FATF Report

Targeted Report on Regulatory Challenges from Decentralised Finance (DeFi)

July 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2026), *Targeted Report on Regulatory Challenges from Decentralised Finance, Paris, France*, *https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/targeted-report-decentralised-finance-2026.html*

© 2026 FATF/OECD. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France or e-mail: contact@fatf-gafi.org

Photo credits cover photo ©Shutterstock

Table of Contents

Executive summary **2**

1. Understanding the landscape **3**
1.1. Introduction 3
1.2. Scope of the report 7

2. Characteristics and vulnerabilities of DeFi arrangements **7**
2.1. Characteristics of DeFi arrangements 7
2.2. Vulnerabilities and barriers to effective AML/CFT/CPF supervision 9

3. Status of implementation of the FATF Standards **10**
3.1 The applicable framework 10
3.2. Jurisdictions' implementation of Recommendation 15 to DeFi Arrangements 13

4. Financial crime risks and typologies associated with DeFi arrangements **15**
4.1. Threat actors, risks and typologies 15

5. Good Practices in Implementing R.15 to DeFi arrangements **18**
5.1. Effective risk assessment of DeFi arrangements 18
5.2. Defining controllers of DeFi arrangements 19
5.3. Considerations to determine control in DeFi arrangements 21
5.4. Assessment of control over DeFi arrangements 24
5.5. Truly decentralised DeFi arrangements 26
5.6. Licensing and/or registration requirements for Centralised DeFi arrangements 27
5.7. Supervisory practices 30
5.8. Interaction between DeFi arrangements and regulated financial institutions and VASPs 32

6. Enforcement and other actions to mitigate risks associated with DeFi arrangements **36**
6.1. Use of blockchain analytics tools in DeFi-related investigations 36
6.2. Co-ordination with other competent authorities 37
6.3. Freezing and recovery of illicit funds 37

7. International co-operation **39**
7.1. Cross-border information sharing 39
7.2. Cross-border investigations 40
7.3. Public-private co-operation 41

Conclusion **42**
Recommendations to mitigate the risk stemming from DeFi arrangements 43
1.1. For jurisdictions 43
1.2. For the private sector 45

© FATF-OECD 2026

Executive Summary

1. DeFi has expanded rapidly since the publication of the FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers in 2021. While still a relatively small share of the broader virtual asset market, its growth, combined with increasing participation by institutional investors, VASPs, and other regulated entities, has heightened its relevance within the global financial system and its potential exposure to money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks.
2. The DeFi ecosystem offers distinct advantages for the development of the global financial sector. However, DeFi's unique features, such as pseudonymity, permissionless access, smart contract automation, composability and cross-border reach, also create structural vulnerabilities that can facilitate rapid, complex and opaque financial transactions. The report finds that these characteristics are increasingly exploited by a range of illicit actors, including fraudsters, ransomware operators, professional money laundering networks and proliferation financing actors. Illicit activity often involves sophisticated techniques such as chain-hopping, cross-chain bridges, decentralised exchanges, mixers and governance manipulation, enabling the layering and co-mingling of illicit funds within legitimate financial flows. These risks are amplified in environments where AML/CFT controls are absent or insufficiently implemented.
3. The FATF Standards are technology neutral and apply whenever a natural or legal person provides financial services. The 2021 FATF Guidance clarifies that DeFi arrangements fall within the scope of Recommendation 15 where a natural or legal person exercises control or sufficient influence over the arrangement.
4. In practice, however, jurisdictions in the FATF Global Network still struggle to identify and regulate DeFi arrangements operating in their territory, due to their cross-border nature, unclear jurisdictional anchors, limited supervisory technical expertise, and challenges in distinguishing between DeFi arrangements' inherently decentralised technology and potentially centralised governance.
5. A key challenge lies in identifying "control or sufficient influence" within DeFi arrangements. Although many arrangements present themselves as decentralised in terms of governance, this report finds that centralised elements frequently persist in practice, including through governance token concentration, administrative privileges, control over upgrades, significant economic benefits, and influence over development and infrastructure. The report identifies a non-exhaustive set of on-chain and off-chain indicators that can support jurisdictions in determining whether such control exists.
6. Based on governance and control structures, the report distinguishes three broad categories of DeFi arrangements: (i) those with identifiable controllers ("centralised"); (ii) those that are centralised in practice but where controllers cannot be readily identified; and (iii) those that are truly decentralised. The FATF Standards apply to the first two categories. While truly decentralised arrangements fall outside the scope of the Standards, as the latter cannot be readily applied to them, such arrangements still present significant risks that require alternative, risk-based mitigation measures.
7. The report highlights that effective implementation of the FATF Standards in the context of DeFi requires a functional and risk-based approach. A number of

© FATF-OECD 2026

recommendations are made to help jurisdictions regulate and supervise DeFi arrangements, including to determine the existence of control. Recommendations are also made to DeFi arrangements, as well as Financial Institutions/VASPs interacting with them, to mitigate the risk of criminal abuse.

