DeFi: Prohibition or Regulation?

A Strategic Opportunity for Gibraltar

Targ Patience, Founder & CEO

idclear

info@idclear.com

www.idclear.com

+35022502015

First Floor, Heritage House, 235 Main Street, Gibraltar, GX11 1AA

Originally published in June 2021 through Dolya Consulting

Executive Summary

Gibraltar, having been the first jurisdiction in the world to implement an effective DLT regulatory framework, benefits from a thriving DLT and blockchain industry and strong international reputation. DeFi, a more recent development in the space, threatens to disrupt global financial systems and markets. By replacing centralised infrastructures with autonomous algorithms, it delivers unprecedented operational and cost efficiencies and eliminates many engrained barriers to entry for financial inclusion. Whilst this may offer a lifeline to the world's 1.7 billion adults without access to banking or financial services, anonymity and freedom of participation also provide potential opportunities to fraudsters, terrorists, and criminals. Having grown to over $81bn in value, the DeFi market has attracted attention and concern from authorities, who have proposed various regulatory developments that may threaten its very existence.

The European Commission published its draft Markets in Cryptoassets Regulation (MiCAR) in September 2020, as part of its Digital Finance Strategy, seeking to provide opportunities and growth, financial stability, and legal certainty. Most activities captured under MiCAR require prior regulatory authorisation and incorporation as a legal entity. This presents a significant problem to DeFi as, definitively, all activities are decentralised, largely supported by unincorporated communities of developers. Meanwhile, the Financial Action Task Force (FATF) has drafted guidance that could bring DeFi project developers within the scope of international anti-money laundering regulations. These proposed changes, requiring incorporation, registration, or authorisation of DeFi developers, seek to establish accountability. This is, ostensibly, so that regulators can protect the public from risks of loss, fraud, theft, or deception, and prevent financial systems from being used to facilitate other financial crimes. The regulatory approaches adopted, however, attempt to force DeFi into traditional structures of oversight and control that are wholly inappropriate.

This document proposes that DeFi can be more constructively and effectively regulated, based on established regulatory precedents. These include the Gibraltar DLT Framework, OECD regulatory principles for innovation, certain controls introduced for automated algorithmic trading under MiFID II, and aspects of the FATF Recommendations. It is proposed that, through innovations in DLT market infrastructure and regulation, Gibraltar can pioneer a framework that provides regulatory certainty for developers, and a viable opportunity to recognise compliant DeFi solutions without stifling innovation. This introduces the concept of authorised and regulated entities who evaluate, test, document and approve DeFi applications ('DeFi Evaluators'), and those who would implement and conduct relevant regulatory processes on behalf of DeFi ecosystems as third parties ('AML Infrastructures'). This is a unique and timely opportunity, through which Gibraltar could realise significant economic, social, and strategic benefits, whilst providing instrumental support to the ongoing innovation and mass adoption of global, compliant Decentralised Finance.

Contents

Introduction

This document has been drafted to present and discuss concepts for a regulatory approach that may be of material strategic and economic benefit to Gibraltar and its stakeholders; namely a viable pathway to compliance for Decentralised Finance (DeFi) protocols and applications, in the context of ongoing international regulatory developments, through innovations in Distributed Ledger Technology (DLT) market infrastructure and associated regulation within the jurisdiction.

The following sections assess the emerging regulatory challenges to DeFi, examine their core underlying objectives, reflect on approaches to regulation and innovation, and explore certain relevant regulatory precedents, before finally introducing a number of proposed concepts as a solution to these complex collective challenges.

Certain sections provide introductory summaries and explanations of topics with which some readers will already be familiar. Please do not feel compelled to read anything other than that which interests or informs. The table of contents on the preceding page can be used to navigate to the various sections and topics addressed throughout.

Please note that nothing contained in this document is intended as, nor should be relied on or used as, legal advice.

Background

Decentralised Finance

DeFi refers to a type of financial infrastructure that does not rely on any centralised institution or authority, such as a bank or trading venue. Lending, borrowing, exchange and trading of assets are conducted on an automated, peer-to-peer basis using DLT, blockchain and 'smart contracts'. Smart contracts are computer programs or algorithms that operate on and interact with specific blockchain protocols, which automatically execute according to pre-determined rules when specific conditions are met. Smart contracts are encoded on the blockchain so that anybody with the relevant knowledge and capabilities can directly review their code and conditions. Decentralised Applications (DApps) are websites or applications that, unlike smart contracts, do not exist directly on the blockchain, but are required to interact with it; essentially, a DApp allows users to communicate with smart contracts, which in turn interact with the blockchain. Decentralised Exchanges (DEXs) are a category of DApp that facilitate trades and transactions in a decentralised and non-custodial manner, with participants' assets held in personal blockchain wallets.

Defining the term DeFi, and by extension DApps, remains the source of some controversy, however, occasionally falling prey to cyclical semantic, philosophical, and technical debates[1]. For the avoidance of doubt, therefore, DeFi, as referenced throughout this document, is intended to mean any "*ecosystem comprised of applications built on distributed ledger* [technology (DLT)]*, for the facilitation of permissionless financial services*[2]", operating autonomously according to pre-defined rules, with no single person or authority capable of nor responsible for making changes or otherwise exerting control or governance over its functions.

Consequences of DeFi

DeFi has the potential to radically disrupt both the structure and nature of global financial systems and markets, eschewing the need for centralised legacy infrastructures. Many complex operational processes, traditionally undertaken by a multitude of inefficient and costly intermediary institutions, can instead be performed by autonomous algorithms, running on distributed networks of internet-connected devices. Transactions executed according to pre-determined rules, confirmed using cryptographic consensus, and immutably recorded on blockchains generate far lower costs, with greater efficiency and transparency. Even more significant, however, is the potential to eliminate many entrenched barriers to entry to the financial system, based on wealth, status, and geography.

'Financial inclusion', recognised as key to reducing poverty and boosting prosperity, simply means that "*individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance –*

[1] https://101blockchains.com/cedefi-vs-defi/
[2] https://philippsandner.medium.com/decentralized-finance-defi-what-do-you-need-to-know-9cd5e8c2a48

delivered in a responsible and sustainable way"[3]. Globally, an estimated 1.7 billion adults do not have access to a bank account or financial services, yet 25% of these – roughly 425 million people – do have mobile phones and internet access[4]. Unlike traditional financial systems, ostensibly anyone with an internet connection and the relevant understanding can access DeFi, with personal custody and control of cryptoassets, and equitable access to low-cost transfers, lending, borrowing, trading, and even insurance[5]. Accenture estimated in 2015 that "*including unbanked adults into the formal financial system … could generate an additional $110 billion*" in annual revenues for banks [6] – revealing both the vast scale of financial exclusion, and the insidious cost of entry to our celebrated 'formal financial system' for the worlds poorest and most vulnerable people.

Use of DeFi expanded rapidly during 2020 and early 2021, as interest in DLT-based alternatives to traditional financial institutions and markets grew in availability, popularity, and value. According to a recent industry report[7], the entire DeFi ecosystem held over $81bn in value at the end of May 2021, demonstrating almost 30,000% growth since early 2019. Concurrently, attention from regulatory authorities has intensified, with growing concerns that, through DeFi, anonymous parties can construct and utilise remote systems to transmit substantial monetary value, without any of the financial crime controls, legal accountability and investor protections present in traditional financial systems and markets. Removal of any centralised authorities and barriers to entry is a double-edged sword, of course. This creates new, exploitable opportunities for fraudsters to swindle and steal, and for terrorists and other nefarious groups to fund illicit activities without detection or identification, all at the risk of detriment to wider society.

In predictable response to such concerns, a number of international regulatory developments have been proposed, the effects of which would either impose on DeFi and DApps many of the obligations and controls that apply to traditional financial institutions, or otherwise constructively proscribe them altogether.

DLT in Gibraltar

Gibraltar was highly responsive to the emerging DLT industry and markets[8], having been the first jurisdiction in the world to implement an effective regulatory framework, which has since proven to be of material benefit to its economy and international significance. The Gibraltar Financial Services (Distributed Ledger Technology Providers) Regulations 2017[9] entered into force on 1st January 2018, based on nine core principles. Since coming into effect, the regulations require any firm carrying out by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belonging to others, to be authorised and licensed by the Gibraltar Financial Services Commission (GFSC), and subject to equivalent levels of oversight

[3] https://www.worldbank.org/en/topic/financialinclusion
[4] https://globalfindex.worldbank.org/
[5] https://medium.com/@blockchain_simplified/decentralized-insurance-an-emerging-sector-in-defi-79bd84502cab
[6] https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_22/Accenture-billion-reasons-bank-inclusively.pdf
[7] https://dappradar.com/blog/dapp-industry-overview-may-2021
[8] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/gibraltar
[9] https://www.gibraltarlaws.gov.gi/legislations/financial-services-distributed-ledger-technology-providers-regulations-2017-4218

and enforcement as other regulated financial institutions. Though the original regulations have since been repealed by the Financial Services Act 2019[10], and replaced by the Financial Services (Distributed Ledger Technology Providers) Regulations 2020[11], the nine principles remain unchanged.

