SPA/2022/01 January 2022

SEACEN POLICY ANALYSIS

STABLECOINS AND REGULATORY CLARITY FROM THE FINANCIAL ACTION TASK FORCE

Mark McKenzie

The SEACEN Centre

The South East Asian Central Banks (SEACEN) Research and Training Centre

SPA/2022/01 January 2022

SEACEN POLICY ANALYSIS

STABLECOINS AND REGULATORY CLARITY FROM THE FINANCIAL ACTION TASK FORCE

Mark McKenzie

The SEACEN Centre

The South East Asian Central Banks (SEACEN) Research and Training Centre

Level 5 Sasana Kijang, Bank Negara Malaysia,
2 Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
Tel. No.: +603 9195 1888
Fax. No: +603 9195 1801
Email: enquiries@seacen.org

For enquiries, please contact:
Mark McKenzie
Senior Financial Sector Specialist
Financial Stability and Supervision & Payment and Settlement Systems (FSS&PSS)
The SEACEN Centre
Email: mark@seacen.org

The ***SEACEN Policy Analysis:*** **Stablecoins and Regulatory Clarity from the Financial Action Task Force** reflects the analysis and views of SEACEN staff and do not represent the views of its member central banks and monetary authorities.

Notes:

The SEACEN Centre recognizes "China" as People's Republic of China; "Hong Kong, SAR" as Hong Kong, China; and Korea as "Republic of Korea".

FOREWORD

The current paper, "Stablecoins and Regulatory Clarity from the FATF" by Mark McKenzie, Senior Financial Sector Specialist, Financial Stability, Supervision and Payments at The SEACEN Centre is a review of the Financial Action Task Force's (FATF's) Updated Guidance for a Risk-Based Approach (RBA) for Virtual Assets (VAs) and Virtual Assets Service Providers (VASPs) issued in October 2021. The paper underscores that one of the biggest challenges hampering the emergence of a clear regulatory framework in the nascent virtual assets space relates to the issue of classification, which has recently attracted significant attention, notably in the virtual asset space of stablecoins.

Stablecoins are a type of digital asset that purports to maintain a stable value by referencing physical or financial assets or virtual assets (FSB (2020)). While today stablecoins are primarily used to facilitate trading of other digital assets, the FATF noted that stablecoin digital currencies have the potential for mass adoption and could be used to launder money or fund terrorism and warned of the risks of this fast-growing virtual asset. Indeed, stablecoins have proliferated during the pandemic. However, policymakers and regulators fear that a sudden loss of confidence could have a devastating impact on financial market stability and potential cross border market contagion.

This study emphasizes the importance of identifying the central party and understanding the governance arrangement underlying stablecoins for AML/CFT purposes. It develops a stablecoin risk assessment framework that can be helpful for policymakers including supervisors and regulators. We acknowledge that risks associated with stablecoins go well beyond ML/TF and fraud risks. The paper concludes that stablecoins and other emerging technologies are fast evolving and as such we can expect further clarifications from the FATF and other standard setting bodies in the future.

We hope that this policy paper provides some initial analysis of the rapid development of the digital financial ecosystem as it can have wide ranging implications of the monetary and financial system, calling for a robust regulatory framework. I wish to emphasize that the views expressed in this and all issues of the SEACEN Policy Analysis series are those of the author and do not represent the views of SEACEN's member, associate member, and observer central banks and monetary authorities. At the SEACEN Centre, we continue to maintain a flexible strategy by providing online learnings of the pandemic, while carrying out policy analysis of the responses on the macroeconomic, monetary, and financial front. We stand ready to provide assistance to members in building and strengthening their capacity during this time.

Mangal Goswami
Executive Director
The SEACEN Centre

January 2022

ABSTRACT

The purpose of this policy paper is to highlight the most recent updates relating to stablecoin based on the FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. We note that one of the biggest challenges hampering the emergence of a clear regulatory framework in the nascent virtual assets space relates to classification. However, we are beginning to see some move towards an accepted classification for regulatory purposes. One area attracting significant attention in the virtual asset space is stablecoins. Based on our review and understanding of the FATF's Updated Guidance, identifying the central party and governance is key for the FATF's AML/CFT risk assessment of stablecoins. In our review of the FATF's Updated Guidance, we also looked at the guidance provided for (i) non-fungible tokens (NFT), (ii) decentralised finance (DeFi), and (iii) software applications. Using the information, we created a stablecoin risk assessment framework as well as provide an Annex with (i) the determining factors, (ii) risk assessment actions requirements and (iii) suggested questions. We are hoping that interested parties including regulatory and supervisory agencies will find our stablecion risk assessment framework and the Annex useful when conducting risk assessment of stablecoins and other emerging technologies. We concluded that stablecoins and other emerging technologies are fast evolving and transforming, and as such we can expect further clarifications from the FATF and other standard setting bodies in the future.

TABLE OF CONTENTS

STABLECOINS AND REGULATORY CLARITY FROM THE FINANCIAL ACTION TASK FORCE

One of the biggest challenges hampering the emergence of a clear regulatory framework in the nascent virtual assets[1] space relates to classification. A virtual asset is 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 Financial Action Task Force (FATF) *Recommendations*.[2] Virtual assets have emerged as a direct result of recent digital technological advances, and their purpose is to provide new possibilities for peer-to-peer (P2P) transactions, investment, and financial transactions.

In terms of classification, the appellation 'cryptocurrency' has been used as a catch-all term to refer to products such as coins and tokens considered native to blockchain technology as well as actual cryptocurrencies irrespective of their purposes or functions. In reality, these products tend to fulfil different functions such as payments, banking, securities, investments, etc.

Very often when considering classification in the fairly nascent space comparisons are made with traditional currencies, securities, banking, and financial products. By categorising them as either currencies, commodities or tokens, we can start to evaluate their regulatory, legal, tax and accounting impact. Many analysts think cryptocurrencies represent an entirely new asset class.