1. Understanding the landscape

1.1. Introduction

1. Decentralised Finance (DeFi) has experienced significant growth in recent years, with total value locked (TVL)[1] reaching USD 86.644 billion in 2026, an increase of approximately 85% compared to 2023.[2] Despite its relatively small share of the estimated total virtual asset market capitalisation[3], DeFi represents a growing vulnerability within the AML/CFT/CPF regime due to its distinct characteristics and increasing misuse by illicit actors.[4] Moreover, institutional investors, virtual asset service providers (VASPs) and other regulated entities are increasingly placing financial resources in DeFi arrangements, drawn by high returns and the advantages offered by the blockchain technology used in DeFi applications, such as cross-border payments, transaction transparency, and easy access to global customers.
2. These trends significantly amplify the risk that DeFi may be misused to co-mingle illicit funds with legitimate assets, thereby undermining the benefits of its innovative approach to finance. In light of these rapid developments, this report examines the financial crime risks associated with DeFi and clarifies in what circumstances the FATF Standards apply to certain DeFi arrangements. Throughout this report, the FATF adopts the following definitions:
    - *DeFi* refers to the technology and services delivered through blockchain-based smart contracts. A *DeFi arrangement*, in contrast, encompasses the broader ecosystem, including the persons, governance structures, and operational components that enable these services to function.
    - The term "*person*", particularly in the context of controllers of a DeFi arrangement, includes individuals, as well as partnerships, foundations, and other forms of legal persons or arrangements.
3. The DeFi ecosystem offers distinct advantages for the development of the global financial sector. The participation of new developers and other actors fosters financial innovation and provides a valuable testing ground for innovative

[1] Total Value Locked (TVL) is a key metric used in decentralised finance (DeFi) to measure the total amount of assets deposited in a DeFi protocol. It reflects how much value users have committed to activities such as lending, staking, liquidity provision, or other smart-contract-based services. However, TVL is not a comprehensive indicator of a protocol's footprint or associated risks; for example, decentralised exchanges (DEXs) typically hold relatively low levels of locked assets while generating significant trading volumes.

[2] According to DeFiLlama, TVL stood at USD 86.644 billion as of 10 May 2026, compared with USD 46.86 billion on 10 May 2023. https://defillama.com/

[3] Estimates indicate that around 4-6% of the virtual asset market is associated with DeFi https://www.coingecko.com/en/charts

[4] https://academic.oup.com/cybersecurity/article/11/1/tyae029/7962044 ; https://www.chainalysis.com/reports/crypto-crime-2026/ ; https://www.crowdfundinsider.com/2026/05/276717-defi-hacks-report-april-2026-becomes-most-hacked-month-in-crypto-history-by-number-of-incidents/

© FATF-OECD 2026

blockchain-based technologies. Protecting the DeFi ecosystem from illicit abuse will allow customers to better leverage the benefits of these innovative financial services.

4. The FATF Standards are technologically neutral and apply equally to all providers of financial services. For DeFi arrangements, the FATF Standards apply whenever an identifiable person has control or sufficient influence over the arrangement. However, in practice, the DeFi sector remains largely unregulated, with many jurisdictions struggling to implement effective AML/CFT measures. This is, in part, due to some DeFi arrangements presenting themselves as truly decentralised when in fact they are controlled by identifiable persons. The key distinction is between the underlying technology, such as blockchain and smart contracts, that enables automated transactions without an intermediary and is inherent to all DeFi arrangements, and the governance frameworks of these arrangements, which may or may not be controlled or influenced by identifiable persons.

5. In 2019, the FATF updated R.15 and extended the application of the FATF Standards to Virtual Assets (VAs) and VASPs. A VASP is defined in the FATF Glossary as:[5] "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."