The nine principles are, broadly speaking, aligned to those at the core of European financial and capital markets legislation – such as the revised Markets in Financial Instruments Directive (MiFID II)[12] – and are substantiated by detailed regulatory guidance issued by the GFSC[13], which is periodically updated, clarified, and refined. This highly principles-based approach has allowed the framework to evolve alongside DLT, its application and markets, whilst remaining aligned to the core regulatory and legislative intentions.

In the near future, a tenth principle relating to market integrity will be introduced[14], which will further substantiate and differentiate from the second principle[15] – that a DLT Provider must pay due regard to the interests and needs of each and all its customers – under which market integrity is currently considered. Efforts are also underway, however, to consider further development and expansion of the Gibraltar regulatory framework to better align with the maturity of the DLT industry and ongoing international regulatory developments. The Gibraltar Association for New Technologies (GANT)[16], the industry association that represents finance, blockchain and DLT in the jurisdiction, intends to work closely with both policymakers and the private sector to support and inform this process.

[10] https://www.gibraltarlaws.gov.gi/legislations/financial-services-act-2019-4690
[11] https://www.gibraltarlaws.gov.gi/legislations/financial-services-distributed-ledger-technology-providers-regulations-2020-4774
[12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN
[13] https://www.fsc.gi/downloads?section=19&type=0
[14] https://www.gibraltar.gov.gi/press-releases/working-group-convenes-to-deliver-10th-principle-of-gibraltars-dlt-regulatory-framework-442021-6591
[15] For reference, all nine DLT Principles are summarised under '**Error! Reference source not found.**', later in this document.
[16] http://www.gibnew.tech/

Emerging Regulatory Challenges

Markets in Crypto-Assets Regulation

On 24th September 2020, The European Commission published its draft Markets in Crypto Assets Regulation (MiCAR)[17] and supplementary Pilot Regime for DLT-based financial market infrastructures[18], which both form part of Europe's wider Digital Finance Strategy[19]. This strategy aims to establish a liberal, sustainable crypto-asset ecosystem, in order to enhance Europe's competitiveness and innovation in the evolving financial industry, while continuing to mitigate any potential risks related to investor protection and financial crime. The intended outcome will be to provide more opportunities and growth while ensuring financial stability and legal certainty.

It is expected that the new European framework will enter into force by 2024 at the latest. As with other European financial regulations, there will be clear 'passporting' and 'third country' provisions, which introduce controls in respect of access by firms to EU-based customers and markets. Third country provisions will require EU recognition that the regulatory frameworks and enforcement of any third country are 'equivalent' to those in Europe.

MiCAR is intended to ultimately replace existing, fragmented national frameworks that regulate crypto-assets within the EU, and has a broad scope that covers any digital representation of value or rights which may be shared or stored electronically, using DLT or similar[20]. Crypto-assets that are already within the scope of existing financial services legislation, such as financial instruments, will not be additionally captured[21]. In seeking to address the multitude of different crypto-asset types that have emerged, MiCAR defines and regulates three specific categories:

1. **Asset-referenced tokens**: those that purport to maintain a stable value by referring to the value of several fiat currencies, one or several commodities, one or several crypto-assets, or a combination of such assets[22];
2. **E-money tokens**: those of which the main purpose is to be used as a means of exchange and that purport to maintain a stable value by referring to the value of a fiat currency that is legal tender[23]; and
3. **Utility tokens**: those that are intended to provide digital access to a good or service, available on DLT, and are only accepted by the issuer of the token[24].

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0594
[19] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684
[20] Article 3, Definitions, 1.(2)
[21] Article 2, Scope, 2.
[22] Article 3, Definitions, 1.(3)
[23] Article 3, Definitions, 1.(3)
[24] Article 3, Definitions, 1.(5)

MiCAR will apply to any issuers of crypto-assets who offer these to third parties, and also to Crypto-Asset Service Providers (CASPs), being any person whose occupation or business is the provision of one or more of the following services to third parties on a professional basis[25]:

1. the custody and administration of crypto-assets on behalf of third parties;
2. the operation of a trading platform for crypto-assets;
3. the exchange of crypto-assets for fiat currency that is legal tender;
4. the exchange of crypto-assets for other crypto-assets;
5. the execution of orders for crypto-assets on behalf of third parties;
6. placing of crypto-assets;
7. the reception and transmission of orders for crypto-assets on behalf of third parties; and/or
8. providing advice on crypto-assets.

Legal Personality

Most of the activities captured under MiCAR require prior authorisation from a competent authority[26] of an EU Member State; there are very limited exceptions, and may only be granted to legal persons (i.e., legal entities):

1. **Asset-referenced token issuers:** Only legal entities that are established in the EU may be granted authorisation to offer asset-referenced tokens to the public and to seek their admission to trading on a trading platform[27].
2. **E-money token issuers:** Only authorised credit institutions or 'electronic money institutions' (licensed under the E-Money Directive, 2009/110/EC) – either of which must be a legal entity – may offer e-money tokens to the public in the EU[28].
3. **'Other' token issuers:** Only legal entities are permitted to issue utility tokens (or any other tokens that are neither asset-referenced nor e-money tokens)[29].
4. **CASPs:** Only legal persons that have a registered office in a Member State of the EU may be granted authorisation as crypto-asset service providers[30].

These requirements have been identified as presenting insurmountable challenges to DeFi projects – where issuance, or the performance of certain defined services of CASPs, is decentralised – as these are often supported by an unincorporated community of developers, without an identifiable 'issuer' or 'operator'. These issues were alluded to in a September, 2020 initial response to MiCAR by the International Association of Trusted Blockchain Applications[31] (INATBA), an industry body that was itself initiated by the European Commission:

> *"Certain analyses suggest that, under the proposed regulation, novel and early-stage developing markets such as Decentralised Finance (DeFi) would likely no longer be accessible to Europe and her citizens."*

[25] Article 3, Definitions, 1.(8) and (9)
[26] https://www.esma.europa.eu/rules-databases-library/eu-acts-and-national-competent-authorities
[27] Title III, Chapter 1, Article 15.1. and 15.2.
[28] Title IV, Chapter 1, Article 43.1.
[29] Title II, Article 4.1.(a).
[30] Title V, Chapter 1, Article 53.1.
[31] https://inatba.org/

In March 2021, INATBA reiterated and expanded upon these concerns in a comprehensive report entitled 'Blockchain Ecosystem's Response to MiCA Regulation Proposal'[32], which had been informed by a survey and series of stakeholder engagement sessions. The report notes a clear incompatibility of DeFi protocols and DApps with the centralised placing of liability; and whilst respondents broadly agreed that the DeFi market requires regulatory intervention, they believe that regulating developers would both disincentivise and slow innovation. The report specifically notes that DeFi often implements decentralised decision-making processes and automated operational mechanisms, making it difficult to determine who is in control and who might bear the liability for operations of a DeFi CASP.

The underlying problem with such a regulatory approach to DeFi is stated rather succinctly in the report, as follows:

> *"The regulatory difficulties associated with DeFi originate in the fact that regulatory measures typically presuppose a point of reference upon which an obligation is imposed or a right grounded. This is sensible because it dramatically increases enforceability and legitimacy – if it is impossible to specify who is the subject of a right or obligation, as is true for decentralised networks, it is also impossible to justify and enforce it."*

Grandfathering

Certain existing decentralised crypto-assets, other than asset-referenced and e-money tokens, may benefit from a grandfathering clause provided in Article 123 of the draft regulation, under which obligations on issuers outlined in Articles 4 to 14 of MiCAR will not apply to crypto-assets issued before it enters into force. Any future decentralised crypto-assets, however, would be unable to comply with MiCAR as drafted, meaning that CASPs would almost certainly be prohibited from admitting them to trading or allowing them to be transacted.

Financial Action Task Force

Formed at the Paris G-7 summit in 1989, the Financial Action Task Force (FATF)[33] has been part of an ongoing effort to strengthen anti-money laundering and anti-terrorist financing practices around the world. It is an inter-governmental body that sets international standards which aim to ensure that financial systems and the broader global economy are protected from threats related to money laundering, organised crime, corruption, terrorism, and the proliferation of weapons of mass destruction (collectively abbreviated as 'AML/CFT' or 'AML/CFTP'). These standards include prescriptive preventative measures that must be adopted, such as the performance of risk-based due diligence, monitoring of transactions, and the reporting of suspicious activities to legal authorities.

More than 200 countries and jurisdictions are committed to implementing the FATF's 40 Recommendations into local law; this includes Gibraltar, whose AML/CFTP framework includes

[32] https://inatba.org/wp-content/uploads/2021/03/2021-02-Blockchain-Ecosystems-Response-to-MiCA-Regulation-Proposal-Final.pdf
[33] https://www.fatf-gafi.org/about/

the Proceeds of Crime Act 2015[34], the Terrorism Act 2018[35], the Sanctions Act 2019[36], the European Freezing Orders and Confiscation Orders (Amendment etc) (EU Exit) Regulations 2020[37], and the European Investigation Order (Amendment etc) (EU Exit) Regulations 2020[38]; these are further substantiated by detailed guidance from the various competent authorities; the GFSC, Office of Fair Trading (OFT) and the Gibraltar Gaming Commissioner. Any countries or jurisdictions that fail to legally implement and adequately enforce the FATF Recommendations are listed as 'Non-Cooperative Countries or Territories' (NCCTs) on what is commonly referred to as the 'FATF Blacklist', with damaging economic consequences arising from barriers to international banking, trade and foreign investment.

