the ownership or economic rights in relation to assets.

2.3. When STOs are conducted in or from within Mauritius, the offering of such Securities Tokens shall be subject to the Securities Act 2005 and any Regulations or FSC Rules issued thereunder including the requirement for a prospectus, as may be applicable.

[1] The term "Digital Assets" is defined under rule 2 of the Financial Services (Custodian services (digital asset)) Rules 2019. This definition is aligned with the interpretation of the term "Virtual Asset" in The Financial Action Task Force (FATF) Recommendations as updated in October 2018.

2.4. Subject to paragraph 2.5, no offerings of Securities Tokens shall be made without prior approval of the FSC.

2.5. No prior approval is required in respect of offerings to the following categories of investors:

2.5.1. Sophisticated[2] investors;

2.5.2. Expert[3] Investors;

2.5.3. Expert Funds[4];

2.5.4. Professional Collective Investment Schemes[5]; and

2.5.5. Specialised Collective Investment Schemes[6].

2.6. Any person soliciting[7] another person to enter into transactions involving Securities Tokens shall be required to hold the appropriate licence under the Securities Act 2005 and shall be required to ensure, at all times, strict compliance with the applicable regulatory requirements, including, but not limited to:

2.6.1. Undertaking adequate due diligence regarding the STOs

Conducting appropriate due diligence in view of developing a detailed comprehension of the STOs, the fitness and propriety of the management of the issuer as well as its development team and rights and obligations attached to the underlying assets backing the Securities Tokens.

2.6.2. Disclosure obligations

[2] The term "Sophisticated Investor" is defined in section 2 of the Securities Act 2005.
[3] The term "Expert Investor" is defined in regulation 78(a) of the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008 (CIS Regulations 2008).
[4] The term "Expert Fund" is defined in regulation 2 of the CIS Regulations 2008.
[5] The term "Professional Collective Investment Schemes" is defined in regulation 75 of the CIS Regulations 2008
[6] The term "Specialised Collective Investment Scheme" is defined in regulation 77 of the CIS Regulations 2008.
[7] The term "solicit" has the same meaning as in section 31(2) of the Securities Act 2005.

Providing clients with information relating to the STO in an accurate, timely and transparent manner with clear warning statements about the risks associated with the Securities Tokens.

2.7. The FSC wishes to highlight that carrying out financial services[8] without a licence is a criminal offence.

2.8. Service providers, issuers and investors shall comply with the Securities Act 2005, any relevant Acts, Regulations and FSC Rules made thereunder, any other enactment, guidelines, Codes and circular letters as may be applicable.

3. Cautionary note to investors

3.1. Given their high-risk nature, the FSC urges all prospective investors to fully ascertain the related risks prior to committing any funds for investment in Securities Tokens.

3.2. In addition, the FSC hereby informs investors that any investment in Securities Tokens is at their own risks and that they are not protected by any statutory compensation arrangement in Mauritius.

For technical queries, please contact the FSC on *innovation@fscmauritius.org*

08 April 2019

[8] The term "financial services" is defined in section 2 of the Financial Services Act 2007.

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND
FINANCIAL CENTRE

BERMUDA MONETARY AUTHORITY

CONSULTATION PAPER

DIGITAL ASSET BUSINESS ACCOUNTS RULES 2020

JUNE 2020

Table of Contents

I. INTRODUCTION 3
II. COMPOSITION OF DIGITAL ASSET REGULATORY FRAMEWORK 3
III. PROPOSED RULES 4

The digital asset industry, and other interested persons, are invited to share their views on this Digital Asset Business Accounts Rules proposal. Comments should be sent to the Authority, addressed to innovate@bma.bm no later than **31 July 2020**.

I. INTRODUCTION

1. The Bermuda Monetary Authority (Authority) continues to enhance its oversight of Digital Asset Business (DAB) as part of the ongoing development of Bermuda's digital asset regulatory framework. The DAB environment is a new and rapidly evolving space. As such, it is important that Bermuda's regulatory and supervisory frameworks keep pace with the rapid rate of change so as to reflect global best practice.

2. While major accounting standard-setting bodies have initiated work in this area, there has been no comprehensive guidance issued to date for the digital asset sector to follow.

3. In light of this uncertainty, the Authority is proposing to introduce Digital Asset Business Accounts Rules 2020 (the Rules), to provide specific guidance to DAB registrants in Bermuda when preparing their Annual Statutory Financial Returns.

4. The Authority makes these Rules in exercise of its powers conferred by Section 7 of the Digital Asset Business Act 2018 (DABA).

II. COMPOSITION OF DIGITAL ASSET REGULATORY FRAMEWORK

5. The DABA is complemented by a number of supporting Rules, Codes and documents that together form the regulatory framework for DABs. We have included a brief overview of each Rule, Code and document for convenience below:

    a. Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018

    This prescribes the format in which the contents and attachments to the Annual Return are to be reported. Required attachments include audited financials, a business plan for the next financial year and a certificate of compliance to be signed by two directors or a director and an officer. The Annual Return includes a number of quantitative and qualitative information about the business' operations, as well as anti-money laundering/anti-terrorist financing (AML/ATF) and sanctions reporting.

    b. Digital Asset Business (Cybersecurity) Rules 2018

    This prescribes the minimum requirements for the cybersecurity programme of a licensed undertaking. Also, it requires the annual filing of a written report by the Chief Information Security Officer in regards to the undertaking's electronic systems and cybersecurity programme, and a requirement to obtain an independent audit of its systems.

    c. Digital Asset Business (Client Disclosure) Rules 2018
    This requires DABs to disclose important information at the time of entering into an agreement to provide products and services to clients, and with each transaction, including material risks

associated with the DABs products and services, the fees involved, as well as complaints handling procedures in case of operational issues, and other disclosures.

d. Code of Practice
The Code of Practice prescribes a general set of duties, requirements, procedures, standards and sound principles to be observed by DABs in the areas of: governance, risk management, client due diligence and monitoring, integrity and ethics, disclosure of information, internal management controls, outsourcing and cooperation with relevant authorities.

e. Digital Asset Custody Code of Practice
The Code defines a standard for operating as a custodian of digital assets and is to be adhered to by every DAB that maintains or is responsible for the custody of its clients' private keys. These DABs are required to adhere to industry best practices in custody safekeeping, custody transaction handling and custody operations.

f. Statement of Principles
The Statement of Principles outlines the principles by which the Authority is expected to act in terms of interpreting the minimum criteria for licensing and the exercise of its powers to grant, revoke or restrict a licence, as well as the power to obtain and require the production of information and reports and other enforcement powers.

g. AML/ATF Sector-Specific Guidance Notes for DAB
These guidance notes provide additional consideration around the AML/ATF obligations under the Acts and Regulations of Bermuda that are specific to DABs, to be read in conjunction with the main guidance notes on AML/ATF Regulated Financial Institutions.

6. Compliance with the regulatory framework is part of the minimum licensing criteria that DABs are required to comply with on an ongoing basis.

7. It should be noted that it is the Authority's goal that the regulatory framework as a whole sets the tone for sound governance and internal control mechanisms to produce accurate and timely financial reporting information.

III. PROPOSED RULES

8. The proposed statutory financial return consists of a statutory balance sheet and accompanying notes to financial statements.

9. The Rules provide specific requirements to DABs as to the format in which the statutory balance sheet accounts are to be reported, and the disclosures required in the accompanying notes.

10. The Rules also provide guidance to the auditors as to which they are opining on, for the purpose of the submission to the Authority.

11. In the proposed Rules, the Authority has added some accounts that are unique for DAB operations.

BERMUDA

DIGITAL ASSET BUSINESS ACCOUNT RULES 2020

Statutory financial return to relate to the relevant year

1. Every statutory financial return prepared in accordance with these Rules shall relate to the relevant year.

   In these Rules, "relevant year" in relation to a statutory financial return means the financial year end to which the statutory balance sheet relates, which is required to be available or filed under section 7 of the Act.

Contents of the statutory financial return

2. The statutory financial return shall consist of:
   1. An auditor's report
   2. Statutory balance sheet
   3. Accompanying notes to statutory balance sheet date

Auditor's report

3. The auditor's report shall be signed by the licensed undertaking's approved auditor, addressed to the Authority, and state whether in his/her own opinion the statutory balance sheet and the accompanying notes have been prepared in accordance with the Act and these Rules.

   Where any event specified below occurs in relation to an audit, the auditor shall qualify his report accordingly and include in his/her report such observations, whether of fact or opinion, as he/she considers necessary for bringing the nature and effect of the qualifications to the attention of the Authority.