6. The FATF 2021 Guidance on VAs and VASPs[6] (hereafter the "Guidance") recognises the complexity of regulating VA activities and specifies when an individual or entity should be classified as a VASP, with a focus on the functions performed rather than the underlying technology. The Guidance urges jurisdictions to distinguish between the decentralised technical nature of the underlying DeFi protocol[7] and the centralised governance framework that may emerge through the control or influence exercised over the arrangement by certain persons, such as creators, software developers or investors. The Guidance further recommends that jurisdictions monitor emerging risks and actively engage with the DeFi community to understand and address potential ML/TF/PF threats. Countries are expected to conduct risk assessments of DeFi, as appropriate on the basis of risk and context, and take proportionate measures in line with R.1. Competent authorities should also issue guidance to financial institutions and VASPs on best practices when interacting with DeFi

[5] The FATF Recommendations, as amended October 2025

[6] Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers

[7] A *DeFi protocol* is the smart-contract code deployed on a blockchain that automatically executes specific financial functions, such as trading, lending, or liquidity provision, without requiring a central intermediary.

© FATF-OECD 2026

arrangements. Since the publication of the Guidance, the DeFi ecosystem has evolved, with different actors, including regulated entities, interacting with DeFi arrangements.

7. The FATF does not define the term "DeFi" in its Standards. This report distinguishes three types of DeFi arrangements based on their governance and control frameworks:
    - **Centralised:** The DeFi arrangement has identifiable controllers or persons exercising sufficient influence (e.g. administrators, governance token holders, developers, funders). Arrangements that present themselves as truly decentralised for marketing purposes may nonetheless be centralised in practice. Such arrangements fall within the scope of the FATF Standards, and should always be regulated.
    - **Centralised where controllers cannot be readily identified**: Control or sufficient influence over the DeFi arrangement exists but the person(s) exercising such control cannot be identified due to pseudonymity or other factors. Such arrangements fall within the scope of the FATF Standards and should be regulated. However, supervisory authorities may encounter practical challenges in enforcing regulatory measures. When regulations cannot be effectively applied, such arrangements should be treated, for practical purposes, as unregulated. In such cases, jurisdictions should apply the same mitigating measures used for truly decentralised arrangements.
    - **Truly decentralised**: No person maintains control or exercises sufficient influence over the DeFi arrangement. Such arrangements fall outside the scope of the FATF Standards and are generally unregulated.[8]
8. Countries should apply the FATF Standards by interpreting the relevant definitions broadly, while remaining mindful of the practical intent of the functional approach. In practice, in the context of DeFi, the FATF Standards apply to:
    i. Person(s) who maintain control or sufficient influence over a DeFi arrangement, even when the arrangement seems or markets itself as decentralised. The FATF Guidance clarifies that jurisdictions may consider different factors to determine control or sufficient influence, including whether someone profits from the DeFi arrangement or has the ability to set or change parameters in the protocol. Additional considerations relevant to assessing control and influence are set out in Section 5.3 of this report. 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.
        - As an example of such person(s), any person facilitating access to a DeFi arrangement (e.g., through front-end interfaces, platforms, applications, etc.) and actively facilitating the provision of

[8] A truly decentralised arrangement may choose to seek regulatory oversight on a voluntary basis in order to demonstrate stronger AML/CFT integrity and facilitate business with obliged entities.

© FATF-OECD 2026

financial services is included in the FATF definition of VASP.[9] This is particularly relevant when the underlying DeFi arrangement is unregulated for AML/CFT purposes.

ii. Any financial institution or VASP interacting with DeFi arrangements should be required to undertake a risk assessment of the products offered by the DeFi arrangement and take appropriate measures to manage and mitigate identified risks, in line with R. 15, first paragraph, on mitigating risks from new technologies.

- If the DeFi arrangement is regulated, financial institutions and VASPs should conduct CDD on the DeFi arrangement and a review of its AML/CFT framework, in line with the requirements of R.10 and R.13.
- If the DeFi arrangement is unregulated, financial institutions and VASPs should ensure that their interactions with the arrangement do not undermine the integrity of their own AML/CFT frameworks. This may include assessing the extent to which the DeFi arrangement effectively incorporates AML/CFT safeguards (e.g., embedded KYC/CDD solutions, use of KYC/CDD third party providers) and implementing appropriate risk-mitigating measures with respect to the arrangement's underlying users (e.g., CDD, use of real-time blockchain analytics monitoring tools).