The source of the problem when classifying virtual assets is the hybrid and transformative nature inherent in the nascent universe of virtual assets and cryptocurrencies.[3] While an uniform lexicon and classification could vastly clarify the regulatory implications, new virtual assets might not necessarily fit cleanly into one asset class. This feature, market developments, and the rapid pace of innovation compound regulatory challenges with gaps that need to be carefully studied and addressed.

Nevertheless, we are beginning to see some move towards an accepted classification for regulatory purposes. To define the appropriate regulatory treatment, authorities find it helpful to differentiate virtual assets by certain criteria. There are a number of different criteria for classifying virtual assets. Examples of criteria being used to define the appropriate regulatory treatment by some jurisdictions or standard setting bodies (SSBs) are based on (i) functionality, (ii) stabilization mechanisms and (iii) systemic importance. The classification criteria are likely to continue to evolve as new business models emerge in the markets.

One area attracting significant attention in the virtual asset space is stablecoins. For example, in October 2021, the FATF issued an Updated Guidance for a Risk-Based Approach (RBA) for Virtual Assets (VAs) and Virtual Assets Service Providers (VASPs) in which it provides clarity on the application of

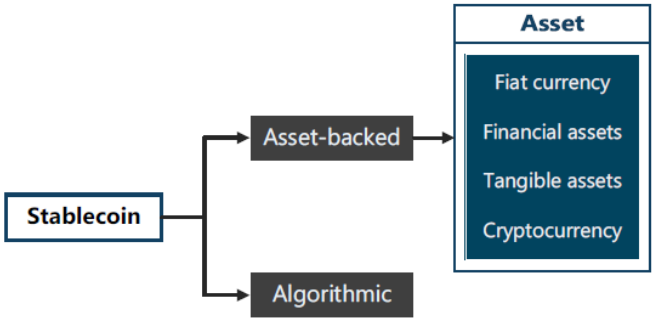
1. For consistency, the term virtual assets will be used instead of cryptoassets.
2. Glossary of the FATF Recommendations.
3. Cryptocurrency is a relatively new type of digital currency/ money that refers to a type of virtual currency that implements cryptography technology to secure and authenticate currency transactions on a decentralized blockchain networks. According to the Corporate Finance Institute, digital currency is a broad concept, referring to all the monetary assets that are in digital form. Virtual currency is a subset of digital currency, and cryptocurrency is a subset of virtual currency. Digital currency can be either regulated or unregulated. A regulated digital currency is issued by a country's central bank and can be denominated to a sovereign currency. The regulated type of digital currency is thus subject to a country's monetary policy. Virtual currency is a type of unregulated digital currency. It is issued and controlled by a private issuer instead of a central bank. Therefore, it is not subject to any monetary policy. A virtual currency can be either centralized or decentralized. Some virtual currencies contain cryptography, and some do not.

the FATF Standards in relation to stablecoins. The FATF noted that stablecoin digital currencies have the potential for mass adoption and could be used to launder money or fund terrorism and warns of the risks of this fast-growing [virtual] asset. To this end, countries and crypto-related companies should pinpoint such risks before stablecoins are launched and take measures to address them. Like cryptocurrencies such as bitcoin, stablecoins risk being used for financial crimes because of "their potential for anonymity, global reach and use to layer illicit funds," said FATF, which underpins global efforts on money laundering and other financial crimes.

Another example of the attention being given to stablecoins is the President's Working Group on Financial Markets (PWG) in the United States. In November 2021, PWG, joined by the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC), released a report on stablecoins. Janet L. Yellen, U.S. Secretary of the Treasury, noted[4] "Stablecoins that are well-designed and subject to appropriate oversight have the potential to support beneficial payments options. But the absence of appropriate oversight presents risks to users and the broader system. Current oversight is inconsistent and fragmented, with some stablecoins effectively falling outside the regulatory perimeter. Treasury and the agencies involved in this report look forward to working with Members of Congress from both parties on this issue. While Congress considers action, regulators will continue to operate within their mandates to address the risks of these assets."

Stablecoins are a type of digital asset that purports to maintain a stable value by referencing physical or financial assets or virtual assets (FSB (2020)). They can be further differentiated into currency-based, financial instrument-based, commodity-based and crypto asset-based stablecoins. There are also algorithmic stablecoins that purport to maintain a stable value *via* protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand (FSB (2020)) (Figure 1).

Figure 1: Stabilisation mechanisms



Source: Garcia *et al.* (2021).

Tether, which is designed to be pegged to the US dollar one-to-one is the most popular and largest stablecoin globally. It has more than $60 billion worth of tokens in circulation, which is more than the deposits of many U.S. banks. Crypto traders often use Tether to buy cryptocurrencies, as an alternative to the greenback. Tether is often compared to money market funds, but without regulation. Policymakers and regulators fear that that a sudden loss of confidence in Tether could result in a "severe liquidity shock to the broader cryptocurrency market." There are also concerns that a sudden increase of Tether withdrawals could lead to potential market contagion, affecting assets beyond crypto. According to Eric Rosengren, Boston Federal Reserve Bank President, "A future crisis could easily be triggered as these become a more important sector of the financial market, unless we start regulating them and making sure that there's actually a lot more […] stability to what's being marketed to the general public as a stablecoin."[5] Fitch Ratings warned that a sudden mass redemption of Tether tokens could destabilize short-term credit markets. (Interestingly enough, Tether is not the only global stablecoin; there are others such as USD Coin and Binance USD).

4. U.S. Treasury Department's Press Release President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins, Nov. 1, 2021.

5. 5 takeaways from Boston Fed President Eric Rosengren's June 25, 2021, remarks to the Official Monetary and Financial Institutions-Federal Reserve Bank Philadelphia Fed Week June 21- 25, 2021 Forum.