FATF & Crypto-Assets

The relevance of FATF Standards to crypto-assets, and more recently DeFi, has evolved gradually over several years. An initial report[39] outlining the potential AML/CFTP risks of 'virtual currencies' was published by FATF in June 2014, which established a conceptual framework of key definitions intended as a basis for further policy development. This was followed in June 2015 by the first FATF guidance[40] on a risk-based approach for 'virtual currency payment products and services (VCPPS)', which focused specifically on points of intersection between 'virtual currencies' and the regulated financial system, and in particular 'convertible virtual currency exchangers'. In July 2018, a FATF report[41] was presented to the G20 Finance Ministers and Central Bank Governors' meeting in Buenos Aires, at which attendees "*recognised the real and growing money laundering and terrorist financing risks from crypto-assets and the urgency of action to address these risks*"[42].

The report outlined FATF's work on 'virtual currencies/crypto assets', their views on the associated risks, and the evolution and revision of global standards and guidance. Then, in October 2018, the FATF updated its Standards[43] to clarify their application to 'virtual assets and virtual asset service providers' and added these as new definitions to the FATF Glossary. This was followed in June 2019 by updated guidance[44] for a risk-based approach to 'virtual assets and Virtual Asset Service Providers (VASPs)', which addressed how virtual assets activities, VASPs and other entities (including banks and broker-dealers) fall within the scope of the virtual asset Recommendations, and how countries and competent authorities should apply the Recommendations in the context of virtual assets or VASPs.

[34] https://www.gibraltarlaws.gov.gi/legislations/proceeds-of-crime-act-2015-2348
[35] https://www.gibraltarlaws.gov.gi/legislations/terrorism-act-2018-4516
[36] https://www.gibraltarlaws.gov.gi/legislations/sanctions-act-2019-4573
[37] https://www.gibraltarlaws.gov.gi/uploads/legislations/european-union/2020=524.pdf#viewer.action=download
[38] https://www.gibraltarlaws.gov.gi/uploads/legislations/european-union/2020=529.pdf#viewer.action=download
[39] https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
[40] https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
[41] http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf
[42] http://www.fatf-gafi.org/publications/fatfgeneral/documents/g20-fm-cbg-july-2018.html
[43] http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html
[44] http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

The FATF definitions are:

1. **Virtual asset:** a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
2. **Virtual Asset Service Provider (VASP):** any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
   i. exchange between virtual assets and fiat currencies;
   ii. exchange between one or more forms of virtual assets;
   iii. transfer of virtual assets;
   iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
   v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

It is noted that FATF's VASP definition is narrower in scope than CASPs defined under MiCAR, with the latter intended to capture a broader range of entities. Recital 8 of MiCAR acknowledges an alignment of objectives, however, stating:

> *"Any definition of 'crypto-assets' should … correspond to the definition of 'virtual assets' set out in the recommendations of the Financial Action Task Force (FATF). For the same reason, any list of crypto-asset services should also encompass virtual asset services that are likely to raise money-laundering concerns and that are identified as such by the FATF."*

FATF Recommendations[45] 9 through 23 outline measures that must be employed by relevant businesses and individuals to prevent the use of the financial system for purposes related to money laundering and the financing of terrorism and proliferation, with additional measures for specific customers and activities. With respect to 'new technologies', Recommendation 15 states:

> *"… countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."*

Licensing & Registration

Further details are provided in an 'Interpretive Note to Recommendation 15 on New Technologies', within the published FATF Recommendations. This requires that VASPs – whether legal or natural persons – be licensed or registered. This may be in the jurisdiction in

[45] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

which the VASP is 'created', or in which their 'place of business' is located, and they may be required to additionally register or become licensed in any jurisdictions where they offer products and/or services to customers or conduct operations. Such measures are, in principle, intended to prevent criminals or their associates from owning, controlling, or managing a VASP.

Once licensed or registered, VASPs must be subject to adequate regulation and risk-based supervision or monitoring by a recognised competent authority[46], to ensure compliance with all relevant AML/CFTP requirements. Any parties – including any directors and senior managers – found to be performing VASP activities without the requisite license or registration can be subject to legal action and sanctions in any relevant jurisdiction. Similar requirements have been in effect in Gibraltar since 2018 – as summarised in the earlier section '**Error! Reference source not found.**', any firm carrying out by way of business, in or from Gibraltar, 'the use of DLT for storing or transmitting value belonging to others' must be authorised and licensed by the Gibraltar Financial Services Commission (GFSC) and is subject to risk-based supervision and monitoring – albeit with a defined scope of activities that is not identical to that recently adopted by FATF.

FATF & DeFi

In July 2020, FATF published a 12-month review report[47] on the revised standards on virtual assets and VASPs, in which they committed to update their guidance for a risk-based approach. In that report, the "*use of decentralised exchanges and applications*" is listed as one of the "*main trends in the virtual asset ML/TF risk landscape since 2019*"[48], under "*tools and methods to increase the anonymity of transactions*" and alongside recognised high-risk mechanisms, such as tumblers, mixers, and anonymity-enhanced cryptocurrencies that prevent the meaningful application of AML/CFTP controls. For context, in FATF's September 2020 report, 'Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing'[49], the use of mixing or tumbling services[50] are variously listed as 'red flags' indicating potential money laundering or terrorist financing activities.

In March 2021, FATF published draft updated guidance for a risk-based approach to virtual assets and VASPS[51], open to public consultation until 20th April[52], in preparation for further amendments to be made at their June 2021 meeting. The amendments within this draft appear to provide a clearer indication of FATF's intended scope or direction of thinking concerning the VASP definition. There is a recognition in paragraphs 56 and 57, for instance, that decentralised or distributed applications (DApps) operate on peer-to-peer networks of

[46] A competent authority is any person or organisation that has the legally or invested authority, capacity, or power to perform a designated function, including financial supervisors established as independent non-governmental authorities with statutory powers.
[47] https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf
[48] 'Section 1: ML/TF Risks and the virtual asset market', paragraph 18.
[49] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf
[50] Tools or services specifically designed to obscure the source of a transaction and facilitate anonymity by linking all transactions in the same address and sending them together in a way that appears as if sent from a different address.
[51] http://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf
[52] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html

computers running a blockchain protocol, and that such DApps are not themselves VASPs, as the FATF Standards do not apply to underlying software or technology. It does also state, however, that DApps "*usually have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative "key" or collecting fees*", which presents a vulnerability.

This vulnerability was demonstrated in a spectacular fashion in April 2021, when crypto-assets valued at over $80m were stolen from DeFi lending protocol EasyFi using administrative keys stolen from a MetaMask[53] wallet after hackers compromised the project founder's personal computer[54].

The scope of individuals or entities who may be considered VASPs, as a consequence of any involvement in a DApp, appears broad indeed. Notwithstanding the noted potential complexities or impossibility of identifying such a party[55], the 'owner/operator' of a DApp is likely to be a VASP, "*even if other parties play a role in the service or portions of the process are automated*". This extends to any person conducting 'business development' for a DApp when they 'facilitate or engage' in exchanging or transferring virtual assets as a business on behalf of another natural or legal person. This is concluded with the following statement:

> *"The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place."*

Later, paragraph 79 provides further insight into the broad intended application of VASP status and responsibilities:

> *"Launching a service that will provide VASP services, for instance, does not relieve a provider of VASP obligations, even if those functions will proceed automatically in the future, especially but not exclusively if the provider will continue to collect fees or realize profits, regardless of whether the profits are direct gains or indirect. The use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibility for VASP obligations. For purposes of determining VASP status, launching a self-propelling infrastructure to offer VASP services is the same as offering them, and similarly commissioning others to build the elements of an infrastructure, is the same as building them."*

If this draft guidance is ultimately agreed upon and finalised without material change, its implications for the DeFi industry and community will be dramatic. It should be noted that many DeFi applications only function through the participation of users[56] – in the form of staking, lending, liquidity provision, 'yield farming'[57] or governance[58] – most of whom 'collect fees or

[53] MetaMask is a software cryptocurrency wallet that allows users to access their Ethereum wallet through a web browser extension: https://metamask.io/

[54] https://medium.com/easify-network/easyfi-security-incident-pre-post-mortem-33f2942016e9

[55] See the section **Error! Reference source not found.**, **Error! Reference source not found.**, earlier in this document.

[56] https://www.entrepreneur.com/article/366908

[57] Yield farming, also referred to as liquidity mining, is a way to generate returns on crypto-asset holdings based on a staking or lock-up mechanism in smart contract-based liquidity pools in return for a percentage of fees generated by the liquidity provided.