9. The FATF allows jurisdictions discretion in determining the criteria used to assess whether a DeFi arrangement has a controller or persons exercising sufficient influence. However, many jurisdictions continue to face challenges in identifying and appropriately regulating DeFi arrangements due to several factors:

   i. The global reach of DeFi, combined with the absence of a clear jurisdictional anchor and, in many cases, the lack of a defined legal form, complicate regulation, supervisory oversight, and enforcement.

   ii. Marketing strategies and claims of "decentralisation" by certain DeFi arrangements, which may create the impression of absence of an obliged intermediary responsible for AML/CFT compliance.

   iii. Limited information and understanding of DeFi's technical, operational and governance structures, which reduces authorities' ability to accurately identify where control or sufficient influence exists.

   iv. Constraints on supervisory resources and technical expertise, which may limit authorities' capacity to identify, understand and monitor emerging DeFi protocols and associated AML/CFT solutions or tools.

[9] See Paragraph 59 of the FATF Guidance on VAs and VASPs: "Conducts" includes the provision and/or *active facilitation* of a service, which refers to active involvement in the provision of activities covered under limbs (i)-(v) of the VASP definition.https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

© FATF-OECD 2026

1.2. Scope of the report

10. The objective of this report is to:
    i. Identify emerging money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks and vulnerabilities within the DeFi ecosystem.
    ii. Clarify how the FATF Standards apply to DeFi arrangements and outline good practices and practical tools that jurisdictions may adopt to identify, regulate, supervise and investigate DeFi arrangements that fall within the scope of the FATF framework.
    iii. Present criteria that jurisdictions may use in a risk-based manner to identify controllers or persons exercising sufficient influence over DeFi arrangements.
    iv. Propose recommended actions for relevant stakeholders.
11. This report updates and complements the FATF's previous analysis of DeFi, as set out in the 2021 Guidance on VAs and VASPs, in light of the sector's substantial expansion and evolution since the publication of that guidance. This targeted report should be read alongside the FATF's broader guidance and work on VAs available on the FATF website and in Annex A.
12. This report is informed by research carried out in preparation for the FATF's 2026 7th Targeted Update on the Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers. References in this report to practices implemented in particular jurisdictions are provided by way of example only and should not be considered FATF-approved or an endorsement of the effectiveness of any jurisdiction's system. As with all FATF Targeted Reports, this guidance is non-binding. In addition, jurisdictions should do further work to fully understand how to test DeFi arrangements for control or sufficient influence in their own context.

2. Characteristics and vulnerabilities of DeFi arrangements

2.1. Characteristics of DeFi arrangements

13. DeFi generally refers to a range of financial services, such as trading, exchanging, lending, borrowing, and asset management, delivered through blockchain-based, self-executing smart contracts rather than traditional financial intermediaries. Users can maintain their funds in hosted or, more commonly, unhosted wallets and interact with DeFi protocols that programmatically enable the execution of complex peer-to-peer and peer-to-pool financial transactions. Users' interaction with a DeFi arrangement may be either direct, through a DeFi platform or underlying protocol, or indirect, through an obliged entity (e.g., a VASP).
14. DeFi arrangements share characteristics with the broader virtual asset ecosystem: they are blockchain or DLT-based, enable immediate cross-border

© FATF-OECD 2026

transfers, and record all transactions publicly, albeit usually on a pseudonymous basis.[10] They also have some unique features:

i. Smart contract-based automation of financial services: DeFi protocols rely on often publicly visible smart contracts to fully automate financial services and functions, which can complicate the attribution of control over the arrangement to a particular person.

ii. Open-source and composable protocol architecture: DeFi protocols are typically, though not always, developed as open-source software, allowing anyone to inspect, reuse and replicate the underlying code. This facilitates the rapid creation of similar DeFi protocols. While this interconnected design offers efficiencies for legitimate users, it may also be exploited by illicit actors to move funds at an unprecedented speed across multiple DeFi layers and related entities, including unregulated offshore VASPs and over-the-counter brokers. The speed of blockchain transactions, together with pseudonymous access and the ability to execute automated operations through smart contracts in rapid succession, constitutes a significant risk factor and may reduce the effectiveness of traditional supervisory and enforcement timelines.