While today stablecoins are primarily used to facilitate trading of other digital assets, stablecoins could be more widely used in the future as a means of payment by households and businesses. Stablecoins that are backed by relatively safe, highly liquid assets may pose fewer risks than either stablecoins that use fractional reserves or adopt higher-risk asset allocations, or bitcoin and other crypto assets, However, regulators are concerned if the footprint is potentially global or systemic.

The purpose of this policy paper is to highlight the most recent updates relating to stablecoin based on the FATF's *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Based on our review and understanding of the FATF's *Updated Guidance*, identifying the central party and governance is key for the FATF's AML/CFT risk assessment. Using this information, we created a stablecoin risk assessment framework as well as provide an Annex with (i) the determining factors, (ii) risk assessment action requirements and (iii) suggested questions that interested parties can use during the risk assessment of stablecoins and other emerging technologies.

Background of the FATF Work

In recent years, FATF has focused its attention on applying its standards to virtual assets (VAs) and virtual assets service providers (VASPs). For example, in February 2012, FATF revised its *Recommendations* to introduce *Recommendation 15* on "New Technologies." *Recommendation 15* was intended to address the AML/CFT risks introduced by new products, businesses, and technologies. More recently, in June 2019, the FATF adopted an *Interpretive Note to Recommendation 15* (INR. 15) to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the Risk Based Approach (RBA) to VA activities or operations and VASPs; supervision or monitoring of VASPs for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes; licensing or registration; preventive measures, such as customer due diligence (CDD), record-keeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation. The FATF adopted this *Guidance* at its June 2019 Plenary. Figure 2 presents a synopsis of the FATF's work on VAs.

Figure 2: Synopsis of the FATF's Work on VAs

June 2014	June 2015	October 2018	June 2019	July 2020
• The FATF issued Virtual Currencies: Key Definitions and Potential AML/CFT Risks in response to the emergence of virtual currencies and their associated payment mechanism.	• The FATF issued the Guidance for a Risk-Based Approach to Virtual Currencies as part of a staged approach to addressing the ML/FT risks associated with virtual currency payment products and services.	• The FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets, and also added two new definitions to the Glossary, "virtual asset" (VA) and "virtual asset service provider" (VASP). The amended FATF Recommendations 15 requires that VASPs be regulated for AML/CFT purposes, licenced or registered, and subject to effective systems for monitoring supervision.	• The FATF adopted an Interpretive Note to Recommendation to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities and VASPs; supervision or monitoring of VASPs; licensing or registration; preventive measures, such as customer due diligence, record-keeping, and suspicious transaction reporting; sanctions and other enforcement measures; and international cooperation.	• Twelve-Month Review of Revised FATF Standards on Virtual Assets and VASPs FATF report that sets out the findings of a review of the implementation of its revised standards 12 months after finalization of these amendments. The report found that while progress has been made, there are gaps in global implementation of the FATF standards, especially among countries in the FATF's global network.

In March 2020, the FATF released its *Guidance on Digital ID* to assist in identifying customers in the digital context, which includes useful information for VASPs. In June 2020, the FATF completed its *12-Month Review of the Revised FATF Standards on VAs and VASPs*, which identified areas where greater FATF guidance was necessary to clarify the application of the revised FATF *Standards*. Simultaneously with this report, the FATF also released its *Report to G20 on So-called Stablecoins*. This report sets out how the revised FATF *Standards* apply to so-called stablecoins and considers the AML/CFT issues.

In September 2020, the FATF also released a report on *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (ML/TF) for use by the public and private sectors. In March 2021, the FATF released its *Guidance on a Risk-Based Approach to AML/CFT Supervision*. While this report addresses AML/CFT supervision broadly, it includes a compendium of information for the AML/CFT supervision of VASPs specifically.

In July 2021, the FATF released its *Second 12-Month Review of the Revised FATF Standards on VAs and VASPs*. This report found that jurisdictions had continued to make progress in implementing the revised FATF *Standards*, but gaps in implementation mean that there is not yet a global regime to prevent the misuse of VAs and VASPs for ML/TF. The report also includes market metrics relating to P2P transactions, which are transactions that do not involve any obliged entity, and notes that the lack of implementation of the travel rule[6] by jurisdictions is acting as a disincentive to the private sector to invest in travel rule solutions. The report concludes that the updated *Guidance on VAs and VASPs* will provide necessary clarity on the application of the revised FATF *Standards* to aid implementation.

The FATF's *Updated Guidance*

The 12-month review report, G20 report, and second 12-month review report committed the FATF to release updated guidance for the public and private sector on the revised FATF *Standards* and their application to VAs and VASPs. In particular, these reports set out six main areas where greater guidance was sought. To address these six areas, this guidance was updated, and in October 2021, the FATF issued an *Updated Guidance for a Risk-based Approach to VAs and VASPs* which incorporates and supersedes its 2019 *Guidance*.

The FATF revisions focused on six key areas where greater guidance from the FATF was sought. These are to:

- clarify the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF *Standards* (either as a VA or as another financial asset),
- provide guidance on how the FATF *Standards* apply to stablecoins and clarify that a range of entities involved in stablecoin arrangements could qualify as VASPs under the FATF *Standards*,
- provide additional guidance on the risks and the tools available to countries to address the ML/TF risks for peer-to-peer transactions, which are transactions that do not involve any obliged entities,
- provide updated guidance on the licensing and registration of VASPs,
- provide additional guidance for the public and private sectors on the implementation of the 'travel rule', and
- include *Principles of Information-Sharing and Co-operation Amongst VASP Supervisors*.

6. The FATF Recommendation 16 commonly referred to as the Travel Rule, was originally made to help anti-money laundering (AML) and counter terrorist financing (CTF) efforts when it comes to wire transfers. In June 2019, the Financial Action Task Force (FATF) made an amendment to this Recommendation to include virtual assets and virtual assets service providers. Under this Recommendation, VAs and VASPs must comply with the requirements of Recommendation 16 (i.e., the 'travel rule'). This includes the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer.