[58] https://medium.com/the-liquidapps-blog/introducing-dapp-network-governance-model-b90541ac7682

realise profits'. This would mean that both codebase developers[59] of such DeFi applications that perform defined 'VASP services', as well as certain participants of those applications, may be at risk of being considered a VASP, and thereby subject to all relevant compliance and registration or licensing obligations. Such parties would be obligated to perform adequate due diligence, risk assessments, transaction monitoring, and reporting of suspicious transactions to the appropriate authorities, as well as the exchange and management of personal data (see '**Error! Reference source not found.**', below). Designation as a VASP may also bring parties within the scope of peripheral or associated regulation in relevant jurisdictions, including certain prudential, investor protection and market integrity obligations[60].

The 'Travel Rule'

FATF's 2019 'Interpretive Note to Recommendation 15 on New Technologies' also affected an amendment to Recommendation 16 on Wire Transfers, commonly known as the 'Travel Rule' as it mirrors a rule of that name in the US Banking Secrecy Act[61]. The FATF Travel Rule requires VASPs to obtain and hold accurate information on the originator and beneficiary of virtual asset transfers; they must submit this information to the beneficiary VASP or financial institution 'immediately and securely' on any virtual asset transfers made, obtain, and hold this information on any transfers received, and all records must be made available to authorities on request. VASPs must also monitor the availability of information, and take freezing action prohibiting transactions with sanctioned persons and entities.

In practice, this means that VASPs will be required to obtain, exchange, record and process the following information – supported by a unique transaction reference that enables tracing of transactions – for any virtual asset transfers exceeding 1,000/EUR or 1,000/USD (or other currency equivalent) in value

i. the name of the originator (sender);
ii. the originator's account number used to process the transaction;
iii. the originator's address, national identity number, unique customer identification number, or date and place of birth; and
iv. the name of the beneficiary and the number of the account receiving the transaction.

According to FATF's July 2020 12-month review report[62] on the revised standards on virtual assets and VASPs, 32 jurisdictions surveyed at the time had imposed AML/CFTP regulations on the virtual asset sector, 18 of which had introduced registration and 14 had introduced licensing regimes. The report noted, however, that both jurisdictions and representatives from the VASP sector had raised a range of issues with the implementation of the revised Standards

[59] With only the *potential* (and improbable) exception of such developers who could in no way collect fees or realise profits, directly or indirectly, from the relevant DeFi application, and would at no point act as its participants.

[60] Paragraph 121 of the FATF draft updated guidance for a risk-based approach to virtual assets and VASPS.

[61] https://www.fdic.gov/regulations/safety/manual/section8-1.pdf

[62] https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

and Guidance, including the so-called 'sunrise issue' of unclear approaches to dealing with VASPs in jurisdictions without the Travel Rule. As a result, FATF committed to undertake a second 12-month review of compliance by June 2021. By this time, the report stated, jurisdictions will have had two years to transpose the revised FATF Standards on VASPs into law, and the VASP sector 'will have had time to implement global Travel Rule solutions'.

Gibraltar was one of the first jurisdictions in the world to enact the travel rule into law, with the Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021[63] commencing on 22nd March 2021. Several leading blockchain AML/CFTP analysis and solution providers[64] are in the process of developing viable solutions to satisfy the Travel Rule requirements internationally, whilst also ensuring compliance with potentially overlapping regulatory obligations[65]. Through active engagement with these parties, and local industry involvement in the deployment and testing of their solutions, Gibraltar is maintaining its position at the forefront of DLT industry developments and regulation.

As with other operational requirements applicable to VASPs, the Travel Rule would present another significant issue to DeFi ecosystems and DApps. Whilst the transmission, reception and record-keeping of such data could be automated to a significant degree, this would require the processing of large amounts of sensitive personal data, including that belonging to third parties, bringing with it additional obligations and risks concerning data protection and privacy. A 2019 study conducted by the European Parliament's Panel for the Future of Science and Technology, 'Blockchain and the General Data Protection Regulation[66]' explored many the complexities of managing personal data in a compliant manner using blockchain, noting that "*the very technical specificities and governance design of blockchain use cases can be hard to reconcile with the GDPR*[67]".

[63] https://www.gibraltarlaws.gov.gi/uploads/legislations/proceeds-of-crime/2021s194/2021s194.pdf#viewer.action=download

[64] Solutions are known to have been developed by Confirm, and through partnerships between Chainalysis and Notabene, and Elliptic and CoolBitX.

[65] Such as those relating to the processing and protection of personal data, e.g., the EU General Data Protection Regulation (GDPR) (Regulation (EU) 6016/679)

[66] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[67] The European 'General Data Protection Regulation' – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Isolating the Regulatory Objectives

Legal Personality

As outlined under '**Error! Reference source not found.**', '**Error! Reference source not found.**' earlier in this document, European regulators propose to mandate legal incorporation and regulatory authorisation and/or supervision for crypto-asset issuers and CASPs. Furthermore, as outlined under '**Error! Reference source not found.**', '**Error! Reference source not found.**', FATF already requires that VASPs – whether legal or natural persons – be licensed or registered and subject to various regulations and risk-based supervision or monitoring. Whilst the draft of MiCAR fails to mention or recognise DeFi or DApps directly, it constructively prohibits their existence. Conversely, recent draft FATF guidance contains explicit yet sometimes clouded descriptions, under which any contributors and participants of DeFi ecosystems or DApps may become subject to the same regulatory obligations and oversight as banks and other financial institutions.

Such consequences would be neither workable nor enforceable in practice; nor would they mitigate the potential risks presented by many affected DeFi ecosystems. Instead, the inexorable demand for DeFi protocols and DApps would force otherwise legitimate users to use illicit systems – the existence of which would be effectively impossible to prevent – in which anonymous or pseudonymous transactions may be undertaken in the absence of any risk control mechanisms. DeFi protocols and applications can be set up and operated between a globally distributed community of internet-connected personal computers, which can be easily anonymised using TOR and VPNs[68]. The only feasible method of enforcement would be via costly, complex, and largely fruitless investigations, resulting at best in occasional perfunctory prosecutions as an ineffectual deterrent. Providing a workable route to regulatory compliance, in a manner that effectively mitigates genuine risks, will far better achieve regulatory intentions, whilst also stimulating innovation, incentivising compliance, and enabling broader public participation in properly governed marketplaces.

The foundational principle motivating these demands for legal personality, registration, authorisation and/or supervision is simple and understandable: accountability. Where members of the public may be exposed to risks – of loss, fraud, theft, or deception, for example – legislators and regulators have a duty to implement controls, oversight, and mechanisms of accountability to protect the marketplace and its participants. Broadly, the purpose and intent of such regulatory controls and oversight are to:

- protect consumers and investors from being misled, exposed to undue risks, or defrauded;
- cultivate and protect fair and efficient market environments that incentivise innovation and drive growth;
- mitigate risks of market and system failures;

[68] The Onion Routing (TOR) project is free, open-source software that enables anonymous communication by directing internet traffic through thousands of worldwide volunteer relays, to conceal a user's location and usage from network surveillance or traffic analysis. Virtual Private Networks (VPNs) encapsulate and transmit data over another network, typically using tunnelling protocols and encryption techniques to increase privacy and security.

- generate confidence and trust in financial markets, products, and systems; and
- protect financial markets, products, and systems from being exploited by criminals and bad actors.

Statements made by S. Chaudary and D. Salvador-Adebayo in their paper, '*Why Regulate Financial Markets?*'[69], during the aftermath of the 2007-2008 financial crisis – itself the product of inadequate regulatory control over highly complex and innovative markets – seem pertinent to the challenge currently facing regulators:

> *"The complexity of the financial services business, the introduction of new products … the diverse needs of individuals which creates an opportunity to confuse and cheat customers, makes it a difficult task to prepare rules which would effectively outlaw the unacceptable behaviour. There are various reasons why the market needs to be regulated which could range from externalities[70], monopoly / oligopoly[71] / monopsony[72], principal-agent problems[73], and barriers to entry / exit, information failures, public good and market integrity which would comprehensively outlaw unethical behaviour."*

The extraordinary innovations witnessed in DLT and DeFi – in particular their many financial mechanisms and use cases – has taken place on a smaller economic scale, and in a more fragmented manner, than that which emerged from the world's financial markets during their riotous heyday of laissez-faire capitalism[74]. As adoption grows, however, DeFi is, in its own way, equally complex and nuanced, providing significant opportunities for risks and failures to materialise, as much from errors or incompetence as from unscrupulous or criminal activities. A viable and acceptable approach to regulating DeFi must, therefore, not only control for risks arising from misinformation, fraud, failures, and exploitation, but also provide an appropriate degree of personal accountability and liability for managing such risks.