   The events referred to in the paragraph above are that—
   a) There were deficiencies in the financial audit consisting of—
      (i) an inability of the auditor to obtain essential information;
      (ii) restrictions on the scope of the audit;
   b) The auditor disagreed with any valuation made in the statutory balance sheet and accompanying notes;
   c) In some respect or respects the statutory balance sheet and accompanying notes do not, in his/her opinion, comply with the requirements of the Act or any applicable Rules and Code of Practice;
   d) The auditor considered that there was significant doubt as to the licensed undertaking's ability to continue as a going concern; and
   e) The auditor considered any other deficiencies that prevent him/her from issuing an unqualified opinion.

Statutory balance sheet

4. The statutory balance sheet shall be prepared using Form 1SFS as outlined in Schedule I, on an unconsolidated basis, which shall be audited by an approved auditor, starting with the first year occurring after the undertaking has obtained a DAB licence.

Accompanying notes to statutory balance sheet

5. Every licensed undertaking shall set forth in a general note to its statutory balance sheet the matters required in Schedule II on an unconsolidated basis.

Requirements relating to the preparation of statutory financial returns generally

6. All statutory financial returns shall be prepared in the English language. All amounts which, for any purposes of these Rules, are to be shown in any account of any licensed undertaking shall be shown in a single currency, and that currency shall be the currency in which the books and records of the licensed undertaking are kept in the licensed undertaking's principal office in Bermuda or, where different books and records are kept in different currencies in that office, then the currency in which the majority of those books and records are kept.

   Notwithstanding the above, where the Authority, pursuant to Sections 7(1)(f) or Section 31 of the Act, directs the production to it of statutory financial returns and amounts in those returns are shown in a foreign currency, those amounts must be converted into their Bermudian equivalent before the said statements are so produced.

   Where the Authority, pursuant to Section 8(1) of the Act, allows the licensed undertaking to report the statutory financial returns in a different currency other than their Bermudian equivalent, the licensed undertaking shall disclose the exchange rate to convert the amounts to their Bermudian equivalent.

   The Bermudian equivalent of an amount in a foreign currency shall be the Bermudian dollar equivalent of that amount as converted into Bermudian dollars at the rate of exchange used by any licensed bank in Bermuda or any central bank in relation to purchases by that bank of that foreign currency on the last day of the relevant year.

7. For all items shown in any account of any licensed undertaking, there shall be shown the corresponding amounts for the immediately preceding financial year.

Commencement

These Rules come into operation on **31 December 2020** and apply to financial years commencing on or after **31 December 2020**.

SCHEDULE I
DIGITAL ASSET BUSINESS ACCOUNTS RULES
FORM 1SFS
STATUTORY BALANCE SHEET
[blank] name of Licensed undertaking
as at *[blank]* (day/month/year)
expressed in *[blank]* (currency used)

	Assets	20XX	20XX-1
1	**Cash and cash equivalents**	**XXX**	**XXX**
2	**Quoted investments**	**XXX**	**XXX**
(a)	Bonds and Debentures		
	i. Held to maturity	XXX	XXX
	ii. Other	XXX	XXX
(b)	Total Bonds and Debentures	XXX	XXX
(c)	Equities		
	i. Common stocks	XXX	XXX
	ii. Preferred stocks	XXX	XXX
	iii. Mutual funds	XXX	XXX
(d)	Total equities	XXX	XXX
(e)	Other quoted investments		
	i. Digital assets	XXX	XXX
	ii. Digital assets to be issued	XXX	XXX
	iii. Others	XXX	XXX
	iv. Total other quoted investments	XXX	XXX
(f)	Total quoted investments	XXX	XXX
3	**Unquoted investment**	**XXX**	**XXX**
(a)	Bonds and Debentures	XXX	XXX
	i. Held to maturity	XXX	XXX
	ii. Other	XXX	XXX
(b)	Total Bonds and Debentures	XXX	XXX
(c)	Equity investments	XXX	XXX
	i. Common stocks	XXX	XXX
	ii. Preferred stocks	XXX	XXX
	iii. Mutual funds	XXX	XXX
(d)	Total equity investments	XXX	XXX
(e)	Other unquoted investments	XXX	XXX
	i. Digital assets (at cost; disclose fair value in Schedule II)	XXX	XXX
	ii. Digital assets to be issued (at cost; disclose fair value in Schedule II)	XXX	XXX
	iii. Others	XXX	XXX
	iv. Total other unquoted investments	XXX	XXX
(f)	Total unquoted investments	XXX	XXX
4	**Investment in and advances to affiliates**	**XXX**	**XXX**

5	**Investment in mortgage loans on real estate**	**XXX**	**XXX**
6	**Equipment, net of depreciation**	**XXX**	**XXX**
7	**Real estate**	**XXX**	**XXX**
8	**Prepaid expenses**	**XXX**	**XXX**
9	**Investment income due and accrued**	**XXX**	**XXX**
10	**Loans receivable**	**XXX**	**XXX**
	i. Due in one year or less	XXX	XXX
	ii. Due over a year	XXX	XXX
	iii. Total	XXX	XXX
11	**Receivables from clearing brokers**	**XXX**	**XXX**
12	**Other receivables from digital asset business**	**XXX**	**XXX**
	i. Due in one year or less	XXX	XXX
	ii. Due over a year	XXX	XXX
	iii. Total	XXX	XXX
13	**Sundry assets:**	**XXX**	**XXX**
	i. Derivative instruments	XXX	XXX
	ii. Net receivables for investments sold	XXX	XXX
	iii. Goodwill and other intangibles	XXX	XXX
	iv. Other sundry assets 1 (specify)	XXX	XXX
	v. Other sundry assets 2 (specify)	XXX	XXX
	vi. Other sundry assets 3 (specify)	XXX	XXX
	vii. Total	**XXX**	**XXX**
14	**Letter of credit, guarantees and other instruments**	**XXX**	**XXX**
15	**Total assets**	**XXX**	**XXX**
	Liabilities and Stockholders' Equity		
28	**Contractual Liabilities arising from Digital Asset issuance**	**XXX**	**XXX**
29	**Commissions, expenses, fees and other taxes payable**	**XXX**	**XXX**
30	**Loans and notes payable**	**XXX**	**XXX**
31	**Income tax payable**	**XXX**	**XXX**
32	**Amounts due to affiliates**	**XXX**	**XXX**
33	**Accounts payable and accrued expenses**	**XXX**	**XXX**
35	**Dividends payable**	**XXX**	**XXX**
36	**Sundry liabilities**		
	i. Derivative instruments	XXX	XXX
	ii. Net payable for investments purchased	XXX	XXX
	iii. Other sundry liabilities	XXX	XXX
	iv. Total sundry liabilities	**XXX**	**XXX**
37	**Letter of credit, guarantees and other instruments**		
	i. Letters of credit	XXX	XXX
	ii. Guarantees	XXX	XXX
	iii. Other instruments	XXX	XXX

	iv. Total Letters of credit, guarantees and other instruments	**XXX**	**XXX**
39	**Total liabilities**	**XXX**	**XXX**
40	**Stockholders' equity**	**XXX**	**XXX**
	i. Common shares	XXX	XXX
	ii. Preferred shares	XXX	XXX
	iii. Additional paid in capital	XXX	XXX
	iv. Treasury shares	XXX	XXX
	v. Retained earnings, beginning of the year	XXX	XXX
	vi. Net income (loss) for the current period	XXX	XXX
	vii. Dividends declared for the current period	XXX	XXX
	viii. Other comprehensive income (loss)	XXX	XXX
	ix. Retained earnings, end of the year	XXX	XXX
	x. Total Stockholders' Equity	**XXX**	**XXX**
41	**Total liabilities and stockholders' equity**	**XXX**	**XXX**

Schedule II INSTRUCTIONS AFFECTING THE STATUTORY BALANCE SHEET		
Balance sheet line	**Instructions**	
1. Cash and cash equivalents	Cash and cash equivalents (maturities of less than 90 days) as at balance sheet date shall be included here. This includes restricted cash as may be required under government laws or by contract. Any encumbrance on cash or cash equivalents must be disclosed, indicating the amount, custodian bank and any relevant restrictive terms.	
2. Quoted investments	There shall be disclosed severally -	
	(a)	Bonds and debentures –
	(i)	Held to maturity: quoted fixed maturities
	(ii)	Other: quoted fixed maturities shall be included here. Where the bonds and debentures are in level 3 of the investments fair value hierarchy, they should be categorized as unquoted.
	(b)	Equities –
	(i)	Common stock: investments in publicly quoted common shares
	(ii)	Preferred shares: investments in publicly quoted preferred shares; and
	(iii)	Mutual funds: investments in publicly quoted mutual funds, etc.