iii. Algorithmic market and risk mechanisms: Some DeFi arrangements create market structures, such as automated market makers, liquidity pools, and lending mechanisms that algorithmically adjust interest rates and trigger automatic liquidations when collateral thresholds are breached often without the involvement of regulated intermediaries. These features enable complex layers of transactions that may be difficult to monitor using traditional compliance tools and blockchain analytics.

iv. User-driven liquidity provision and fee-earning: DeFi arrangements allow users to act as liquidity providers, earning fees proportionate to their share of liquidity pools while remaining pseudonymous. This feature can be exploited by illicit actors, who may deposit and co-mix illicit proceeds within large pools of legitimate liquidity and earn fees on those funds.[11]

v. Participation: Many DeFi arrangements allow anyone with a blockchain wallet to access and use financial services without undergoing customer due diligence. This frequently open, unrestricted access creates significant ML/TF/PF risks, as illicit actors can enter the ecosystem pseudonymously and take advantage of its complexity to launder funds.

[10] In this context, "pseudonymous" means that transactions are associated with unique digital identifiers rather than real-world identities, allowing activity to be publicly observable without directly revealing the identity of the parties involved. The identities of the parties to a transaction are therefore not known, unless the DeFi arrangement implements Customer Due Diligence (CDD), or the transaction involves a regulated VASP that may hold such information as part of its Compliance Programme. While most DeFi arrangements operate under a pseudonymous model, some smart contracts may be private or confidentiality-preserving and obscure key details such as transaction amounts, addresses, or contract logic, thereby preventing third parties from linking activity to specific users or even tracing transactions on-chain.

[11] https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, pages 18-19

© FATF-OECD 2026

vi. Reliance on oracles: DeFi arrangements may depend on oracles, which provide external data (e.g., asset prices, interest rates) to smart contracts. Oracles enable core functionalities of the DeFi ecosystem, including pricing, collateral valuation and liquidation mechanisms. However, weaknesses in oracle design, governance, or data feeds may be exploited by illicit actors to manipulate inputs and distort market conditions. Such manipulation may facilitate illicit activity, including fraudulent liquidations and the laundering of illicit proceeds.

2.2. Vulnerabilities and barriers to effective AML/CFT/CPF supervision

15. DeFi arrangements share several inherent vulnerabilities with the broader virtual asset ecosystem.[12] Some of their defining characteristics, particularly their borderless, open-source design and ability to enable complex financial operations create inherent risks. In addition to these intrinsic features, the DeFi ecosystem also displays structural vulnerabilities shaped by underlying technology, policy choices, governance frameworks, and the current stage of market development. These include:

    i. *Lack of regulatory framework:* Many jurisdictions in the FATF Global Network still do not implement R.15 with regards to DeFi arrangements that fall within the scope of the FATF Standards (see: Section 3.2). This allows illicit actors to take advantage of the uneven and often fragmented implementation of regulations at the global level (regulatory arbitrage) and weakens consumer protection.

    ii. *Lack of compliance by qualifying DeFi Arrangements*: DeFi arrangements that fall within the scope of the FATF Standards may fail to register with relevant competent authorities or to implement required AML/CFT measures, including targeted financial sanctions, KYC and CDD obligations. Many also lack mechanisms to cooperate with law enforcement authorities (LEAs) and supervisory authorities, thereby hindering investigative and supervisory efforts.

    iii. *Cyber vulnerabilities*: DeFi arrangements are exposed to significant cyber risks due to weaknesses in smart-contract security, uneven maturity of cybersecurity practices and the open-source nature of many protocols, which allows malicious actors to analyse code and identify exploitable flaws.[13] Arrangements that hold large volumes of assets are particularly attractive targets for hackers, increasing the potential impact of successful exploits.[14] The emergence of new

[12] https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html

[13] Some commentators argue that open-source software is more resilient and secure than closed-source software, on the basis that broader review and contribution, often by technically sophisticated users with diverse perspectives, increases the likelihood that vulnerabilities are identified and addressed. Risks associated with open-source software may be further mitigated by DeFi arrangements through measures such as smart contract audits, bug bounty programmes, and the engagement of white-hat hackers. Other commentators note that risks are evolving, and the advent of Frontier AI can exacerbate cyber vulnerabilities in DeFi arrangements also through the analysis of open-source software.