Financial Crime Compliance

Addressing risks presented by financial crime has been a key priority for governments and regulatory authorities throughout recent decades. Financial crime impacts the world in many diverse ways, but it is widely recognised that the prevalence of economically motivated crime can substantially threaten the development and stability of societies and their economies. For all its diversity, financial crime falls within three fundamental types of conduct:

1. activities that dishonestly generate wealth for those engaged in the conduct in question. This includes the exploitation of inside information or the acquisition of property by deceit;
2. activities that protect a financial benefit that has already been obtained by illicit means, or to facilitate the realisation of such a benefit. This includes attempts to launder the financial proceeds of an offence; and

[69] Journal of European Studies, 2014: 'Why Regulate Financial Markets? The Underlying Rationale for Financial Regulation in the Wake of the Current Crisis'.
[70] https://link.springer.com/referenceworkentry/10.1057%2F978-1-349-95121-5_126-2
[71] https://link.springer.com/referenceworkentry/10.1007/978-1-349-58802-2_1216
[72] https://link.springer.com/referenceworkentry/10.1057/978-1-349-95121-5_2282-1
[73] https://link.springer.com/chapter/10.1007/978-3-642-14200-0_1
[74] https://www.thebalance.com/laissez-faire-definition-4159781

3. activities that protect or disguise the provision of financing or other support to those engaged in illicit activities, such as terrorism or the proliferation of illicit weapons of mass destruction.

Effective AML/CFTP controls within financial systems are critical tools in the fight against financial crime. As the complexity of those systems increases, however, so does the complexity of detecting and preventing money laundering and terrorist financing, with the risk of this becoming an insurmountable challenge.

Financial institutions implement and operate the majority of their financial crime controls internally, with staff or officers of the firm appointed and approved to perform certain regulated functions, for which they are personally accountable. In Gibraltar, this is outlined in the Regulated Individuals (RI) Regime[75], under which firms must nominate a Head of Compliance and a Money Laundering Reporting Officer (MLRO), each of whom must be approved by the GFSC. Although the GFSC may consider outsourcing of particular regulated functions on a case-by-case basis, overall responsibility for each function must still be assigned to an individual within the regulated firm, who must oversee the outsourced function and ensure compliance with all relevant requirements. In such circumstances, it is the individual who oversees the outsourced function from within the firm that is subject to approval and accountability.

Technologies available to firms and authorities to aid the detection and prevention of financial crime have also benefited from recent strides in technological advancement. Early solutions designed to meet the AML/CFTP needs of businesses were essentially unsophisticated search functions of external data libraries; however, with the advent of machine learning and artificial intelligence, the sophistication and reliability of many automated tools – and the nature of the checks they can perform – has developed significantly, with modern solutions providing for highly automated AML/CFTP processes, including aspects of 'Know Your Customer' (KYC), due diligence and transaction monitoring.

Such processes cannot be wholly automated, however, as any alerts and potential matches identified by automated systems still require human analysis, investigation, and response. Irrespective of the aspirations and predictions stated by enthusiasts and devotees, artificial intelligence capable of replicating or replacing such human intelligence and insight remains a remote prospect. Attempts to fully automate financial crime controls result in inconsistent and flawed outcomes, without any attributable accountability; thereby acting against the interests of both the financial systems themselves, and their legitimate participants. As noted by Anupam Mehrotra[76], Professor in Banking and Management at Amity University, Dubai:

> *"The results produced by AI systems should be accurate, precise and reliable. However, they may be doubtful or incorrect also, at times, depending on the quality of algorithm*

[75] As outlined in Part 8 of the Gibraltar Financial Services Act 2019: https://www.gibraltarlaws.gov.gi/uploads/legislations/financial-services/2019-26/2019-26(25-03-21).pdf

[76] 2019 International Conference on Automation, Computational and Technology Management (ICACTM) – conference paper 'Artificial Intelligence in Financial Services – Need to Blend Automation with Human Touch'.

they are using or based on. In an AI driven business model, devoid of human intervention, no one takes responsibility of the outcome of the decision-making process. No one is answerable for the incorrect outcome of an algorithm."

The need for human intervention and operational processes represents an existential threat to autonomous DeFi ecosystems and DApps, should FATF-aligned AML/CFTP requirements be applied to them. As previously stated, the growth of the DeFi market, and the ability of its participants to transact anonymously in the absence of any meaningful financial crime controls, is an increasing and understandable concern to regulatory and legal authorities. A viable and acceptable approach to regulating DeFi must, therefore, enable the application of FATF-compliant AML/CFTP controls – with some identifiable party being accountable and liable – whilst still allowing and incentivising the development of innovative DeFi solutions. It will be vital that developers have an accessible and viable route by which they may create and launch compliant DeFi solutions, whilst remaining securely outside of the regulatory perimeter themselves.

Relevant Regulatory Precedents

As outlined in the preceding sections of this document, regulatory approaches thus far seem, at best, intent on manipulating DeFi – however uncomfortably – into familiar structures of oversight and control. Yet, despite its novel appearance and revolutionary potential, the particular challenges and risks presented by DeFi can be more constructively and effectively addressed, based on certain clear precedents from established regulatory frameworks.

It is important to preface this section by stating, categorically, that it does not imply any intention or suggestion that cryptocurrency-based DeFi should become subject to onerous and prescriptive regulations, nor be treated as equivalent to traditional capital markets or regulated financial instruments. It is recognised that certain DeFi ecosystems – such as those facilitating markets in security tokens or financial derivatives – may provide products and services that fall within the regulatory perimeters of such markets. Such scenarios have not been directly addressed here, although the same general principles should also apply, notwithstanding any additional regulatory obligations.

The precedents described below are presented solely to draw out, in context, particular aspects as they apply and are relevant to DeFi. It is important that any regulation of DeFi, irrespective of its basis and precedents, be applied logically and proportionately, in a way that effectively mitigates real risks without carelessly suppressing its many benefits.

Regulatory Approach (OECD)

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental economic organisation with 38 member countries, founded in 1961 to stimulate economic progress and global trade, whose stated goal "*is to shape policies that foster prosperity, equality, opportunity and well-being for all*"[77]. The following text, drawn from the foreword and summary of their 1996 report, 'Regulatory Reform and Innovation'[78], is as pertinent to regulating today's cutting-edge market innovations as it was to those of 25 years ago:

> "*Government regulations can have both positive and negative effects on the innovation process. Among other goals, regulatory reform is intended to enhance the positive regulatory effects on innovation. Reforms should help ensure that regulations in all spheres of activity are fully responsive to changes in the economic, social and technical conditions surrounding them. The regulatory process must take into account the effects of regulation on innovation as well as the implications of technical change for the rationale and design of regulation. The regulation/innovation interface is mutual and dynamic; an understanding of this interface is crucial to regulatory reform efforts.*

[77] https://www.oecd.org/about/
[78] https://www.oecd.org/sti/inno/2102514.pdf

Review of the regulation/innovation interface leads to several general conclusions on how to improve the positive regulatory effects on innovation without jeopardising the original regulatory objectives:

1. ***Understand regulation/technology linkages.*** *The regulatory process – whether in the economic, social or administrative spheres – must be ever vigilant to the effects of technical change.*
2. ***Introduce competition.*** *In all economic sectors, a certain degree of competition among firms is essential to the innovative process.*
3. ***Streamline regulations.*** *In the interest of economic efficiency and innovation, regulatory reform should seek to remove duplicative, onerous and inefficient regulations, particularly to aid small and medium-sized enterprises.*
4. ***Use technology-driving approaches.*** *Maximum use should be made of regulatory approaches or alternatives which are technology-friendly, such as economic instruments, voluntary agreements and performance rather than design standards.*
5. ***Harmonize internationally.*** *Countries should pursue greater compatibility among their regulations to remove uncertainties, inefficiencies and market barriers which can slow innovation."*

Gibraltar DLT Framework

The Gibraltar Financial Services (Distributed Ledger Technology Providers) Regulations 2020[79] enact into law, inter alia, the nine principles that apply to any firm carrying out by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belonging to others.

The regulations set out concise authorisation conditions, conduct of business, notification and reporting requirements, and the applicable regulatory powers of the GFSC. The nine Regulatory Principles, outlined in the Schedule, are that a DLT Provider must:

1. conduct its business with honesty and integrity;
2. pay due regard to the interests and needs of each and all its customers and must communicate with them in a way that is fair, clear, and not misleading;
3. maintain adequate financial and non-financial resources;
4. manage and control its business effectively, and conduct its business with due skill, care, and diligence; including having proper regard to risks to its business and customers;
5. have effective arrangements in place for the protection of customer assets and money when it is responsible for them;
6. have effective corporate governance arrangements;
7. ensure that all of its systems and security access protocols are maintained to appropriate high standards;
8. have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing; and
9. be resilient and have contingency arrangements for the orderly and solvent wind-down of its business.

[79] https://www.gibraltarlaws.gov.gi/legislations/financial-services-distributed-ledger-technology-providers-regulations-2020-4774

As noted under '**Error! Reference source not found.**', earlier in this document, a principles-based approach has allowed the framework to evolve alongside DLT, its application and markets, whilst remaining aligned to the core regulatory and legislative intentions. Principles-based regulation, supported by detailed guidance that can be periodically updated, clarified, and refined, provides for appropriately flexible and responsive oversight of a nascent and developing industry. Many aspects of the DLT Principles would also be appropriate to include in a regulatory framework for DeFi.