	(c)	Other quoted investments: i. Digital assets - The fair value and cost of each type of digital assets the licensed undertaking is holding as at the end of relevant year. The licensed undertaking shall disclose the quantity of each type of digital assets held. Licensed undertaking-generated digital assets for future issuance or sales, which have been mined or minted but have not been issued yet shall be valued at **Nil** by default, unless the licensed undertaking, upon application to the Authority can provide a valid cost model to support the recording and valuation of said tokens as an asset. ii. Digital assets to be issued - The licensed undertaking shall disclose the total cost (and fair value if available) of each digital asset, as well as the unit value and quantity. This also includes participations in Simple Agreement for Future Tokens. iii. Other quoted investments not included above e.g. alternative funds which are publicly traded). The method of valuation of must be described. Any encumbrance on quoted investments must also be disclosed.
3. Unquoted investments	There shall be disclosed severally -	
	(a)	Bonds and debentures -
	(i)	Held to maturity: unquoted fixed maturities
	(ii)	Other: unquoted fixed maturities shall be included here
	(b)	Total bonds and debentures: The total of (i) and (ii).
	(c)	Equities –
	(i)	Common stock: investments in unquoted common shares
	(ii)	Preferred shares: investments in unquoted preferred shares; and

	(iii)	Mutual funds: investments in unquoted mutual funds, etc.
	d.	Other unquoted investments: i. Digital assets - The fair value and cost of each type of digital assets the licensed undertaking is holding as at the end of relevant year. The licensed undertaking shall disclose the quantity of each type of digital assets held. Licensed undertaking-generated digital assets for future issuance or sales, which have been mined or minted but have not been issued yet shall be valued at **Nil** by default, unless the licensed undertaking, upon application to the Authority can provide a valid cost model to support the recording and valuation of said tokens as an asset. ii. Digital assets to be issued - The licensed undertaking shall disclose the total cost (and fair value if available) of each digital asset, as well as the unit value and quantity. This also includes participations in Simple Agreement for Future Tokens. iii. Other quoted investments not included above e.g. alternative funds which are publicly traded). The method of valuation of must be described. Any encumbrance on quoted investments must also be disclosed.
4. Investment in and advances to affiliates (equity method)	Unconsolidated Investment in affiliates shall include total investments in affiliates on an equity basis and be reflected in the statutory balance sheet. Advances to affiliates shall be carried at fair value and determined in good faith. If any amount is in the opinion of the directors uncollectible, that amount shall be deducted. For the purposes of this Schedule, an "affiliate" refers to an entity as defined under Section 86 (3) of the Companies Act 1981.	
5. Investments in mortgage loans on real estate	Residential and commercial investment loans shall be included here.	
	There shall be disclosed severally, indicating both the cost and fair value of	

	(a)	First liens.
	(b)	Liens other than first liens.
	(c)	Total investments in mortgage loans on real estate: The total of (a) and (b)
6. Equipment, net of depreciation	Disclose cost and accumulated depreciation and a general description of the equipment held, including expected useful lives.	
7. Real estate	Commercial investments occupied by the licensed undertaking shall be included here.	
	(a)	Occupied by the licensed undertaking (less encumbrances): Both land and
		buildings and any other commercial investments occupied by the licensed undertaking shall be included here.
	(b)	Other properties (less encumbrances): Other residential and
		commercial investments.
	(c)	Total real estate: The total of (a) and (b).
	(i) the method of valuation; and (ii) where there are encumbrances, the value of the real estate before encumbrances, the amount and nature of the encumbrances and the repaying terms and interest rates applicable to the encumbrances, shall be disclosed.	
9. Investment income due and accrued	Accrued investment income shall be included here.	
10. Loans receivable	Description and amount of the loans receivable must be disclosed. The licensed undertaking shall also disclose the portion of the loans which have been issued using digital assets, disclosing the amount, the terms and the valuation method used to determine fair value.	
11. Receivable from clearing brokers	Disclose the nature and usual terms of business, indicating the expected collection or settlement period, whether it is within one year or beyond.	

12. Other receivables from digital asset business	The licensed undertaking shall disclose the nature and amount of any amounts reported, disclosing whether the expected collection period is within one year or more. The licensed undertaking shall also disclose the valuation method used to determine fair value.	
13. Sundry assets	The nature and terms of these assets. There shall be disclosed severally –	
	(i)	Derivative instruments with a favourable position shall be included here. Disclose nature of the instrument and relevant terms as appropriate.
	(ii)	Net receivables for investments sold
	(iii)	Goodwill and other intangible assets - Intangible assets can be recognised and measured at a value other than zero only if they can be sold separately and the expected future economic benefits will flow to the Licensed undertaking and the value of the assets can be reliably measured. These assets must be separable and there should be evidence of exchange transactions for the same or similar assets indicating that they are saleable in the market place. If the value assessment of an intangible asset cannot be reliably measured, then such asset should be valued at nil.
	(iv)	Other sundry assets (please specify)
	(v)	Other sundry assets (please specify)
	(vi)	Other sundry assets (please specify)
	(vii)	Total sundry assets: The total of (i) to (vi) inclusive.
14. Letters of credit, guarantees and other instruments	This shall be comprised of contractual rights arising from off-balance sheet arrangements to receive financial assets through Letters of Credit, Guarantees, and Other Instruments.	

28. Contractual Liabilities arising from Digital Asset issuance	Consist of any contractual obligation to be settled in cash or other financial assets arising from issuance of digital assets. This would include any contingent settlement provision to deliver cash or another financial asset which solely depends on the outcome of an uncertain future event, whether or not the licensed undertaking has the ability to settle the contractual obligation. The licensed undertaking shall disclose the total value of obligation in fiat or the value and quantity of digital asset if the contractual obligation is to be settled as such. For digital assets issued with dual purposes, for example a digital asset which can be exchanged for services or has convertibility feature to ordinary shares at the holder's discretion for a set rate, the licensed undertaking shall disclose a breakdown of the digital assets with a description of the privileges and rights, including the right to vote (if any), to receive future dividends or to convert said token into common or preferred shares.	
29. Commissions, expenses, fees and taxes payable	Indicate the nature and terms of these payables here. The Licensed undertaking shall also disclose where there are any portion of this liability that is payable in digital asset, outlining the unit value and fiat conversion rate used	
30. Loans and notes payable	Loans and notes payable shall be included here. This shall include subordinated debt. The licensed undertaking shall also disclose where there are any portion of this liability that is payable in digital asset, outlining the unit value and fiat conversion rate used.	
31. Income tax payable		There shall be disclosed severally
	(a)	Income taxes payable
	(b)	Deferred income taxes
32. Amounts due to affiliates	This shall be comprised of the affiliate's name, repayment terms, rates of interest and that nature of collateral given, if any on a per instrument basis. The licensed undertaking shall also disclose where there are any portion of this liability that is payable in digital asset, outlining the unit value and fiat conversion rate used. For the purposes of this Schedule, an "affiliate" refers to an entity belonging to the same group of companies in which the licensed undertaking is a part of.	

<table>
<tr><td>33. Accounts payable and accrued liabilities</td><td colspan="2">All accounts payable and accrued liabilities shall be included here. The licensed undertaking shall also disclose where there are any portion of this liability that is payable in digital asset, outlining the unit value and fiat conversion rate used.</td></tr>
<tr><td>35. Dividends payable</td><td colspan="2">All dividends payable shall be included here. The licensed undertaking shall also disclose where there are any portion of this liability that is payable in digital asset, outlining the unit value and fiat conversion rate used.</td></tr>
<tr><td rowspan="5">36. Sundry liabilities</td><td colspan="2">There shall be disclosed severally:</td></tr>
<tr><td rowspan="2">(i)</td><td>Derivative instruments: Derivative instruments with an unfavorable position shall be included here.

The licensed undertaking must also disclose a description of the policies surrounding the use of derivatives; and</td></tr>
<tr><td>the market value and nominal exposure of each derivative by issuer with nominal exposure greater than 5% of the aggregate sum of the total quoted and Unquoted investments. Disclosure should be separated between long and short positions.</td></tr>
<tr><td>(ii)</td><td>Net payable for investments purchased; and</td></tr>
<tr><td>(iii)</td><td>Sundry liabilities (please specify)</td></tr>
<tr><td>37. Letter of credit, guarantees and other instruments</td><td colspan="2">This shall be comprised of contractual obligation arising from off-balance sheet arrangements to receive financial assets.