For the purposes of this paper, we will focus primarily on the FATF *Updated Guidance* specifically relating to stablecoins. More specifically, stablecoins have proliferated during the pandemic. Their potential to reduce the volatility typical of bitcoins could encourage their widespread use, FATF said. Issuers of stablecoins should assess the risks of new products and launch measures such as limiting anonymous transactions or using software to monitor suspicious activity. The FATF reaffirms statements in its G20 report that a stablecoin is covered by the standards as either a VA or a financial asset (e.g., a security) according to the same criteria used for any other kind of digital asset, depending on its exact nature and the regulatory regime in a country.

The rest of this paper is organized as follows: (i) non-fungible tokens (NFT), (ii) decentralised finance (DeFi), (iii) software applications, (iv) stablecoins, (v) stablecoin risk assessment framework, and (vi) conclusions.

Non-fungible tokens

In its update, the FATF noted that digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as non-fungible tokens (NFTs) or crypto-collectibles. Depending on the features of assets known as NFTs, the FATF noted that generally these assets are not considered to be VAs under the FATF definition.

Coming back to the issue of classification, it is imperative to explore the nature and function of NFTs in order to make a final determination. This is because the FATF *Standards* may cover them, regardless of the terminology or marketing terms that are used. The FATF recognizes the multifaceted nature and complexity of VAs and VASPs, and consequently, on the initial surface some NFTs may not appear to constitute VAs. However, on deeper examination such NFTs may reveal that they fall under the VA definition. This may be the case if they are to be used for payment or investment purposes in practice.

In cases where NFTs are being used as digital representations of other financial assets already covered by the global AML/CFT standards, they are excluded from the FATF definition of VA. The reason provided in the update is that such NFTs would be covered by the FATF *Standards* similar to the type of financial asset represented. In this regard, the functional approach is particularly relevant based on the rapidly evolving space of VAs and other similar digital assets including NFTs. Countries should therefore consider the application of the FATF Standards to NFTs on a case-by-case basis.

Decentralised Finance

The FATF recognises the rapid pace of digitalization and innovations which has been accelerated by the global COVID-19 pandemic and the widespread significant use of advanced technologies, including decentralized finance (DeFi). The FATF notes that exchange or transfer services may also occur through technology commonly referred to as decentralized exchanges or platforms. A “decentralized or distributed application (DApp),” for example, is a term that refers to a software program that operates on a blockchain or similar technology. Consequently, the FATF noted that DApps are often used to facilitate or support other protocols, applications, or digital assets and their transfer. Although distributed ledger technologies are used to run these applications or platforms, they very often still have a central party.

The central party’s involvement or control may be related to creating and launching a VA, developing DApp functions and user interfaces for accounts holding an administrative “key,” or collecting fees. Often, a DApp could be programmed to require a user to pay a fee to interact with the DApp which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community. DApps can facilitate or conduct the exchange or transfer of VAs. Where these DApps offer financial services, such as those offered by VASPs, the term DeFi is commonly used.

A DeFi application (i.e., the software program) is not a VASP under the FATF *Standards*, as the *Standards* do not apply to underlying software or technology. The critical issue when considering DeFi is to examine very closely if any of the parties involved falls within the FATF definition of a VASP where they are providing or actively facilitating VASP services. It is crucial to determine whether or not the DeFi arrangements are centralized or decentralized. This is important because the creators, owners and operators or some other persons may maintain control or sufficient influence in the DeFi arrangements, and this could present ML/TF risks. This is the case, even if other parties play a role in the service or portions of the process are automated. Owners/operators can often be distinguished by their relationship to the activities being undertaken.

There may be other factors worth considering when looking at DeFi, for example jurisdictions may wish to consider whether any party profits from the service or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement. However, these are not the only characteristics that may classify the owner/operator as a VASP, but they are illustrative. Depending on its operation, there may also be additional VASPs that interact with a DeFi arrangement.

The FATF provides the following example: there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols.

Due to the global presence of the many open-source projects and developmental contributors in this space, DeFi projects are rapidly expanding in their number and capabilities. From this point of view, DeFI arrangements must be examined and evaluated closely on a case-by-case basis to understand the nature and scope of such arrangements, and identifying the parties involved. This will be necessary in order to make a reasonable determination whether there is an identifiable person(s), whether legal or natural, that is conducting a service covered by the FATF *Standards*. The point is that being marketed or self-identified as a DeFi is not determinative if its owner or operator is classified as a VASP. Neither is the specific technology involved a determinant factor.

As one examines the FATF update, it should be apparent that the responsibilities, scope and tasks for oversight with respect to DeFi is enormously complex. In the case of DeFi, jurisdictions are required to interpret and apply the definitions of the global AML/CFT standards and guidance broadly. From this point of view, it would be prudent to consider the practical intent of the functional approach. It is a relatively common practice for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence. In this regard, given the levels of scams, frauds and nefarious activities that have already taken place in the nascent DeFi space, countries should apply the VASP definition without respect to self-description or self-identification as a DeFi.

One of the most fundamental principles of the FATF *Standards* is the requirement to identify the natural or legal persons who conduct the financial services covered in the definition as a business. In the case of DeFi, if they meet the definition of VASPs, owners/operators should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to manage and mitigate these risks in an ongoing and forward-looking manner. In cases where a person can purchase governance tokens of a VASP, the VASP should retain the responsibility for satisfying AML/CFT obligations. An individual token holder in such a scenario does not have such responsibility if the holder does not exercise control or sufficient influence over the VASP activities undertaken as a business on behalf of others.