Algorithmic Trading (MiFID II)

Algorithmic trading uses computer algorithms to automatically determine parameters of orders and trades in financial markets, such as the timing, price, and type of financial instrument to execute, with limited or no human intervention. High-frequency algorithmic trading (HFAT) is a sub-category of this, which uses specialised technologies, techniques, and quantitative models to minimise latency[80] and execute high volumes of orders in quick succession – with intervals often measured in microseconds; millionths of a second – to exploit or arbitrage slower-paced market events and price formation.

Certain economists have argued that HFAT provides potential advantages for markets, with greater efficiency achieved with increased liquidity[81], facilitation of larger trades[82], improved pricing efficiency[83], tighter bid-ask spreads[84] and lower transaction costs[85]. New risks are also created, however; namely the increased speed of shock transmission across different markets, and consequent increases to systemic risk[86]. As algorithmic trading and HFAT evolved during the first decade of the 21st century, numerous 'flash-crashes' were attributed to their activities. Author Michael Lewis explained the most notorious of these in his 2014 book, Flash Boys[87], when on May 6th, 2010, the Dow Jones index rapidly collapsed and rebounded, briefly losing 998.5 points and an estimated $1trn in value and triggering immense panic across international markets. These events were later determined to have been triggered by a single order of futures on the S&P 500 index that prompted an uncontrolled cascade of automatic HFAT sell orders.

Several of the obvious benefits offered by automated DeFi applications and smart contracts – such as increased liquidity, improved efficiency, better pricing, and lower costs – are similar to those touted by automated algorithmic trading. There are also similarities to be seen in the concerns of regulatory authorities regarding the potential risks that automation presents. Prior to the introduction of MiFID II, algorithmic trading – including HFAT – was not subject to any specific regulatory controls, beyond those applicable to any other trading activities in the

[80] https://www.exegy.com/2020/02/ultra-low-latency-trading-infrastructure/
[81] Henershott, Jones and Menkveld, 'Does Algorithmic Trading Improve Liquidity?', 2010.
[82] Joel Hasbroucka, Gideon Saarb, 'Low-latency trading', 2013
[83] Brogaard and Garriott, High-Frequency Trading Competition', 2014
[84] Hagstromer and Nordén, 'The Diversity of High-Frequency Traders', 2012
[85] Chlistalla, 'High-Frequency Trading – Better than its Reputation?', 2011
[86] See https://corporatefinanceinstitute.com/resources/knowledge/finance/what-is-systemic-risk/
[87] http://michaellewiswrites.com/#flash-boys

financial markets in which they operated. Article 17 of MiFID II[88] introduced specific requirements for firms engaged in or facilitating algorithmic trading, including specific detailed record-keeping requirements for HFAT.

It is of course recognised that the nature of algorithmic trading and HFAT differs substantially from DeFi in many fundamental ways; the relevance in this context is that existing regulatory solutions have been agreed upon and adopted to mitigate specific risks arising as a result of automation. This provides a sound precedent and foundation from which appropriate and proportionate solutions may be developed for DeFi.

Under MiFID II, any firm engaged in algorithmic trading must:

- have effective systems and controls to ensure its trading systems are resilient and have enough capacity;
- implement appropriate trading thresholds and limits, and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market;
- have effective systems and risk controls to ensure the trading systems cannot be used for any purpose that is contrary to the market regulations, or rules of a trading venue to which it is connected; and
- test and monitor these systems, and have effective business continuity arrangements to deal with any failures.

DApps definitively operate in a decentralised manner, meaning their 'systems' are a globally distributed network of internet-connected computers, and any requirements around resilience, monitoring, testing, and business continuity are largely irrelevant. Conceptually, minimum requirements for the number of nodes a DApp must operate across might ensure resilience and capacity; however, increased adoption of a given blockchain incentivises growth in the number of nodes powering it. It may also be argued that establishing any such limits would be inappropriate or regulatory overreach, providing information on the number of active nodes is publicly available. Furthermore, as DApps merely facilitate the execution of transactions – as opposed to trading algorithms that make decisions and behave as autonomous participants – requirements relating to thresholds and limits would not be applicable.

It is reasonable, however, that a regulatory framework should seek to ensure that a DApp cannot create erroneous transactions, or otherwise function in a way that may create a disorderly marketplace, and cannot be used for any purpose that is contrary to any applicable laws and rules.

[88]Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=en

Testing & Development

Requirements for the testing and deployment of trading algorithms, systems and strategies are outlined in Chapter II, Section I of the Regulatory Technical Standards (RTS) for firms engaged in algorithmic trading[89]. Prior to the deployment or any substantial update of an algorithmic trading system or algorithm, firms must subject them to clearly defined testing methodologies in a dedicated 'non-live' environment, where there is no risk of interaction with operating market systems. These tests ensure that the system or algorithm:

- does not behave in an unintended manner;
- complies with the firm's regulatory obligations;
- complies with the rules and systems of the trading venues being accessed;
- does not contribute to disorderly trading conditions, and continues to work effectively in stressed market conditions; and
- where necessary, can be switched off or disabled.

This includes conformance testing, which ensures the system or algorithm conforms with the trading venue or DEA provider's systems, continuing to operate correctly and according to all applicable requirements. Subsequent to testing, a designated individual is required to formally authorise the deployment or material change. All material changes to the system or algorithm must be recorded, including the nature of the change, when and by whom it was made, and who approved it. Once tested and approved, the system or algorithm must be deployed in a controlled manner, with predefined limits on the number of instruments being traded, the price, value and numbers of orders and the number of trading venues to which orders can be sent.

As noted previously, only specific aspects of the requirements relating to algorithmic trading are appropriate in the context of DeFi. Limits on the instruments, prices, values, orders, and venues for trading algorithms are unlikely to be relevant to the functions of a DApp, and any such limits imposed may result only in unfavourable conditions for its participants. It stands to reason, however, that a regulatory framework should require comprehensive testing and assessment of DApps, in a controlled environment, to ensure they behave as intended and do not contribute to disorderly conditions for their participants. Such testing and assurance would appropriately extend to any material changes to a DApp, and record-keeping of testing details would provide accountability for all testing. The ability for a DApp to be deactivated, in the event of unexpected or detrimental behaviours, may also be an appropriate control to protect the interests of DeFi participants.

Direct Electronic Access

Direct electronic access (DEA) is a service or arrangement under which a member of a trading venue allows a client to make use of their trading code – essentially their account – thereby giving that client direct access to the trading venue's systems and order book. DEA is largely

[89]Commission Delegated Regulation (EU) 2017/59 of 19 July 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0589&from=EN

used to facilitate algorithmic trading, primarily HFAT, as it enables the incredibly precise determination of order entry times and the lifetimes of orders. However, under Chapter II of the RTS[90], firms that offer DEA remain responsible for the activities of their clients on the trading venue, and must ensure:

- proper assessment and review of the suitability of clients using the service;
- that clients using the service cannot exceed any pre-set trading and credit thresholds;
- that trading by clients using the service is properly monitored; and
- that appropriate risk controls prevent trading that may create risks to the firm itself or that could create or contribute to a disorderly market.

Trading venues that permit DEA must have effective systems, procedures, and arrangements in place to ensure that:

- only appropriately regulated members are permitted to provide DEA;
- appropriate criteria are applied regarding the suitability of those to whom DEA is provided; and
- the DEA provider retains responsibility for the trading activity.

Trading venues must be able to halt trading by those using DEA, separately from the member's other trading activity, and to suspend or terminate the provision of DEA by a member. They must also be able to temporarily halt or constrain trading, and in exceptional cases to cancel, vary or correct transactions. Such powers must be calibrated in a way that takes into account the liquidity of different products, and the nature of the market and its users, to avoid significant disruptions to orderly trading and market conditions.

These requirements may be considered relevant to DeFi insomuch as they apply controls to regulated entities who enable or allow automated trading algorithms to access and influence marketplaces. Accordingly, the assessment of DApps by a regulated entity, who remains accountable for the operation of any DApps they approve, would be an effective approach that would be internationally justifiable and comparable, yet not necessitate the regulation of developers. Again, the potential ability to limit or halt the activity of a DApp under specific circumstances may be an appropriate control. The relevance of concepts such as trading and credit thresholds would be limited to very specific DeFi applications, and would fall within the proper assessment and testing of a DApp by a regulated entity.

Key Information Documents (PRIIPs)

A Packaged Retail & Insurance-based Investment Product (PRIIP) is defined as an investment where the amount repayable to a retail investor is subject to fluctuations due to exposure to reference values or the performance of one or more assets that are not being directly purchased. The EU PRIIPS Regulation[91] came into effect in January 2018, and requires anyone 'manufacturing' (i.e., creating) or 'distributing' (i.e., selling on) a PRIIP to provide retail investors

[90] Commission Delegated Regulation (EU) 2017/59 of 19 July 2016)

[91] Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1286&from=en

with a Key Information Document (KID), drafted in a standardised format and according to regulatory criteria.