[14] For more information on cyber vulnerabilities in DeFi arrangements please consult https://www.fsb.org/uploads/P160223.pdf

© FATF-OECD 2026

technologies, including AI and quantum computing, may further increase these risks.

iv. *Shift towards payments without centralised on/off ramps*: As payment systems evolve, users may no longer need to convert virtual assets into fiat currency through regulated financial institutions or VASPs. They may also have reduced incentives to convert virtual assets into stablecoins or deposit tokens to facilitate payments. As a result, the mitigating effect of regulatory access points[15] for DeFi arrangements may weaken.

v. *Perimeter-based regulatory arbitrage*: While the FATF Standards require jurisdictions to identify DeFi arrangements that fall within their regulatory perimeter, jurisdictions maintain a level of flexibility in determining how this is assessed in practice. Differences in national approaches, while reflecting domestic policy choices based on risk and context, may enable globally distributed DeFi arrangements to locate activities in jurisdictions with less stringent or less clearly defined regulatory frameworks, thereby increasing the potential for regulatory arbitrage.

3. Status of implementation of the FATF Standards

3.1 The applicable framework

16. As a principle, the FATF Standards are technology neutral, and risk-based AML/CFT measures should be applied to services and activities that fall within their scope, irrespective of the technology used. Jurisdictions should be guided by the principle that the FATF framework applies to natural or legal persons who as a business conduct the financial services covered by the VASP definition. [16]

17. The DeFi ecosystem has evolved significantly since the publication of the FATF Guidance in 2021. It has progressed from primarily technical platforms aimed at broadening access to financial services to increasingly sophisticated arrangements that offer a wide range of financial products, generate revenues, and seek to scale their operations, including through the provision of services to regulated financial institutions. Growing investment by institutional investors in certain DeFi arrangements indicates that some of these arrangements are emerging as more substantial providers of financial services, similar in function to traditional financial institutions, albeit operating through blockchain-based infrastructure.

18. Jurisdictions should establish appropriate regulatory frameworks to ensure that persons who maintain control or sufficient influence over DeFi arrangements implement risk-based AML/CFT/CPF measures in line with the

[15] *Regulatory access points* refer to centralised intermediaries, such as regulated VASPs, that act as key control points through which users move funds into or out of the DeFi ecosystem. Because these entities or individuals are subject to AML/CFT requirements, they provide a critical opportunity for authorities to apply oversight, identify illicit actors, and disrupt financial crime.

[16] Paragraph 68, FATF VAs and VASPs guidance https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

© FATF-OECD 2026

FATF Standards by taking into account the indicators set out in Section 5.3. of this report, though relevant factors may vary depending on the specific characteristics of the arrangement.[17]

19. The DeFi ecosystem is typically described as a multi-layered architecture, where each layer builds on the one below it (also called the "DeFi stack"). The different layers have different levels of automatisation and decentralisation, and the FATF Standards may apply differently to each layer:

    i. Settlement Layer: Foundational distributed-ledger infrastructure (e.g., Ethereum, Solana, Hedera, etc.) that records transactions and provides security, consensus and final settlement for all transactions that occur in the higher application layer.

        - The FATF Standards generally do not apply to payment infrastructure, unless persons operating in this layer also provide services that fall within the FATF definition of VASP.

    ii. Asset Layer: includes the native tokens of blockchains (e.g., ETH, SOL, HBAR, etc.), which are integral to the operation and security of the blockchain, and other digital assets that are built or programmed and deployed to and run on a blockchain, including stablecoins. These assets represent units of value that can be traded, or otherwise used in financial transactions, occurring on or through DeFi protocols.

        - The FATF Standards apply to persons who provide digital asset services that fall within the FATF definition of VASP.[18]

    iii. Protocol Layer: includes smart contracts that encode financial logic, such as automated market makers (AMMs), lending/borrowing markets and liquidity pools. These protocols define how assets move, how prices are formed and what rules users must follow, and represent the "back-end" of the DeFi ecosystem.

        - The FATF Standards do not apply to smart contracts themselves, as they are automated and decentralised software. However, the FATF Standards apply to persons who exercise control or sufficient influence over the smart contracts.

    iv. Application Layer: includes front-end interfaces, such as websites and smartphone apps, dashboards, applications or wallets and other tools that make the underlying protocol providing DeFi services accessible to non-technical users. Most retail and institutional users of DeFi access services through this layer, though it is not required. The application layer may be managed separately from the protocol layer and have different controllers.

        - The FATF Standards apply to persons operating in the application layer to the extent they provide or facilitate the provision of VASP services.