What happens if you are unable to identify a legal or natural person in a DeFi arrangement? In some situations, it might not be possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement. In other words, there may not be a central owner/operator that meets the definition of a VASP.

Here the key risk management strategy that jurisdictions should take is to monitor for the emergence of risks posed by such DeFi services and arrangements. This could involve monitoring the DeFi arrangement 's interaction and engagement within the VAs and DeFi ecosystem, and where appropriate, take risk mitigating actions. Ideally, it would be much better if countries could take risk-mitigating actions before the launch of the DeFi service. However, risk control measures can also be implemented during the course of the DeFi services being offered, as necessary. As an example, where no VASP is identified, a jurisdiction may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement in line with the country 's RBA or other mitigants. This is similar to the approach very often used for non-bank entities such as FinTechs, Payment Systems Service Providers, mobile-money and e-wallet providers, and Money Services Businesses (MSBs). In addition to this requirement, national authorities may also consider the ML/TF risks and potential mitigating actions in relation to P2P transactions when doing their risk assessments of DeFi.

Software Applications

As mentioned above, a person that creates or sells a software application or a VA platform (i.e., a software developer) may not constitute a VASP, when solely creating or selling the application or platform. However, when the application or platform is used to engage in VASP functions, as a business on behalf of others, this fact changes the determination.

It is also likely that when a software or platform is being developed with the intention to provide VASP services as a business for or on behalf of another person, one or more of the parties involved also qualifies as a VASP. The key here is to make the determination on the reason and purpose behind the software or application and to identify if there are any parties that retain control or sufficient influence over the assets, software, protocol, or platform or any ongoing business relationship with users of the software. It is important to note that such control or influence might be exercised through a smart contract, and thus will also encompass the FATF's definitions of VASP, requiring the compliance with the relevant AML/CFT obligations. As such, they should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to mitigate the risks in an ongoing and forward-looking manner.

One of the areas of ongoing discussion is the use of cloud services providers in banking and financial services. A frequent question is what is the nexus, if any, of regulatory requirements and obligations? In banking regulations, these are typically covered under third party services agreements. The FATF, in its consideration of ancillary services or products to a VA network, notes that it does not seek to regulate as VASPs natural or legal persons in such cases. The provisions of ancillary services may include hardware wallet manufacturers or providers of unhosted wallets. However, if an unhosted wallet provider performs virtual asset activities or operations for or on behalf of another person, it would likely qualify as a VASP and falls within the global AML/CFT standards. By way of definition, a hosted stablecoin wallet is a digital account hosted by a third-party financial institution, which does "know your customer " (KYC) on all of its customers; for example, one's balances of Tether or USD Coin held on an exchange like Coinbase. An unhosted one is controlled by the consumer. An unhosted stablecoin wallet exists when a user self-custody their stablecoin balances. For the most part, stablecoins currently make no effort to identify un-hosted users.

Likewise, natural or legal persons that solely engage in the operation of a VA network and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers (e.g., offering internet network services and infrastructure, offering computing resources such as cloud services and creating, validating, and broadcasting blocks of transactions) are not VASPs under the FATF *Standards*, even if they conduct those activities as a business.

Stablecoins

The main functions performed by a stablecoin arrangement are: (1) creation and redemption of the stablecoin, (2) its transfer between parties, and (3) storage of the stablecoin by users. As is quite common in the VA and VASP space, there are multiple entities involved in any stablecoin arrangement performing a range of different activities. The entities involved may be bank, government, non-bank, tech company, not-for-profit, consortium, etc. While there is some variation among stablecoin arrangements, the key functions are generally supported by the following activities[7]:

- Governance – Governance functions include defining and ensuring compliance with standards related to the purchasing, redeeming, holding, and transferring of stablecoins.
- Management of Reserve Assets – Stablecoin arrangements that are supported by reserve assets typically define the standards for the composition of those assets and purport to ensure a one-to- one ratio between reserve assets and the par value of stablecoins outstanding. Management of the reserve assets involves making investment decisions with respect to the reserve, including with respect to the riskiness of the assets.
- Custody of Reserve Assets – Stablecoins that are supported by reserve assets typically require a custodian or trust to acquire and hold the assets and execute transactions to facilitate management of reserve assets, in adherence with standards for reserve assets described above.
- Settlement – Transfers of digital assets such as stablecoins on a distributed ledger require other parties to process stablecoin transactions (e.g., to engage in authentication and validation) and, for on-chain transactions, to update the ledger in accordance with the underlying protocol.
- Distribution – Distribution of the stablecoin to users, such as consumers and businesses, involves providing access channels and other services that allow users to obtain, hold, and transact in the stablecoin.

These activities may be conducted by one or more parties and may be highly distributed and complex. Stablecoins may have a central developer or governance body consisting of one or more natural or legal persons. These persons are responsible for setting the rules governing the stablecoin arrangement. They will help to establish and determine the functions of the stablecoin, access rules and risk management including whether/how AML/CFT preventive measures are built into the arrangement.

They may also be actively involved in management of the stablecoin arrangement, or they may also have the power to delegate authority with respect to the management of the arrangement. This may include basic operational function such as managing the stabilization function. They may also manage the integration of the stablecoin into telecommunications platforms or promote adherence to common rules across the stablecoin arrangement.

Undoubtedly, in cases where a central governance body exists in a stablecoin arrangement, they will, in general, be covered by the FATF Standards either as a financial institution (FI) or a VASP. This is very important especially in cases where the governance body is deeply involved in the management and operational functions in the stablecoin arrangement. Such a body should therefore undertake ML/TF risk assessments prior to the launch or use of the stablecoin and take appropriate measures to manage and mitigate risks across the arrangement before launch. However, not all stablecoins may have a readily identified central body which is a VASP or a FI.