All contractual liabilities or contingent liabilities arising from off-balance sheet arrangements are reported in this line. A liability is recorded decreasing the statutory capital and surplus equal to the present value of such contingent obligations discounted to take into consideration the time value of money at an appropriate rate (to be disclosed). Where the present value of contingent obligations cannot be determined, the amount of the liability must be recorded at its undiscounted value. There shall be disclosed severally –

a. Letters of credit
b. Guarantees
c. Other instruments
d. This shall be the total of (a) to (c) inclusive</td></tr>
<tr><td></td><td colspan="2"></td></tr>
</table>

40 i. Common shares	This shall comprise common shares issued by the licensed undertaking. The licensed undertaking shall disclose the par value, number of shares authorized, and issued and outstanding. The Licensed undertaking shall also disclose any conversion provisions, if applicable.
ii. Preferred shares	This shall comprise preference shares issued by the licensed undertaking. The aggregate liquidation value is also required to be disclosed. The licensed undertaking shall disclose par value, number of shares authorised, and issued and outstanding, including whether the shares are cumulative or non-cumulative.
iii. Additional paid in capital	This shall comprise of contributed capital in excess of par value. Contribution made to additional paid in capital from shareholders shall be added to this line and capital distributions to common shareholders shall be deducted from this line.
iv. Treasury shares	This shall comprise of treasury shares issued. The licensed undertaking shall disclose the number of shares and cost of treasury shares purchased.
v. Retained earnings, beginning of the year	This shall be equivalent to retained earnings (deficit) at the beginning of the year.
vi. Net income (loss) during the period	Consist of net results of operations for the period ended.
vii. Dividends declared	This shall be comprised of all dividends declared during the relevant year, whether such dividends were or were not paid before the end of the relevant year. The licensed undertaking shall also disclose the amount and nature of any dividend paid during the relevant year that was other than a cash dividend, such as stock dividend or dividends in the form of digital assets.
viii. Other comprehensive income (loss)	This may include any unrealised appreciation (depreciation) of investments as well as changes in any other surplus. The licensed undertaking shall disclose the nature of such adjustments to any other surplus.

	Schedule III **NOTES TO STATUTORY BALANCE SHEET** **Matters to be set forth in a General Note to the Statutory Balance Sheet**
1	• Licensed undertaking information, including date of incorporation, license and any regulatory approvals obtained in Bermuda or abroad, as well as products/services authorized under said license(s). • The name of the shareholder controllers of the licensed undertaking. • Changes to the shareholder controller(s); or to the place of the incorporation of a licensed undertaking's affiliates during the relevant year, in this regard, provide the date and details of such change.
2	Description of the licensed undertaking's governance, risk management and internal controls, in relation to the following financial and control assertions, as applicable: • Existence of digital assets reported in the Balance sheet • Safekeeping and custody of digital assets • Segregation of client assets
3	Summary of accounting policies adopted, and the accounting standard in which it is based upon, particularly on: • Fair value definition • Valuation methods and sources used in determining fair value of digital assets – Indicating the digital asset Exchange used, the unrealized gain or loss borne by the licensed undertaking, if any, and the cut off time used at end of the relevant year. • Active market definition • Any significant changes made during the relevant year to such policies and the effect, if any, of changes to the information contained in the financial statements.
4	The basis of recognition of revenue from performing the digital asset business undertaking.
5	• The currency in which amounts are shown in the licensed undertaking's statutory balance sheet and accompanying notes and whether that currency is the currency in which those amounts are required by paragraph 5 to be shown; • the rate or rates of exchange used in compliance with paragraph 5 for the purposes of financial information required by these Rules; • The method used to translate amounts denominated in currencies other than the currency of the statutory balance sheet and accompanying notes, the amounts, if

	material, gained or lost on such translation and the manner in which those gains or losses are recorded in those statements.
6	Liquidity and capital resources
7	The gross amount of arrears of dividends on preferred cumulative shares, and the date to which those dividends were last paid.
8	Breakdown of investments based on the following fair value hierarchy: • Level 1: Quoted prices (unadjusted) in active markets for identical assets and liabilities that the reporting entity can access at the measurement date • Level 2: Inputs other than quoted prices in active markets for identical assets and liabilities that are observable either directly or indirectly • Level 3: Unobservable inputs
9	The contractual maturity profile of the licensed undertakings' fixed maturity and short-term investments: • Due within one year • Due after one year through five years • Due after five years through ten years • Due after ten years
10	Related party transactions should be disclosed, detailing the nature of the relationship, description of transactions including transactions where no amounts or nominal amounts were ascribed, monetary amounts of transactions for each of the periods for which the licensed undertaking's financials are presented and the effects of any change in the method of establishing the terms from that used in the preceding period, and amounts due from or to related parties as of the date of each balance sheet presented and, if not otherwise apparent, the terms and manner of settlement. • The amount of any loan made during the relevant year by the licensed undertaking, to any director or officer of the licensed undertaking, not being a loan made in the ordinary course of business.
11	<u>Contingencies and Commitments</u> The nature and amount of any material contingencies or commitments made by the licensed undertaking.
12	<u>Subsequent events</u> Any transaction made or other event occurring between the end of the relevant year and the date of approval of the financial statements by the board of directors and materially affecting the financial statements, not being a transaction made or an event occurring in the ordinary course of business.
13	Any other information which in the opinion of the board of directors is required to be disclosed if the statutory balance sheet and accompanying notes are not to be misleading.

PROVIDED BY ADC FORUM TO
SENATE SELECT COMMITTEE
ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

Digital Asset Market Place-FSC guidelines May 2021 (For sophisticated/Institutional participants only) Digital Asset Marketplace Regulation May 2021

Foreword:

From 2018 to 2021, the appetite for retail investors and users of digital assets, especially in the area of peer-to-peer transactions of virtual assets (VA's) and growth of virtual asset service providers (VASPS) has grown exponentially. Digital asset marketplaces (including virtual (crypto) currencies exchanges) are becoming more and more sophisticated and mainstream. Social adoption, especially in the emerging world is high. Policy amendments are needed for Mauritius to capitalise on this. The regulations of a digital asset marketplace, in the context of both institutional and retail clients of this paper would remain by and large the same. If the Digital asset marketplace licensee is to conduct business in both the retail and institutional space the main point of difference would be disclosure rules (to the general public) and a "buyer beware caveat". Also, in a retail peer to peer context the digital asset marketplace licensee could be both custodian and platform provider. There is no requirement for clearing and settlement, as the assets are atomically swapped between the buyer and seller. The digital asset marketplace licensee is the platform where buyers and sellers are matched, no novation takes place, and the platform acts a merely a matching engine. All transactions are prefunded. The same methodology to virtual assets (namely crypto currencies) applies as to the regulating of securities token platforms the FSC (Mauritius) has already issued guidance notes on.
As the ecosystem grows, new digital assets are added to the platforms. Non-Fungible Tokens (NFT's) are the latest assets as the sweet of product offerings grows and become more sophisticated.

Policy makers will need to address this within the drafting of the new legislative requirements for the Digital Asset Act 2021. In the view of the author of this document, the participation of sophisticated investors and institutional investors needs to widen to include retail investors.

Methodology of operations of a digital asset marketplace

Background:
For the purpose of this guidance paper Institutional and sophisticated investors are referenced only.
The digital asset marketplace under current recommendations cannot accept retail money or investors as per recommendations of Fintech and innovation-driven financial services, Regulatory Committee (April,2018).

1.Methodology of guidance notes for licencing requirements for a Digital asset marketplace for sophisticated and institutional investors only

For the purposes of this paper:

The digital asset marketplace will use existing institutional brokers who are already fully regulated entities for financial markets

Sophisticated investors can access the digital asset marketplace directly or have direct market access depending on which class of investors are allowed
-if retail are investors are allowed in the future, direct access to the digital asset marketplace is allowed after appropriate KYC and due diligence obligations are met. (see peer to peer considerations)

In the context of an institutional grade marketplace, the KYC and enhanced due diligence requirement is already fulfilled with existing rails
Institutions will be directed to use brokers however, in rare circumstances individuals who are deemed sophisticated investors can be granted direct Market place access.

The guidance is principle based.

ONBOARDING PROCESS

All online and digital

REGISTRATION PROCESS ONBOARDING OF CLIENTS

Stage One

1. Individual
2. Corporate

Both complete registration form

(Enhanced due diligence and enhanced KYC for individuals and corporates not already KYC'ed through brokers)

3. Site visitors
4. Registration process complete then login process
5. Stage 1 (validation checks, AML/CTF procedures followed in line with jurisdiction laws (world check, watch lists, PEPS and associated fraud lists
6. Choice of validation of transactions
7. Acceptance of T&C's, check box
8. Email/Pin/SMS 2 x step authentication. validation
9. Via the above process email and mobile confirmation links /codes sent to customer

Stage Two

Validation checks:

These include email links, Master authentication PIN set up

SMS code -correct code-upload of KYC Documents, transaction questionnaire completion

These processes have two attempt limits, as with bank regs multi fails suggest potential frauds.

- Customer watch lists must be updated
- Link monitoring data to blacklist
- Report suspicious transactions of over $10 000 USD to relevant authority
-

TRADING ON THE EXCHANGE

Order Matching

As in line with IOSCO Principles rules for market conduct and surveillance apply

Although the asset is decentralised itself for purposes of institutional trading the trading platform would have traditional order book features such as a central limit order book, one for each digital asset traded on the exchange (digital asset marketplace).

The order book should follow a price time priority model

The order book is a list of buy/sells sorted by price and timestamp

NEW ORDER METHODOLOGY

When a new order is received it is checked against the other side of the market (e.g., for new buy order check the sell side orders to see if there are

Are any orders matching the conditions imposed by the new order. If this is the case the trades will be "matched". The trades will continue to be generated until a trade happens or the conditions are invalidated, or the order is filled

The Institutional clients of the exchange are given access to the order book through a web interface.