[17] Further guidance on determining control is included in section 5 of this report (Good practices)

[18] https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html

© FATF-OECD 2026

v. Aggregation Layer: includes off-chain and/or on-chain protocols that enable numerous DeFi protocols to be combined in one convenient location at the application layer. Aggregators are intended to provide end users with an optimal path for lending assets, purchasing or selling assets, minting new assets, etc.[19]

- the FATF Standards apply to persons operating in the aggregation layer to the extent that they provide or facilitate the provision of VASP services.[20]

Box 1. International Bodies' view of DeFi arrangements

The FATF Standards are technology neutral, meaning that DeFi arrangements are subject to AML/CFT/CPF measures where they conduct one or more activities within the scope of the FATF Recommendations. Other international bodies have emphasised the principle of technology neutrality in the context of DeFi, calling for *regulatory parity* and for DeFi arrangements to achieve investor protection and market integrity outcomes comparable to those in traditional financial markets. In practice, this approach can be operationalised through a *function-based analysis* that focuses on the activities performed by DeFi arrangements and on how existing regulatory frameworks may be applied or adapted to the DeFi context.

Financial Stability Board (FSB): the FSB finds that DeFi replicates some functions of the traditional financial system, which causes it to inherit and at times amplify conventional vulnerabilities such as the automatic liquidation of derivative positions embedded into smart contracts.[21]

International Organisation of Securities Commissions (IOSCO): IOSCO finds that, in line with "same activity, same risk, same regulation/regulatory outcome", regulators should analyse DeFi arrangements within their jurisdictions with a view to applying their regulatory frameworks, where applicable. They should aim to identify persons or entities exercising control or sufficient influence over financial products and services offered by DeFi arrangements, requiring them to disclose clear and comprehensive information to promote investor protection and market integrity. IOSCO also notes the importance of regulatory co-operation to address cross-border risks and potential regulatory arbitrage.[22]

[19] https://hedera.com/learning/defi-stack/#:~:text=The%20DeFi%20ecosystem%20is%20built,the%20settlement%20and%20asset%20layers

[20] Examples of aggregators that may fall outside the FATF definition of a VASP include those that merely provide informational or comparison services, such as dashboards or price aggregators displaying publicly available market data, without controlling or facilitating the transfer of virtual assets. Similarly, interfaces that solely enable users to view, analyse, or compare DeFi protocols without executing transactions, routing orders, or otherwise participating in the transfer, exchange, or custody of assets may not meet the VASP definition. The classification of such aggregators should be assessed on a case-by-case basis, taking into account whether they perform, or facilitate the performance of, activities covered by the VASP definition under the FATF Standards.

[21] https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/

[22] FR14/23 Final Report with Policy Recommendations for Decentralized Finance (DeFi)

© FATF-OECD 2026

International Monetary Fund (IMF): The IMF considers DeFi as an innovative but risk-intensive development that remains within the regulatory perimeter and may pose financial stability and financial integrity risks as it becomes more interconnected with the traditional financial system. It emphasises that many DeFi arrangements retain effective governance or control through developers, concentrated governance tokens, protocol design, or Decentralised Autonomous Organisations (DAOs), such that regulatory responsibilities and AML/CFT expectations may still apply. Accordingly, the IMF advocates a technology-neutral, activity-based regulatory approach focused on risks rather than legal form, including identification of regulatory "anchors" where control or economic benefit exists, and proportionate mitigation measures, including restrictions where risks cannot be adequately managed.[23]

3.2. Jurisdictions' implementation of Recommendation 15 to DeFi arrangements

20. Since 2021, the FATF has collected data and monitored market developments in the DeFi ecosystem through its Targeted Updates on the implementation of the FATF Standards to VAs and VASPs. [24] The 2026 Targeted Update Report indicates that most responding jurisdictions[25] have yet to implement R.15 with regards to DeFi arrangements that fall within the scope of the FATF Standards. Only a minority (26 out of 142) have assessed the risks linked to DeFi, while a large majority (132 out of 142) have not identified any qualifying arrangements operating in their territory. Furthermore, only four jurisdictions have implemented licensing and registration requirements, and just two, in practice, have actually licensed or registered such arrangements.