PRIIPs KIDs are an investor protection mechanism, designed to help retail investors understand investment products and how they behave, to enable fair and informed comparisons with other, similar products. The KID is a 3-page document that clearly communicates the nature, risks, costs and potential gains and losses of the relevant investment product in plain, easily understandable wording. It must be provided in the local language of the potential investor, and must be published on the firm's website prior to the product being made available to retail investors.

This is relevant to DeFi in the context of the complexity in understanding the functions and behaviours of a given DApp or DeFi ecosystem for many potential participants. It is understood that many crypto enthusiasts, developers and cypherpunks[92] are equipped with the skills and expertise to interrogate source code and understand the functions and vulnerabilities of a DApp and its smart contracts, whereas the overwhelming majority of current DeFi participants – not to mention the general public whose participation will drive mass adoption – are certainly not. The need to trust and depend upon the veracity of assessments by others, who are mostly anonymous and always unregulated and unaccountable, is not conducive to a fair and functional marketplace.

A regulatory framework should require that the key information required for potential participants to understand the functions and behaviours of DApps is documented, in a clear and consistent format, and made available to potential participants by regulated and accountable parties. Such basic principles of transparency, investor protection and accountability align to the interests of both regulators and DeFi participants, and are necessary to facilitate ongoing, sustainable innovation and mass adoption of DeFi.

FATF Recommendations

FATF's Interpretive Note to Recommendation 15 (New Technologies) states that Recommendations 10 to 21 apply to VASPs, encompassing customer due diligence, record keeping, additional measures for Politically Exposed Persons (PEPs), cross-border and domestic transfers, reliance on third parties, internal controls, higher-risk countries, and the reporting of suspicious transactions.

Under Recommendation 10, Customer due diligence, FATF requires the following measures:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information.
b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions understanding the ownership and control structure of the customer.

[92] https://en.wikipedia.org/wiki/Cypherpunk

c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Under Recommendation 17, Reliance on Third Parties, financial institutions may be permitted to rely on third parties to perform elements of customer due diligence, but such reliance must be limited to measures a) to c) of Recommendation 10, as outlined above, and requires that the financial institution:

- immediately obtain the necessary information concerning the due diligence performed;
- satisfy itself that copies of identification data and other relevant documentation will be made available from the third party when requested and without delay; and
- satisfy itself that the third party is regulated, supervised, or monitored for, and has measures in place for compliance with, due diligence and record-keeping requirements.

Where such reliance is permitted, the ultimate responsibility for due diligence measures remains with the financial institution that is relying on the third party. FATF contrasts 'reliance on third parties' with an outsourcing or agency relationship, however, stating in their Interpretive Note to Recommendation 17 that:

> *"the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity".*

It is evident that neither a third-party reliance, nor an outsourcing/agency approach, would be appropriate to meet the requirements of the FATF Recommendations. As previously noted under '**Error! Reference source not found.**', '**Error! Reference source not found.**', earlier in this document, human intervention and operational processes completely corrupt the DeFi concept and model. A viable and acceptable approach to regulating DeFi must, therefore, enable the application of FATF-compliant AML/CFTP controls, without enforcing these on developers. Such controls must be conducted by an authorised and regulated entity, to ensure accountability and alignment with existing regulatory standards. The corollary is that such an entity would need to be regulated as a financial institution, requiring the determination of an appropriate regulatory category; this should not reasonably be an intractable obstacle, however.

Recommendation 26, Regulation and Supervision of Financial Institutions, states that financial institutions should be subject to adequate regulation and supervision and must effectively implement the FATF Recommendations. The interpretive note to Recommendation 26 describes the risk-based approach, which refers both to the flexibility in how supervisors may choose to allocate their resources to AML/CFT supervision, according to their understanding of the risks; and to the specific process of supervising institutions that themselves apply an AML/CFT risk-based approach. The Introduction to the Recommendations[93], FATF states:

> *"The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way."*

Providing all regulatory control requirements and outcomes can be satisfied, and identified risks mitigated to an equivalent extent as in traditional market structures, the efficient separation of autonomous functionality from regulated manual operations in DeFi is both rational and achievable. Decentralising the legacy functions of a single financial institution, with consistent and appropriate regulatory controls, accountability and oversight for respective activities performed, can be realised without deviating from the FATF Recommendations and intentions.

[93] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Proposed Solutions

This section draws from earlier assessments of emerging regulatory challenges, the underlying central objectives, identified relevant precedents, and reflections on appropriate approaches to regulation for DeFi, to outline proposals and concepts that could present a solution to these various complexities and responsibilities.

As noted earlier in this document, aspects of MiCAR and the draft FATF Guidance would restrict DeFi in ways that are neither workable nor enforceable, whilst simultaneously failing to mitigate the potential risks presented. Constructive prohibition of DeFi ecosystems would senselessly criminalise their development, decimating innovation, and forcing residual participants – through want or need of DeFi products or services – to use illegal, still-unregulated, ecosystems. Notably, such an approach and potential outcome is in stark discord with each of the OECD's conclusions on positive regulation for innovation, as summarised earlier under '**Error! Reference source not found.**'. Alternatively, providing a viable and accessible pathway to compliant DeFi environments – in a manner that effectively mitigates risks and cultivates investor protection and confidence – could both fulfil all defensible regulatory objectives, and facilitate the ongoing innovation, growth, and broad adoption of DeFi. Provided with the choice, the majority of people will gravitate towards trustworthy and accountable marketplaces over those that are unregulated and anonymous, generating natural momentum of participants and liquidity towards compliant environments.

The following proposals are intended as an introductory exploration of the concepts presented, as a foundation for discussion and debate; they should therefore be considered neither final nor complete. Numerous outstanding questions and issues would require careful consideration and input from relevant technical experts.

Legal Personality

The regulatory intentions of accountability and liability, for compliant DeFi ecosystems and DApps, can be achieved with the introduction of authorised and regulated entities who are responsible for evaluating, testing, documenting and approving DeFi ecosystems and DApps (hereafter referred to as 'DeFi Evaluators'). Providing for accountability and liability concerning AML/CFTP compliance is outlined separately, under '**Error! Reference source not found.**', below.

Regulated DeFi Evaluators

Under this concept, DeFi Evaluators would receive submissions of DApps from developers in order to undergo formal review and approval. This may be considered as somewhat similar to listing processes conducted by regulated financial institutions for financial instruments submitted for listing on a regulated market or stock exchange. Listing requires, inter alia, that due diligence be performed on the instrument's issuer, and the structure and terms of the issuance and all supporting documentation (such as prospectuses) are reviewed to ensure compliance with all applicable regulatory requirements. This well-established process ensures

that identifiable regulated parties are accountable for the legitimacy of financial instruments that are admitted to sale to the public.

The DeFi Evaluators would be responsible for conducting comprehensive evaluations, including analysis of the source code[94], of each DApp and its smart contracts, to identify any issues, vulnerabilities, or flaws. Rigorous testing and assessments should be performed, in a controlled environment, to ensure that the DApp and smart contracts:

- operate in a stable and predictable manner;
- function as stated and intended;
- do not create or contribute to a disorderly or detrimental market environment; and
- cannot be used for any purposes that are contrary to any applicable rules or the fair treatment of its participants.

Full and precise details of all automated functions should be documented in a clear and consistent prescribed format, to provide any participants with the key information required to understand all functions and behaviours. This Key Information Document ('DeFi KID[95]') should include, but not be limited to:

- all rules regarding the functioning and use of the DApp, such as the calculation of prices or rates;
- levels and distribution of any fees;
- mechanisms of exchange, settlement and/or custody; and
- any eligibility criteria for participants.

Accountable verification of a DApp's compliance with applicable rules may require that DeFi Evaluators ensure the second identified regulatory challenge, **Error! Reference source not found.**, is also satisfied. The envisaged solution for this is outlined separately, below; however, it is recognised that this would require the inclusion, testing and verification of specific additional components in approved DApps, and may necessitate coordination between both regulated parties.

Should there exist any administrative keys, or other ability to modify the DApp or smart contracts in future, the DeFi Evaluators should act as custodians of at least one set of multi-signature[96] keys needed to affect any such modifications or events. This would ensure that no changes could be made to the DApp, as tested, and documented by the DeFi Evaluators, without their knowledge and involvement. As necessary, the DeFi Evaluators may therefore undertake further reviews, testing and documentation of any changes, prior to their release or activation. Such controls will be important, both for the DeFi Evaluators – who will be held accountable for the DApp's performance and activities – and for participants, whose assets may be at risk from any issues or compromises.

[94] https://searchapparchitecture.techtarget.com/definition/source-code
[95] For regulatory context on this name, see **Error! Reference source not found.**, **Error! Reference source not found.**, earlier in this document.
[96] Multi-signature, or 'multisig' refers to a contract that can execute actions only when a predefined number of trusted parties agree to it.