This enables the user to access multiple order types and multiple order execution options available through the interface to facilitate trading strategies.

The most common types of orders that are available:

1. Limit order the most used orders in the current crypto exchange environment. They allow the user to create an order with a specific price that gets filled at that specific price or better.
2. Market order. Market orders prioritise completing the order for the specified amount ignoring the price. they take priority in the order book, and they guarantee fulfilment (fills) in markets with sufficient liquidity
3. Stop orders. Stop orders become active only after a specific price level is reached. In this manner, they work in opposite to a limit order. Once activated they are automatically converted to market or limit order.

The matching engine is comprised of multiple "client orders" that are components of the digital asset marketplace (exchange) which receive order requests from end users, validates them against their available funds and sends them to be matched.

The communication between the client and the matching engine should be done through a series of messages sent over a highly specialised real time data streaming pipelines in strict order. This is essential as it ensures that when an order is accepted onto a messaging queue it will be processed in the same order by the engine as well.

As these digital asset places (exchanges) do not "novate "trades as do traditional exchanges there needs to be technology components built into the matching engine that can recreate the order book as a disaster recovery mechanism should the system crash and or need to be rebooted.
Through a series of complex algorithms, the matching engine's job is to listen to the message stream, execute the command on the order book hash it and publish the result in the form of a message that can then be sent back to where the user is configured to manage their ledger.
Mauritius has already issued guidance notes on custody of digital assets. It would be recommended that any licensed digital asset marketplace holder is also the custodian of such assets. It is further recommended that the Hardware security module (HSM) resides with the custodian, to which the exchange is linked via an API
The configuration of these marketplaces is based largely on traditional market infrastructure configuration with enhanced security and data protection modules.
It is also to be noted these marketplaces operate 24/7 unlike traditional asset exchanges. Hence enabling continuous order markets there should be the provision for the market participants to be offered by the digital asset marketplace providers an auction market option.
Unlike other asset classes, digital assets can often be very illiquid and hence price discovery almost impossible. These auction mechanisms are similarly used by traditional stock exchanges for the market to reach a final auction price which is established as the price that executes the greatest aggregate quantity and minimises the imbalances between buy and sell orders across both the auction and continuous order books.
This mechanism is no different to what Nasdaq, ARCO, LSE and most other world federation of exchange members do.
Similarly institutional investors demand block trading facilities.
IOI (indication of interest) facilities are important for takers of block trades

The taker specifies:
1.buy/sell
2.quantity
3.Minimum required fill quantity and price limit
Market makers only receive the quantity, minimum required fill quantity and collar price
*EFP's operate in largely the same way in fixed income markets and may be replicated as the model later.

ON RAMP AND OFF RAMP OF FIAT CURRENCY INCLUDING PRICING

All fiat deposits are to be held in segregated (escrow) accounts.
AML/CTF/KYC requirements and consumer protection applied to all deposits
Suspicious transactions over $10000 USD are to be reported to the appropriate regulatory authority.
AS PER THE FSC GUIDENCE NOTES
Each exchange must propose an institutional architecture on all participants in the ecosystem. There will be no FIAT ON/OFF ramps directly to the exchange.
As per conventional exchange norms the only activity that the exchange performs is the order matching
No process of novation occurs on such digital asset marketplace which is the defining difference between such marketplaces and traditional market infrastructure.
Settlements (using blockchain T+0) of matched trades happens off exchange.

Models:

Brokers can use a licensed custody provider of digital assets
The custodian connects to exchange via API
The digital asset marketplace licence holder can connect to banks through CPI compliant API interface
Once a trade has taken place on the platform a message is broadcast via the relevant API to the banks and custodians to carry out settlement process off exchange.
If a broker transacts with the Digital asset marketplace as the market maker, the custodian will be sent a message to wire the fiat payment of the crypto asset into the Digital Asset marketplaces account.
If two brokers transact on the platform (buy order from. One broker, sell from another) the buyer's custodian will be instructed to send fiat to the bank account of the selling brokers customer.
RELATIONSHIPS with brokers, other intermediaries and banks:
Regulated brokers will be majority of trade volume on these digital asset marketplaces (some Sophisticated high net worth individuals). All will have direct market access to both the exchange and the custody providers that will work through API's.

Life cycle of trades:

The exchange will accept all PCI DSS compliant API interfacing with both domestic and international banks.

The Digital Asset marketplace will only ever receive fiat deposits from regulated brokers or existing high net worth customers and only make payments to either brokers or clearing banks

DETAILS OF SYSTEMS and CONTROLS

-INFRASTRUCTURE
-SECURITY
-SAFEKEEPING MECHANISMS of DIGITAL ASSETS traded on platform

The Digital Asset Market place should be protected by multiple security layers, including 2 finger authentication, hardware security, anti-phishing features, geofencing that can detect VPN's and TOR nodes, multiple levels of database encryption, DDoS mitigation, network and trade anomaly detection.

Trade anomaly detection uses machine learning to analyse pre -trade and post-trade stat to identify suspicious activity including pass through trades, wash trades, spoofing, stuffing, hammering, momentum ignition and money laundering allowing administrations to freeze accounts as needed and generate suspicious activity reports for regulators

Any software that us used or developed by the platform needs to have undergone independent penetration testing and source code analysis.

It is important that these platforms have global grade institutional systems ensuring the jurisdiction is globally competitive.

It would be advised that each digital asset marketplace holds a custody licence to ensure the highest level of safety and accessibility of client's digital assets is maintained.

As per custody requirements, multi-signature wallets are used between the exchange and the client. Both shall hold one key; a third key should be stored on a HSM (hardware security module also called cold wallets) With the custodian

The methodology for this:

The wallet is said to be a 2nd or 3rd multi signature wallet, as 2 out of the 3 keys are necessary to access the funds on the wallet.

This will allow the digital asset marketplace users to have full access to their digital assets as well as guarantee of their safety.

It is of the utmost importance that custody of these client funds is secured completely separately from the exchange platform as it mitigates the risk of a hack or a theft on the exchange.

DETAILED AML/CTF PROCEDURES

FATF methodology takes into consideration the industry specific risks and adds controls that need to be put in place including:

1.CDD systems and procedures
2.Detection of suspicious / fraudulent transactions

*Must refer and adhere to FSC Mauritius "anti-money laundering and countering of terrorist financing compliance manual

*Best practises and substance requirements must also apply to the digital asset marketplace operations

As noted over 2020-2021 with Mauritius under review for FATF rec 15 and rec 5 further procedures and processes may be developed and customised according from time of writing this paper. All updates must be added as further recommendations to those who apply

All digital asset marketplaces that apply to be regulated inn Mauritius must have a partner or in-house ability to source for any flagged addresses / wallets from which crypto assets

A partner or inhouse blockchain investigative tool is paramount for this regulation

Both law enforcement and financial institutions must be able to have a comprehensive view of the public blockchain ecosystem and use advanced analytics and data scraping techniques used in cryptography to map suspicious transactions and related entities.

These new and advanced tool kits created by blockchain technology uses a wide range of state-of-the-art features that help investigations on the blockchain be done very effectively.

It is important to note bitcoin is not anonymous, as often cited. Blockchain is in fact just a large data base that is distributed. It is also the most secure database in existence and its immutability and transparency make it reliable to track and trace all transactions since the genesis (first) block of Bitcoin was created.

Public blockchains contain vast amounts of data, investigative software can scrape all public networks and analyse to look for patterns of fraudulent activity.

One feature of the blockchain is that its data is typically not limned to a specific person (although FATF rec 15 now requires that all digital asset marketplaces and (VASPS) must know the beneficial owner and receiver of digital assets behind wallet addresses.

For this reason, deep analytical forensics beyond the blockchain layer are required to source information on bitcoin addresses in other ways. These sources include website like forums, social media channels and any other platform where blockchain users congregate or addresses have been published and publicised.
Licence holders must prove, that they are able to unveil an entity address as well as their name in the real world.
Bitcoin is best known for its secure protocol and although it was designed to protect the privacy of the user, it was never intended to be completely anonymous. It has 2 characteristics that ensures every transaction leaves a Digital footprint and that be followed by accountants and digital investigators.