7. U.S. Treasury Department's Press Release President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins, Nov. 1, 2021

A stablecoin arrangement might have an entity driving the development and pre-launch efforts before its release. Here the key is to determine if this entity is a business and carries out VASP functions. In such a situation, this arrangement would create the nexus and scope for regulatory or supervisory action during the pre-launch phase.

If there is not a clearly identifiable VASP or FI, the risk management strategy should carefully consider the risks that a given stablecoin poses and the need for mitigation measures. The risk mitigation strategies could be like those used for P2P transactions. Additionally, this point is not meant to apply to those only developing software code, but rather to the persons involved in stablecoin arrangements that conduct or provide financial services covered by the tenets of the VASP definition. A range of other entities in the stablecoin arrangement may also have AML/CFT obligations, such as exchanges or custodial wallet services. It is important to note that the exact details of any arrangement must receive independent scrutiny to make these determinations.

From an ML/TF risk point of view, it is important to assess the risk of stablecoins on an ongoing and forward-looking manner especially given their potential for mass-adoption and use for P2P transactions. VASPs and other obliged entities should assess the ML/TF risk when they are developing new products before bringing them to market. Risk mitigation measures should be implemented before launching. Potential mitigation measures may include, for example, restricting the scope of users' ability to transact anonymously and controlling access privileges. Other risk mitigating measure could include the use of advanced technologies such as machine learning and artificial intelligence to control whether/how AML/CFT preventive measures are built into the arrangement. These new technologies could also be used in ensuring that AML/CFT obligations of obliged entities within the arrangement are fulfilled. For example, software could be used to monitor transactions and detect suspicious activity. Supervisors should look for these mitigation measures to be in place and on an ongoing basis before granting registration/licensing. It will be more difficult to mitigate risks of these products once they are launched.

icensing or registration process of a VASP or other obliged entity that is proposing to create or use a stablecoin, it is imperative that an assessment of the ML/TF risks and mitigation of the risks form part of the approval process. The key is for supervisors to determine and identify any VASP or other obliged entity involved with the stablecoin arrangement, especially when being told by the applicant that no entity qualifies based on the FAFT Standard. As noted above, during the pre-launch phase, it is unlikely that the process of creating and developing an asset for launch is purely automated. The potential for mass adoption should be included as an important factor meriting consideration in the licensing or registration procedure and risk assessment for all VASPs. As a general rule, the licensing or registration procedure for VASPs and obliged entities launching, or involved in, stablecoins should be similar to that of other VAs.

VASPs or FIs involved in stablecoins should be supervised in the same manner as VAs or financial assets as appropriate. Like other VAs, assessment of their risks should form part of this process, and stablecoins may pose higher or lower ML/TF risks, according to the judgement of supervisors, with attendant consequences for the type and intensity of supervision. If a given stablecoin qualifies as a financial asset, it should be supervised according to that determination in the same manner as all other similarly categorized assets. Given the cross-border nature of VA transfers, international co-operation of VASP supervisors is very important in this context.

Beyond the ML/TF risk concerns addressed by the recent FATF Update, the President's Working Group on Financial Markets (PWG) made a number of key recommendations to the U.S. Congress to address the prudential risks of payment stablecoins. The PWG recommended that Congress **promptly enact legislation to ensure that payment stablecoins and payment stablecoin arrangements are subject to a federal prudential framework on a consistent and comprehensive basis**. Because payment stablecoins are an emerging and rapidly developing type of financial instrument, legislation should provide regulators flexibility to respond to future developments and adequately address risks across a variety of organizational structures. Such legislation would complement existing authorities

with respect to market integrity, investor protection and illicit finance, and would address key prudential concerns:

1. **To address risks to stablecoin users and guard against stablecoin runs**, legislation should require stablecoin issuers to be insured depository institutions, which are subject to appropriate supervision and regulation, at the depository institution and the holding company level.

2. **To address concerns about payment system risk**, in addition to the requirements for stablecoin issuers, legislation should require custodial wallet providers**4** to be subject to appropriate federal oversight. Congress should also provide the federal supervisor of a stablecoin issuer with the authority to require any entity that performs activities that are critical to the functioning of the stablecoin arrangement to meet appropriate risk-management standards.

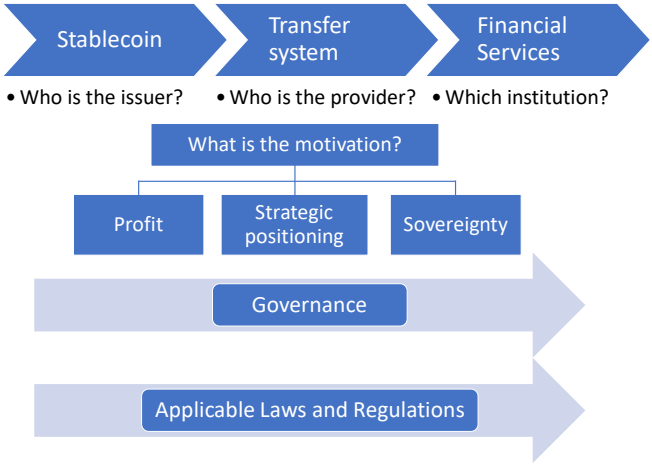
3. To address additional concerns about **systemic risk and concentration of economic power**, legislation should require stablecoin issuers to comply with activities restrictions that limit affiliation with commercial entities. Supervisors should have authority to implement standards to promote interoperability among stablecoins. In addition, Congress may wish to consider other standards for custodial wallet providers, such as limits on affiliation with commercial entities or on use of users' transaction data.

Stablecoin Risk Assessment Framework

As noted above, there are multiple entities involved in any stablecoin arrangement, and in the absence of a universal risk assessment framework it is extremely difficult to evaluate and identify the potential for and gaps of stablecoin arrangements. Against this background, we develop a proposed stablecoin risk assessment framework. However, we acknowledge that risks associated with stablecoins go well beyond ML/TF and fraud risks addressed by the FATF Update, and consequently we believe a more comprehensive framework will be needed.