Where a DApp operates on the basis of participant governance – whereby governance proposals are created and voted on by distributed holders of governance tokens[97], for example –DeFi Evaluators should be responsible for ensuring that:

- any voted changes do not conflict with nor undermine the criteria on which the DApp was tested and verified;
- the developers implement changes in accordance with the votes; and
- any material changes are subject to appropriate reviews, testing and documentation in the DeFi KID.

The possibility that DeFi Evaluators should hold separate 'master' administration keys, with specific and limited functionality, should also be explored. This may enable, for example, the halting of some or all of a DApp's operation in the event of unexpected behaviours or issues, without the need for coordination between multiple parties. Any such abilities on the part of the DeFi Evaluators should be subject to clear and prescriptive regulatory limitations, and the details of any such mechanism should be clearly identified in the DeFi KID.

Requirements for the periodic re-assessment of DApps by DeFi Evaluators should be considered, including the degree to which such requirements should be proportionate to the scale, complexity and volumes of a given DApp, and what ongoing controls may be necessary to ensure market integrity in certain DeFi ecosystems. The combination of periodic re-evaluation and automated ongoing risk control mechanisms are inherent in traditional algorithmic and HFAT trading environments. Highly leveraged cryptocurrency trading instruments in both centralised and decentralised marketplaces can lead to similar 'flash-crash' risks as those seen in traditional markets[98]. In light of this, the use and efficacy of automated pricing and execution 'shock absorber' or selective 'kill switch' algorithms, for enhanced market integrity and autonomous risk management, should be assessed both qualitatively and quantitatively. Theoretically, such controls may utilise specialised DeFi 'oracles'[99] – which relay information from non-blockchain data sources to smart contracts within a blockchain ecosystem – to provide relevant, dynamic risk data.

The possibility of establishing minimum requirements for the number of nodes[100] that a DApp must run on, to ensure sufficient decentralisation, resilience, and capacity, should be explored. It may be argued, however, that such limits would need to be proportionate to the value of assets exposed to the DApp, and that increased adoption of a given blockchain will generate a higher volume of nodes. Viable approaches to financing the activities of the DeFi Evaluator and DApp approval process should also be explored; conceptually, certain developers may prefer to fund this directly, or it may alternatively be funded by apportioning an agreed share of the fees or value generated by the DApp to the DeFi Evaluator. It is recognised that receiving

[97] https://academy.shrimpy.io/post/what-are-governance-tokens
[98] https://cryptonews.com/news/flash-crash-post-mortem-overleveraged-crypto-gamblers-did-it-10390.htm
[99] https://dataflog.com/read/a-comprehensive-guide-defi-oracles-fundamentals/13081
[100] https://101blockchains.com/blockchain-nodes/

a share of DApp fees may expose DeFi Evaluators to some commercial risk, in addition to potential conflicts of interest, which therefore requires careful consideration.

Financial Crime Compliance

The regulatory intentions of applying adequate and effective ongoing AML/CFTP controls within DeFi ecosystems and DApps can be achieved with the introduction of authorised and regulated entities who implement and conduct the relevant regulatory processes on behalf of third parties, including (but not necessarily limited to) DeFi ecosystems and DApps (hereafter referred to as 'AML Infrastructures').

Regulated AML Infrastructure

Under this concept, developers would be able to request the services of an entity that is authorised and regulated to perform all relevant financial crime risk management activities on behalf of third parties, including DApps, and who has the necessary operational infrastructure and capabilities to do so. As with the DeFi Evaluators, proposed above, potential approaches to financing such activities should be explored. The ongoing nature of AML/CFTP requirements and controls may mean that funding via a share of fees or returns generated by the DApp seems practical. As noted with respect to DeFi Evaluators, however, this would give rise to potential risks and conflicts of interest, where an AML Infrastructure may be economically incentivised to maximise numbers of users, at the expense of proper controls.

The AML Infrastructure should be required to conduct due diligence and risk assessments on each DApp, to determine the appropriate controls to apply, and to produce and maintain relevant policies specific to each DApp or DeFi ecosystem served. The AML Infrastructure should have in place sufficient systems and capabilities to perform all necessary screening and monitoring, and to ensure their staff have the understanding, knowledge, and training to adequately manage such activities. Officers of the AML Infrastructure should be subject to approval by the GFSC as Regulated Individuals, to ensure accountability and alignment with existing regulatory standards.

The AML Infrastructure would provide an interface and process by which applicants seeking to participate in a DApp may be onboarded, including the capture, verification and screening of information and documents, in accordance with the relevant AML/CFTP requirements and policies. The eligibility criteria for access to a DApp should be aligned both to relevant laws and any criteria stipulated in the (previously proposed) DeFi KID. The AML Infrastructure would be responsible for managing all ongoing controls, in compliance with all AML/CFTP regulations and guidance, including ongoing monitoring of identities, risks and transactions, the performance of ongoing, incremental, and enhanced due diligence as required, and the preparation and submission of necessary reports to regulatory and legal authorities. The AML Infrastructure would also be responsible for satisfying all requirements related to the FATF

Travel Rule[101], although much of this could be internalised by such an infrastructure, diminishing the need for data transmission.

It will be important, when seeking to realise the potential societal benefits DeFi offers, to restrict the perpetuation of financial exclusion and unjust barriers to entry, as referenced earlier under '**Error! Reference source not found.**'. AML Infrastructures should, therefore, be required to implement meaningful measures that facilitate financial inclusion and avoid exclusionary de-risking[102]. This must be achieved in ways that do not undermine the integrity of financial crime risk management, but which nonetheless provide equitable access to DeFi products and services.

In order to protect the personal data of applicants and participants, the AML Infrastructure should be subject to strict systems, cybersecurity, and physical security regulatory requirements, as required for DLT Providers under the Gibraltar DLT Framework[103]. Conceptually, participation in a DApp by eligible and verified applicants could be enabled by the issuance of non-transferrable[104], non-fungible[105] tokens ('NTNFTs') by the AML Infrastructure to the relevant wallets of each verified participant. Such an NTNFT would enable the AML Infrastructure to link the wallet and activities to the relevant participant, without their personal data or identity being exposed to the DApp or any of its other participants. Once a party has been onboarded by the AML Infrastructure, they should be able to access additional DApps using the same issuance mechanism, without necessarily requiring a repeated onboarding process.

It is noted that, under this proposal, each DApp would be required to encode specific controls to prohibit participation by wallets not containing such an NTNFT, and that the integrity of such controls would be of vital importance to the management of financial crime risks. The potential need for supplementary forms of verification between DApps and AML Infrastructures should be explored, such as additional layers of authentication, to mitigate any risks of fraudulent or hacked tokens bypassing these controls. As previously noted under '**Error! Reference source not found.**', above, such components would need to be included in the testing, verification, and documentation of the DApp.

Developers

The express intent of these proposals is to satisfy the aims and objectives of regulators with respect to financial systems and markets, whilst enabling DeFi developers and innovators to remain outside of the regulatory perimeter. The necessity for and, if relevant, the appropriate extent of AML/CFTP due diligence to which developers of DApps should be subject, however, must be considered.

[101] See '**Error! Reference source not found.**', earlier in this document.
[102] https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector
[103] See '**Error! Reference source not found.**', earlier in this document.
[104] https://medium.com/@cryptolions/introducing-non-transferable-tokens-ntts-2f1a532bf170
[105] https://en.wikipedia.org/wiki/Non-fungible_token

Whilst the solutions proposed above would substantially mitigate risks of compliant DeFi solutions being used to commit fraud or theft, or to launder the proceeds of crime, there remains an inherent risk that DApps might be developed by parties who are subject to sanctions or engaged in terrorism or proliferation financing. Consequently, screening for connections to these activities should be conducted as a minimum. Whether such screening should be conducted by the DeFi Evaluator, by the AML Infrastructure, or both parties together, should be explored.

Next Steps

An abridged version of this document will be submitted to the Gibraltar Association for New Technologies (GANT), for consideration in ongoing working groups and industry engagement initiatives. As previously noted, the proposals and concepts presented are intended as an introductory exploration of the topics addressed, to provide a foundation from which to initiate and inform discussion and debate. Subsequent to review, challenge, discussion and debate with relevant experts, industry peers and stakeholders, there is an intention that collective proposals for appropriate enhancements to the Gibraltar regulatory framework be agreed and presented for discussion with appropriate representatives of Her Majesty's Government of Gibraltar and the GFSC.

In conclusion, Gibraltar has a unique and timely opportunity to build upon its current standing as one of the world's foremost DLT jurisdictions. Given the chance to access compliant and accountable DeFi ecosystems, a far broader audience will be incentivised to enter these new, highly efficient, and innovative marketplaces. This would provide instrumental support to the mass adoption of DeFi, further enhance Gibraltar's attractiveness to many businesses, innovators, and developers, and help to fuel the jurisdiction's ongoing prosperity. Thanks to its progressive stance towards technical innovation, and the agility afforded by its scale and domestic legislature, Gibraltar is able to adopt and enact legislative and regulatory developments more efficiently than almost any other jurisdiction; and by pioneering a framework that offers regulatory certainty and a viable pathway for compliant and accountable DeFi innovation and adoption, has the potential to realise significant economic, social, and strategic benefits.