1. All valid transactions must be on the blockchain and therefore accessible to anyone (Public blockchain)
2. The blockchain is a digital network

The digital footprint on the blockchain can be used to form the bedrock k of KYC/AML procedures that can be used by financial institutions and service providers to effectively police against bad actors attempting to Lauder the proceeds of bitcoin procured through illegal activity.
Bitcoin and the blockchain can provide significant for regulatory bodies and law enforcement as the blockchain allows all trace all transactions involving a bitcoin address of interest back to the very first transaction (genius block)." Following the money "is much easier with bitcoin than ever possible with cash.
In recent years there have been several academic studies and guidelines issued by OECD. IMF, OSCE and FATF that have outlined different techniques that have outlined different techniques that can be used to de anonymize the bitcoin system so that is it is possible to detect with a high degree of certainty whether a bitcoin has been used or originates from an illicit or suspicious activity.
The use of these techniques effectively is a highly complicated process, with time and computer resource intense.
Consequently, a number of these business service providers have emerged such as Chain analysis, blockseer, elliptic, Bitfury, bold, Numisight, and score chain to name a few.
These companies have taken the ideas from this research and used it to offer commercial professional services that enable Fintech and financial service companies to ensure that any bitcoin or other crypto asset has not be used or originated in illicit or suspicious activities.
There are many different variations of primary techniques to derive a credit /risk score for the bitcoin they apply their services to. These principles are found on examination of various types of identifiers on the blockchain and searching for references to those identifiers on the wider internet and form links that can be used to associate users with transactions and therefore highlight any coins that may have been used in known illicit transactions.
Analysis on the blockchain can be executed using two different techniques, transactions graphic analysis and traffic analysis. Both methodologies are focused on identifying patterns of cluster transactions around wallets using network flow algorithms to help find patterns that are effective tools such as community findings, block modelling, network flow algorithms to help find patterns that are effective in identifying any number of transactions between any number of different wallets to the same identity.
Once a source has been identified it then falls to already well-established techniques developed by cybercrime fighters to link IP addresses, MAC addresses or physical locations to wallets and identity. Many of the companies mentioned above are required in the chain for regulations of Digital Asset marketplaces have deep understanding of how the businesses offering services (VASPS) in this area use different variations of the fundamental techniques used to deanonymize the blockchain.
They are used to develop a detailed risk scorings mechanism that helps highlight to clients any Bitcoins that may have been used in suspicious transactions associated with a previous address or a point of withdrawal. Risk scoring is based on using the above mechanisms to identify and group originators of illicit bitcoin and identity and group conversion services that are commonly used to hide the origin of illicit bitcoin

NUMBER OF ILLICIT ENTITIES CONSIDERED BY TYPE>

Darknet marketplaces
Darknet services
Darknet Vendors
Fraud activity
Ponzi schemes
Ransomware (FIGS DIFFER SLIGHTLY BETWEEN VASPS)

NUMBER OF CONVERSION SERVICES CONSIDERED BY TYPE>

Bitcoin ATM operators
Bitcoin exchanges * Market Places
Crypto exchanges * Market places
Gambling service

Mixer
Multi Service
As a result, all VASPS and digital asset marketplace licensees and custodians must work with these Service providers. Regulation will require this to ensure that no cryptocurrencies and bitcoin that are been offered by potential market participants have been touched by other of these groups and consequently ensure the integrity of this regulatory framework for Mauritius and has mitigation of reputational damage to the jurisdiction.

EXPLANATION NOTE: SCENARIO WHEREBY A POTENTIAL CLIENT PASSES THROUGH CDD SCREENING BUT THE CLIENT'S DIGITAL ASSET IS TAINTED>

If a digital asset of a client is tainted when about to come onto the trading platform of the Digital Asset market Place for the first time the account/wallet holding will be immediately frozen.
Compliance team of the licensee must inform the potential client. If the Digital asset were to become tainted whilst already on the platform (e.g., new inclusion on a watch or blacklist) the assets MUST be frozen by the compliance division, and they must contact the client immediately and regulatory body as to next steps. A regulatory requirement must be the digital asset marketplace platform must and appropriately fully co-operate with the authorities.

DETAILS OF ARRANGEMENTS TO ENSURE CONFIDENTIALITY< SECURITY AND RELIABILITY OF CLIENT(S) INFORMATION

Regarding reliability, trusted third parties offering solutions for identity and document verification must be engaged to ensure this information is reliable and the appropriate partnership docs given to the regulator.
All critical information should be encrypted and stored on cloud servers at blue chip providers such as Amazon web Services. In addition, in order to deal with the Human risk, factor no staff member of the licensee should ever have access to all customer data.
As well as the risk of user accounts being hacked there is also the risk that malicious users will attempt to impersonate legitimate users. This is often done by stealing credentials, bypassing the security controls and internal threats etc. A malicious employee could change the withdrawal address in accounts and redirect Bitcoin withdrawals to his own wallet.
The Digital Asset Market Place must control identity theft by:
-use of best practice library for all user's accounts
-always require 2 finger authentications for all withdrawals using SMS authentication
-Always require a real ID validation to enable traders over a certain amount
-require than withdrawals and/or deposits over a certain amount requires administrator approval
If a malicious employee can copy the private key for a wallet during normal operation and its transfer out it'd contents without any access to the system, it can be difficult to identify the source of the leak in many scenarios. The security measure needs to consider 5 types of security risk
-application privilege escalation
-Server/cloud service compromise
-Administrative account compromise
-Internal threats -malicious staff and developers
-External account (bank accounts, third party linked accounts) compromise
A detailed description and risk mitigation strategy must be provided by the applicant and the measures place to counter risk
External threat mitigation
-component isolation
-circuit breakers/alert systems
Real time visualisations
-DDOS protection

Physical security measures (crypto /fiat asset protection)

-air gap machines; cold storage is used to store the Digital Asset marketplace reserves
-Multi signatures are required to access the "reserve' cold storage wallet of the platform
-a separate cold storage wallet is used to maintain the operating profits
-all could servers are encrypted
-Physical (paper) logs and signature are required to authorise cold storage and large withdrawals operations

Systems/data integrity

-This is the risk of a malfunction rather than a malicious risk. The threat is that the software or hardware malfunctions which may result in an inconsistent or corrupt state.

An example would be if a user withdraws money from a wallet whilst at the same instant the wallet makes a purchase larger than the remaining balance in the wallet, both transactions may go through. Again, the mitigation and controls to address these threats must be set out in detail to the regulators
-Atomic transactions
-sanity checking
-integrity checks
-backup automation
-human escalation

DETAIL FOR DERIVATIVE MARKET ADD ON

Futures and derivatives markets in traditional markets have always complemented the cash products that underlie them
Given these regulations are guided towards only institutional and sophisticated investors in markets sense to regulate beyond vanilla cash products.
These market participants have demands and investment needs that go beyond vanilla spot markets.
Only OTC derivatives are offered at present to this new asset class.
A derivatives framework which aims to target what is done OTC.
In this regard, as the asset class becomes more mature and diversified, standardisation of contracts, efficiency and transparent pricing enhances market conduct, best practises and most importantly reduces risk.
Given crypto assets trade 24/7 the margin risk management of these products offers various pros and cons to traditional and conventional markets but with technology advancements and post trade risk reduction through atomic swapping of assets on the blockchain at T+0 in essence, these products are significantly safer to manage.
In broader regulatory terms, it best to start with vanilla options initially only on BTC to facilitate the existing demand for this in the current market.
Options can be linked to the BTC price on an index and cash (physically) settled at expiry.
It is suggested a separate consultation paper be prepared after discussions with different market participants and the regulator Start preparation work one contract standardisation, size, expiry and EFP trading.

CAPITAL REQUIREMENTS/EVIDENCE of SOURCE OF FUNDS/ESCROW REQUIREMENTS and SHAREHOLDING

As per relevant act to be released in Mauritius, head office and directors must be in jurisdiction
Beneficial owners are subject to both criminal and regulatory liabilities if they act nefariously or breach the relevant law governing these activities.
As in line with other Guidance notes issued on Digital assets, custody of Digital assets ad custody of digital assets capitalisation should be USD $1 million ore equivalent.
Setup costs will vary however, from market research these platforms cost approx. USD$ 500000
The escrow however, given high risk nature of the platform should sit around USD $5 million
Operational and interface configuration costs will vary
Custodian licence costs need to be included
All shareholders, beneficiary owners, directors must adhere to producing relevant documentation as per FSC Rules across licence holders

FIT AND PROPER MANAGEMENT AND KNOWLEDGEABLE PERSONS AND TECHNICAL EXPERTISE and QUAILIFIED CTO

Given the nature of the industry, unique globalised reach and in-depth technical knowledge required to run a digital asset market place the management teams must show in-depth new market and market infrastructure knowledge.
The CTO should be knowledgeable in technical aspects of the exchange from an operational perspective
Compliance officer with in-depth knowledge of compliance from both a traditional and blockchain perspective is a requirement.

DETAILS OF PROPOSED OUTSOURCED FUNCTIONS:

IP should be in-house,
For professional services like, accounting, legal, corporate advisory and broking requirements can be both in house and outsourced to recognised service providers, brokers, management companies and financial institutions. Audit requirements see below.

OPERATIONS

A local Mauritius entity must be set up to manage the full operations of the Exchange in jurisdiction.