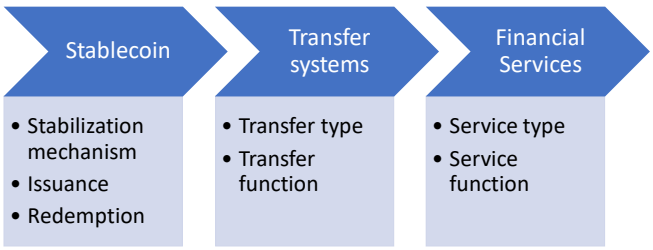
Based on our understanding of the FATF *Guidance* we start our assessment by understanding (1) the stablecoin structure and arrangements; (ii) transfer systems; and (iii) the related financial services. Our key objective is to understand the risks of stablecoins to ensure AML/CFT compliance. In the first stage, we want to understand the key parties involved, the motivation, the governance arrangements, and if any, applicable laws and regulations (Figure 3). Some of the key questions are: who is the issuer? Who is provider the transfer system; and which financial institutions and products are involved?

Figure 3



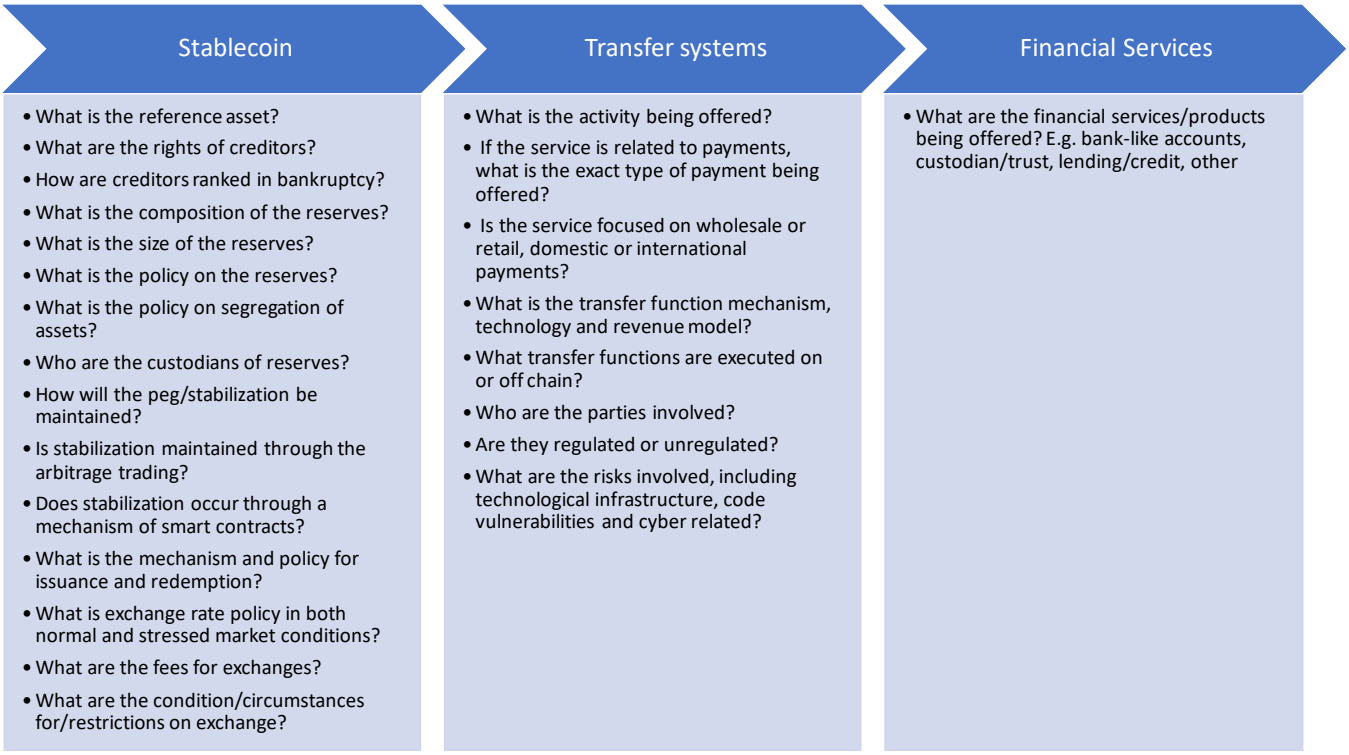
In the next stage, we look closer at the stabilization mechanism, issuance and redemption, the transfer and financial services type as well as the transfer and financial services function (Figure 4).

Figure 4



Finally, we develop some of the key questions that should be answered when evaluating stablecoin arrangements (Figure 5).

Figure 5



In developing the stablecoin risk assessment framework our overarching principle is the idea of "same business, same risks, equivalent rules" given that there may be different risks depending on the technological choices and service providers.

Conclusion

The emergence of a clear regulatory framework in the nascent virtual assets space is hampered by the lack of common classification. One of area in which we are beginning to see the emergence of greater clarity is stablecoins. Perhaps this is because stablecoin digital currencies have the potential for mass adoption. On the one hand, this could be beneficial for financial inclusion and enhance cross border payments. One the other hand, this raises alarms for financial stability risks as well as concerns about its potential use to launder money or fund terrorism.

An examination of the FATF update revealed that the responsibilities, scope and tasks for oversight with respect to stablecoins and other emerging technologies such as NFTs, DeFi and software applications are enormously complex. For example, terminology or marketing terms or self-identifying as an NFT or DeFi is not a sufficient condition for whether AML/CFT rules are applicable.

A key feature of the FATF's requirements is understanding (i) the purpose, nature and scope of the stablecoins and other nascent emerging technologies, (ii) the roles, responsibilities and functions of central parties, and (iii) nexus to other VAs, VASPs as well as banking and payment services. Clearly, stablecoins and other emerging technologies are fast evolving and transforming, and as such we can expect further clarifications from the FATF and other standard setting bodies in the future.