DETAILED BREAKDOWN OF OPERATIONAL < TRADING>CLEARING>SETTLEMENT>MAIN EXCHANGE>DERIVATIVE AUDITOR

The licensee must appoint an independent Auditor. The auditor must have conducted a readiness assessment of the digital asset marketplace business and the risk and compliance processes behind its operations and financial statements.

EXCHANGE AND CLEARING

1.After matching trades, the exchange sends trade data to the clearing house (CCP) (not as per traditional model) T+0

-All trades due for clearing are netted by CCP, this is a singe net amount in cash and digital assets due to or from the participant. Taxes, commissions, dividends and interest are included in netting

-CCP sends clearing data to the Digital Asset marketplace which receives and verifies the data

After immediate reconciliation clearing participants prepare assets or funds for settlement based one the clearing results.

2.Cash payables are deposited into cash clearing accounts

Digital assets are deposited into these accounts at CSD. CCP is informed accordingly.

Settlement takes ace at the CCP. Assets are transferred from the sell side participants digital asset account to the central securities settlement account at CSD and from the account at CSD to the buy side participants digital asset account.

Funds are then transferred accordingly.

POST SETTLEMENT

-Settlement results are sent to the clearing house to participants and Exchange for reconciliation * settlement is T+0

-Participants provide clients with account balance enquiry service and cash withdrawals based on reconciliation results

-The Digital Asset marketplace can perform pre trade monitoring based on the settlement results

CHAIN OF PARTICIPANTS

-Investors> broker and custodian >EXCHANGE/CH/CSD/CFSA>Selling investors>broker and custodian

2.Methodology of guidance notes for licencing requirements for a Digital asset marketplace for peer to peer and retail.

Regulatory considerations: licensing and authorization peer to peer

Digital asset marketplaces (often referred to as “exchanges” by the industry, are internet-based platforms designed to facilitate the trading of digital assets and accordingly they can access customers across the world with a relatively limited physical footprint in any single jurisdiction.

Traditional exchanges and trading platforms are subject to laws and regulations (usually in the form of a licensing or authorisation regime) in the jurisdiction(s) in which they operate and/or market and the intermediaries (brokers/trading and clearing participants) who can access the platform also usually need to have some form of license or authorisation.

Digital asset marketplaces are direct-to-customer platforms and typically operate without the need for intermediaries to place orders on behalf of their users or hold users’ assets in custody. As such, a digital asset marketplace can function as a broker, custodian and trading venue at the same time.

Since 2018, Mauritius has shown interest in regulating the space and are increasingly scrutinising these marketplaces on two fronts; firstly, to ensure that digital asset marketplaces are not facilitating trading in regulated financial products (e.g., tokens which have the characteristics of securities (See FSC guidance note 2019)

without holding the appropriate license or authorization and, secondly, to understand how these businesses market their services to potential customers and whether such marketing activity itself constitutes some form of regulated financial activity for which a license or authorisation is required. Other features, such as the provision of leverage, have also triggered regulatory scrutiny.

The regulatory sandbox was set up to address these concerns.

These issues are exacerbated by the absence of any internationally harmonised view of token characterisation, meaning that a token which is not classified as a ‘security’ (or other regulated product) in the jurisdiction of Mauritius might be classified as a ‘security’ (or other regulated product) in another jurisdiction. Additional features and services, such as leverage, derivatives, futures etc., are also subject to jurisdictional differences.

Digital asset marketplaces businesses have challenges presented by the patchwork of varying international approaches to regulation.
In order to establish compliant but also commercially efficient, scalable platforms this ecosystem needs to regulated in a jurisdiction that gives legal clarity and regulatory certainty.
Mauritius can be the lead jurisdiction in providing that guidance.
One approach to curtail this issue, which currently seems to be the most widely adopted approach in the market, is that the website for the exchange is accessible globally, but certain jurisdictions and categories of customer are 'switched off' pursuant to the digital asset marketplace, terms and conditions and its client onboarding procedures.
Under the terms and conditions of the exchange, customers from certain prescribed jurisdictions are expressly prohibited from using the services of the business. Customers are required to submit detailed 'know your customer' KYC information to the marketplace and, based on a review of that information, the marketplace can verify that the customer is not from a restricted jurisdiction.
As discussed above in this document focuses on centralised digital asset marketplaces suitable only for institutional investors. For completeness, and to highlight that innovation in the space is accelerating at such a pace that there will be a host of other considerations for decentralised digital asset marketplaces. For example, where the listing of a token is purely based on user voting, certain tokens which may be characterised as 'securities' (or other regulated products) could be listed and traded on the decentralised platform which may then trigger licensing and authorisation issues for the marketplace. In addition, there will be regulatory developments in the future which result in a listed non-security token becoming a security, there will be further considerations as to how these tokens should be dealt with.
Individuals not otherwise prohibited from accessing the platform services (e.g., because the individual is subject to sanctions).
The same 'switching off' approach could be taken with respect to specific digital assets. For example, a digital asset which is not classified as a 'security' in Switzerland but would be classified as a 'security' in Mauritius could be made available for trading for Swiss persons but 'switched off' for Mauritius citizens. This approach would reduce the risk of the marketplace facilitating trading of 'securities' without a license in a particular jurisdiction but, as a commercial matter, may result in limiting the range of digital assets that are available to trade in some jurisdictions.
This approach allows the flexibility to 'switch off' an entire jurisdiction, where this is required by applicable laws and regulations, and to fine tune the exchange's offering in other jurisdictions by only 'switching off' the ability trade specific tokens.
Marketing of services should follow applicable laws and regulations of the target jurisdiction (e.g., marketing activities should not be conducted in 'switched off' jurisdictions). Where marketing is conducted through a website, measures should as those discussed below should be adopted. In conjunction with these 'switching off' safeguards, it also would be prudent for these platforms to limit active/concerted marketing campaigns to permitted jurisdictions (i.e., jurisdictions which have not been 'switched off') and in which there are not a significant number of tokens on the exchange which are 'switched off'.
In addition, the digital asset marketplace also may need to implement further measures including, but not limited to, the following:
Include a generic catch-all clause in the terms and conditions of the marketplace stating that services will not be provided to persons where the use of such services would be contrary to applicable laws and regulations notify customers about tokens which are 'switched off' in the relevant jurisdictions.
Implement systems and controls so that such persons cannot trade the 'switched off' digital assets, including geo-blocking and IP address checks; and avoid inadvertently triggering any marketing restrictions, the website and marketing materials of the exchange should list the jurisdictions which are not 'switched off' (i.e. are 'switched on'). The 'switching off' approach for jurisdictions such as Mauritius is only a partial solution, given the pervasive use of Virtual Private Networks (VPN's) in the industry. The above outlined approach therefore needs to be coupled with necessary sanctions screening using a reliable provider for sanctioned persons and entities. For completeness, another approach is to only permit the trading of tokens in certain jurisdictions as prescribed by the digital asset marketplace and block all other jurisdictions (i.e. the 'switching on' approach). Customers will therefore be unable to access the platforms website or trade tokens in jurisdictions which have not been 'switched on'. The advantage of the 'switching on' approach is that operational risk of providing services in a jurisdiction where such services are prohibited should be lower. This also provides a more comprehensive mechanism for dealing with legal and regulatory risk.

From an efficiency standpoint, it also narrows the jurisdictions that need to be monitored on ongoing basis. Irrespective of whether a 'switching on' or 'switching off' approach is adopted, the key will for these platforms will be to carry on thorough jurisdictional analysis and have effective customer screening and robust controls.
One further consideration is that these businesses should have appropriate procedures in place to react to abrupt changes to regulations or regulatory expectations in another jurisdiction. For example, if a regulatory change in a certain jurisdiction results in the trading of digital assets becoming unlawful or a certain token is recharacterised as a security, exchanges will need to immediately 'switch off' the relevant jurisdiction or the trading of the relevant token. To address this, digital asset marketplaces should consider implementing the following best practices:
Monitor regulatory developments in jurisdictions where the platforms tokens are traded and on an ongoing basis. If there is a potentially adverse change, the platform should assess whether these merits 'switching off' the jurisdiction as a whole or certain tokens from being traded in the jurisdiction. Where there is some ambiguity, the digital asset marketplace may wish to obtain an updated legal opinion from the issuer or from the businesses own legal counsel as well as the regulator to confirm the legal and regulatory status of the relevant tokens.
Require issuers to disclose to the marketplace, among other things, (i) any material issues with the status or condition of the project, financial condition, management team of the issuer; and (ii) any other material changes to information submitted in the original listing application by the issuer, pursuant to the continuing obligations requirements under the listing rules.
Prohibit users in affected jurisdictions from 'buying' the relevant tokens but (subject to the bullet point below) permitting them to sell such tokens; and
The regulator should maintain discussions with the digital asset marketplace business to resolve how the affected token holders can exit their positions (e.g., whether it is permissible for the token holders to make a final trade within a prescribed timeframe). Otherwise, such token holders may have to hold on to tokens which they cannot dispose of, which may therefore be valueless. In any event, this risk should be clearly identified to platforms users.
These issues, in respect to customer and investor protection are only the beginning. As technology advances, innovative products and services offered by digital asset marketplaces will only increase. The challenge for regulation is to minimise the risk whilst not stifling innovation.

3.Methodology of guidance notes for licencing requirements for custody of client funds on Digital asset marketplace

A digital asset marketplace licensee must also h

Other custody issues and recommendations:

A digital asset marketplace licensee must also hold a custody licence as issued FSC guidance 2019.
As mentioned earlier, a digital asset exchange can function as a broker, custodian and trading venue at the same time. The term 'custody' is used here generally (i.e., holding assets on behalf of the end user/client).
To date, digital asset custody models have primarily been based around co-mingled omnibus-like accounts, where similar users' assets are pooled in one account. The identification and ring-fencing of users' digital assets is arguably far preferable, to ensure that the assets will not form part of the estate available to the liquidator in the event of the insolvency of the custodian. It also helps assure users of the protection of their assets despite the custodian's liabilities incurred through operational losses, particularly where regulatory capital requirements do not apply. Segregated accounts do come with their challenges and costs, however. Set out below is an overview of some of the key advantages and challenges of omnibus accounts versus segregated user accounts:

Omnibus accounts		Segregated user accounts	
Advantages	Challenges	Advantages	Challenges
Operationally straightforward, reducing operational risk	Insolvency risk for users - not recorded on chain as the owner	Relies on strong record-keeping mechanics at the exchange level	Higher operational risk
Cost effective for the exchange and therefore also for the user	Becomes a centralized 'honey pot' that may attract internal or external theft and cybersecurity attacks	Cybersecurity attacks and theft in relation to other accounts should not taint the user	Higher costs, slower settlement

		account, unless directly hit	
Can facilitate fast settlement - user generally does not need to wait for assets to be shifted from cold storage (i.e., usually not affected by % of assets stored in hot vs. cold wallets)	Relies on strong record-keeping mechanics at the exchange level		Unless users' interest recorded on chain (or via trust arrangements - see below), arguably offers no higher protection than omnibus accounts

Set out below are important factors to consider:

Third parties – The use of reputable professional third parties to act as independent custody service providers should be considered. However, we recognise that there remains a paucity of such providers at this stage with the right track record and expertise.

User options – A combination of models, with variable pricing, should be considered where feasible, to enable users to choose the level of protection they wish for their assets.

Disclosure – Adequate risk disclosure is essential. At minimum, users should be advised prominently about the way in which assets are held on the exchange, and whether moving assets to their own personal digital wallets is a safer option.

Own assets – Extreme care is required in relation to proprietary digital assets. These should be segregated altogether and not commingled with user assets.

Trust arrangements – Trust arrangements can strengthen custody models from a user standpoint in markets that recognise trust structures. That is, a declaration of trust over assets in an omnibus account and/in segregated user accounts can help ensure that in an insolvency event, the assets are appropriately treated as those to which users (and not other creditors) are beneficially entitled. However, licensing requirements should be carefully considered, and the arrangements must be documented properly.

General principles for custody: Safety of digital assets temporarily held on exchanges are matters of priority for the industry, given the large number and scale of exchange hacks. The list below represents only some of the digital asset custody best practices and recommendations. It should not be construed to be an exhaustive list of all required controls and appropriate safeguard measures.

Digital asset marketplaces should screen all employees appropriately and always ensure adequate training and supervision. An appropriate internal function should be assigned to the safekeeping of assets, such as a security officer.

Digital asset marketplaces should establish and maintain internal procedures that ensure the maintenance of appropriate standards of recording and management with respect to user digital assets and fiat currencies.

Digital asset marketplaces that store, hold, or maintain custody or control of digital assets and fiat currencies on behalf of a person must hold that same type and amount of digital assets and fiat currencies owed to the person.

Digital asset marketplaces should not create a right of lien, offset or encumbrance or any other right with respect to user digital assets or fiat currencies, excluding (i) custodian fees and (ii) transaction fees.

Customer terms and conditions should not only cover the products and services available, but also make clear the respective rights, obligations, responsibilities and risk allocation of the parties, plus appropriate dispute resolution mechanisms. Procedures should also be clear on the digital asset marketplaces, with frequently asked questions posted and updated from time to time.

Digital asset marketplaces should have a clear fee structure that is readily accessible to customers. Where fees involve calculations, illustrative examples should be considered.

Digital asset marketplaces should keep the following books and records for at least 7 years from the date of creation, or such longer period as is required by applicable law:

Similar principles could be applied to custody services providers.

Amount, date, time, payment instructions and fees for each digital assets and fiat currencies transaction non-completed, outstanding, or inactive digital assets and fiat transactions. Bank statements and bank reconciliation records Any statements or valuations sent or provided to customers. Records of all customer complaints and investigations

When applicable, a digital asset marketplace should conduct reconciliations between its internal accounts and those of any third party by whom custody assets are held.

Real-time controls should be implemented for matching and reconciliation to confirm the validity of all digital asset transactions executed using private keys which belong to the exchange.
Cold storage refers to digital assets kept offline as opposed to hot wallets which are being used to cope with withdrawal request. Exchanges should develop a custody plan in line with liquidity management principles, e.g. assess technical options for cold storage custody services to enhance the security of assets left on the exchange. Amounts kept in hot wallet should be kept to a minimum (ideally more than 97% of customer assets should be stored offline). Customers should be educated and encouraged to utilize cold storage wallet custody solutions. In addition to liquidity management principles, limits and triggers on the percentage of assets held in hot storage should be set, with monitoring measures put in place to ensure limits are adhered to, whilst the exchange is liquid and operating effectively.
For both cold storage and hot wallet, measures shall be put in place by digital asset marketplaces to safeguard customer and proprietary assets from fraud, negligence and mishandling:
-Digital asset marketplaces should use hardware security modules ('HSM') which are physical computing devices that safeguard and manage cryptographic keys and provide secure execution of critical code. HSMs come with a certain level of regulatory assurance, such as the Federal Information Processing Standard certification and Common Criteria (an international standard).
-Digital asset marketplaces should use a multi-signature storage vault set up (ideally requiring at least three keys out of five or more to initiate a transaction).
- Security protocols surrounding management of private keys for both hot and cold storage should be audited.
-Digital asset marketplaces should proactively communicate their strategy for newly created digital assets in case of hard fork or airdrop.
-For each account, digital asset marketplaces should provide periodic personalised reports detailing the holdings both in digital assets and fiat currencies.
-Digital asset marketplaces should publish on their website risk assessment indicators outlining the level of risk of the digital asset to (potential) users.
-Digital asset marketplaces should monitor customer accounts to check for any inactive/ dormant accounts and set out the procedure by which those accounts may be closed, and claims may be made for relevant assets.
-Customers should have a clear understanding as to how they can have access to and withdraw their digital assets, particularly in times of stress.
-Digital asset marketplaces should implement a business continuity and recovery plan with clear policies and procedures in the case of a catastrophic event. Relevant information should be made available to users of the market.

*****Digital Asset Market Place-FSC guidelines May 2021 *****

Digital Asset Act 2021 Serbia

PROVIDED BY ADC FORUM TO SENATE SELECT COMMITTEE ON AUSTRALIA AS A TECHNOLOGY AND FINANCIAL CENTRE

The Serbian Parliament enacted the new Digital Assets Act ("DAA"), which will come into force on 29 June 2021. The main points of the new framework are outlined below, and the topic is discussed in more detail in our latest blog article here:

- The DAA regulates all digital assets regardless of the technology on which those digital assets are based.
- The DAA recognises two types of digital assets: virtual currencies and digital tokens.
- The DAA recognises the concept of digital assets mining, but this area is excluded from the scope of the DAA.
- The government authority with competence over virtual currencies is the National Bank of Serbia ("NBS"), while the authority with competence over digital tokens is the Serbian Securities Commission ("SEC").
- Digital assets can be issued with or without a "white paper".
- Secondary and OTC trading are allowed with or without an intermediary, and the use of smart contracts is explicitly allowed for secondary trading.
- Digital assets services providers must be incorporated in Serbia and hold the appropriate NBS/SEC licences.
- A pledge may be established over digital assets, but it must be registered with a service provider specifically licensed to operate a digital asset pledge register.
- Parties may enter into a fiduciary agreement for securing receivables or for other purposes.
- Fines and criminal liability: the maximum penalty for a breach of the DAA is RSD 5,000,000 (approx. EUR 43,000) or up to 10 % of annual turnover for the preceding financial year, whichever is higher. Individuals engaged in insider dealing or market manipulation may also be criminally liable (with a prison term of five to eight years and a fine).

https://www.sec.gov.rs/index.php/sr/вести/актуелности/685-закон-о-дигиталној-имовини