REFERENCES

Garcia, A, Lands, B and Yanchus, D (2021), "Stablecoin Assessment Framework," Bank of Canada Staff Discussion Paper 2021-6.

Financial Action Task Force (FATF), "Updated Guidance for a Risk-Based Approach (RBA) for Virtual Assets (VAs) and Virtual Assets Service Providers (VASPs)," October 2021.

Financial Stability Board (2020), "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements – Final Report and High-Level Recommendations," 13 October.

President's Working Group on Financial Markets (2021), "Report and Recommendations on Stablecoins," U.S. Treasury Department Press Release, 1 November.

Rosengreen, E (2021), "5 takeaways from Boston Fed President Eric Rosengren's 25 June 2021, remarks to the Official Monetary and Financial Institutions Forum (OMFIF)," Federal Reserve Bank of Boston.

ANNEX

Determining Factors, Risk Assessment Actions Requirements and Suggested Questions

	Determining factors	Risk Assessment Actions Required	Key Question(s)
Non-fungible tokens (NFT)	Generally, not considered to be VAs under the FATF definition. Self-identifying or terminology or marketing terms are not indicative of qualifying as VAs.	Treat on a case-by-case basis. Look for connection to VAs or VASPs, payments, banking, securities, investments, etc.	Is NFT a digital representations of other financial assets already covered by the global AML/CFT standards? If yes, excluded from the FATF definition of VA. NFTs would be covered by the FATF *Standards* similar to the type of financial asset represented.
Decentralized Finance (DeFi)	DApps and DeFi applications (i.e., the software program) do not qualify as VASPs Level of central party involvement or control. Central parties such as creators, owners, and operators who control or maintain influence in the arrangement of DApps and DeFi applications may fall under the definition of VASP Being marketed or self-identified as a DeFi is not determinative if its owner or operator is classified as a VASP.	Whether centralized or decentralized, examine and identify the central party, legal or natural person who can exercise control or sufficient influence of DeFi. Determine whether DApp is/can be programmed to require a user to pay a fee to interact with the DApp which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/ community. Look for other VASPs that interact with a DeFi arrangement. Examined and evaluated closely on a case-by-case basis to understand the nature and scope of such arrangements, and identifying the parties involved. Owners/operators of DeFi, that meet the definition of VASPs, should undertake ML/TF risk assessments prior to the launch or use of the software or platform Take appropriate measures to manage and mitigate risks on an ongoing and forward-looking manner. In cases where a person can purchase governance tokens of a VASP, the VASP should retain the responsibility for satisfying AML/CFT obligations.	Is there a central party? If yes, what is the role of the central party? Does any of the parties involved falls within the FATF definition of a VASP? where they are providing or actively facilitating VASP services? Is any party profiting from the services? Does any party have the ability to set or change parameters to identify the owner/operator? Does the individual token holder exercise control or sufficient influence over the VASP activities undertaken as a business on behalf of others?

	Determining factors	Risk Assessment Actions Required	Key Question(s)
Software Applications	A person that creates or sells a software application or a VA platform (i.e., a software developer) may not constitute a VASP, when solely creating or selling the application or platform. When the application or platform is being developed or used to engage in VASP services as a business for or on behalf of another person, one or more of the parties involved qualifies as a VASP. Central party, legal or natural, who exercise control or influence will meet the FATF's definitions of VASP, are required to comply with the relevant AML/CFT obligations. The definition of VASP does not cover natural or legal persons providing ancillary services or products (e.g. developers or providers of unhosted wallets) to a VA network.	Examine and determine the reason and purpose behind the software or application Identify if there are any parties that retain control or sufficient influence over the assets, software, protocol, or platform or any ongoing business relationship with users of the software. This includes through the use of a smart contract They should undertake ML/TF risk assessments prior to the launch or use of the software or platform Take appropriate measures to mitigate the risks in an ongoing and forward-looking manner. However, if an unhosted wallet provider performs virtual asset activities or operations for or on behalf of another person, it would likely qualify as a VASP. Are there natural or legal persons that engage in or facilitate any of the activities or operations of a VASP on behalf of their customers?	What is the reason and purpose behind the software or application? Is the application or platform being developed or used to engage in VASP services? Who are the central parties? Are there natural or legal persons providing ancillary services or products (e.g. developers or providers of unhosted wallets)? If yes, are there natural or legal persons that engage in or facilitate any of the activities or operations of a VASP on behalf of their customers?
Stablecoins	Central governance body or developer of a stablecoin arrangement, will likely be covered by the FATF Standards either as a financial institution (FI) or a VASP. A governance body that is deeply involved in the management and operational functions in the stablecoin arrangement will be covered as a FI or VASP.	Determine and examine the nature and scope of a stablecoin arrangement prior to its launch or use. Determine and identify the central governance body. Determine and examine the role of the central governance body. During the development and pre-launch stage, determine if the entities involve is a business and carries out VASP functions.	What is the reason and purpose behind the stablecoin arrangement? Is there a central governance party? If yes, identify the central party, what is its role, responsibilities and functions? If no, determine if any of the any of the entities involved during the development or pre-launch stage is a business and carries out VASP services?

The SEACEN Centre

Since its inception in the early 1980's, The South East Asian Central Banks Research and Training Centre (the SEACEN Centre) has established its unique regional position in serving its membership of central banks in the Asia-Pacific region through its learning programmes in key central banking areas (including Macroeconomic and Monetary Policy Management; Financial Stability and Supervision, and Payment and Settlement System; and Leadership and Governance), research work, and networking and collaboration platforms for capability building in central banking knowledge.

The SEACEN Centre

The South East Asian Central Banks (SEACEN) Research and Training Centre