21. These results indicate that countries continue to face significant challenges in applying R.15 to DeFi arrangements, including:

    i. Conducting an appropriate risk assessment, considering the complex governance structures of DeFi and its cross-border nature.

    ii. Identifying DeFi arrangements that fall under the jurisdiction's regulatory framework.

    iii. Identifying the persons, if any, that maintain control or sufficient influence over the DeFi arrangement.

    iv. Applying regulatory or enforcement measures to DeFi arrangements that fall within the scope but fail to comply with applicable requirements.

22. Challenges in implementing R.15 stem in part from the imprecise use of the term "DeFi arrangement", which allows some arrangements to present themselves as decentralised despite exhibiting centralised governance or

[23] https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/

[24] 2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf ; https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf ; https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html ; https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

[25] These statistics are based on the results of the 2026 FATF Survey on the state of implementation of R.15. A total of 142 jurisdictions provided information.

© FATF-OECD 2026

control. Where such control or sufficient influence exists, these arrangements fall within the scope of the FATF Standards and should be subject to appropriate regulation.

Box 2. Risk-based approach and materiality considerations

While this guidance aims at providing greater clarity on the application of R.15 in the context of the DeFi ecosystem, it recognises that countries' exposure to potential ML/TF/PF risks related to DeFi varies considerably. Jurisdictions in the FATF Global Network should apply the FATF Standards in accordance with their national risk profile and materiality, consistent with the risk-based approach. Countries should identify their most significant ML/TF/PF risks and prioritise their responses and mitigating measures accordingly.

The FATF Standards require all jurisdictions to assess ML/TF risks associated with VAs and VASPs, including DeFi. Jurisdictions with more significant DeFi activity should allocate more resources to understanding, supervising, and developing approaches to mitigate the illicit finance risks associated with DeFi arrangements, taking into account the characteristics of the sector. Conversely, low capacity jurisdictions with more limited exposure to VAs, VASPs and DeFi should dedicate fewer resources proportionate to the risks identified, focusing for example on monitoring market developments and emerging typologies.

In terms of materiality, available data indicate that DeFi activity is highly concentrated, with North America and Europe accounting for approximately 60% of global activity, whereas the Middle East and Africa together are estimated to contribute to less than 10%.[26] [27] Similarly, despite the large number of DeFi arrangements, many of which are small-scale, inactive, or duplicative, activity within the sector is highly concentrated. The top 12 protocols account for over 60% of global TVL, and the top 20 protocols are estimated to represent more than 70% of total DeFi liquidity.[28] Regulatory and supervisory efforts should therefore take these market asymmetries into account and prioritise engagement with the largest and most systemically relevant DeFi protocols and associated stakeholders.

[26] https://coinlaw.io/decentralized-finance-market-statistics/ ; https://www.chainalysis.com/blog/middle-east-north-africa-crypto-adoption-2024/

[27] Regional DeFi activity is typically estimated using a combination of proxy indicators, including TVL, transaction and trading volumes, user participation, and capital flows, with geographic attribution inferred from data such as exchange on-ramp activity, wallet clustering, platform usage patterns and investment origin.

[28] https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

© FATF-OECD 2026

4. Financial crime risks and typologies associated with DeFi arrangements

4.1. Threat actors, risks and typologies

23. Illicit actors exploit both the inherent characteristics and vulnerabilities of DeFi arrangements. These risks are further exacerbated where effective regulation is absent or insufficiently implemented, particularly in arrangements that fall within the scope of the FATF Standards but fail to comply with applicable obligations.

Scammers and Fraudsters

24. Global virtual assets-related fraud has grown exponentially in recent years and increasingly leverages DeFi arrangements to launder the proceeds of crime.[29] In addition, some scams exploit DeFi protocols directly or impersonate DeFi platforms to deceive victims. While DeFi arrangements have the potential to support innovative payment solutions, they may also provide complex financial services to users with limited financial literacy, thereby raising significant consumer protection concerns as their adoption becomes more widespread.[30]

Box 3. Case Studies - The SafeMoon Token Scheme and the Forsage Case (US)

The SafeMoon Token Scheme

The SafeMoon Token (SFM) scheme, which operated between March 2021 and June 2022, involved over two million investors and a market capitalisation exceeding USD 9 billion. The investigation found that Person X, the original SafeMoon (SFM) developer, created a fraudulent scheme based on false claims about locked liquidity and the absence of insider trading. Despite representing that liquidity pools were secured, Person X and two coconspirators secretly retained control over the liquidity through LP tokens, enabling them to withdraw large amounts of SFM for personal gain. Over several weeks in early 2021, they removed tens of trillions of SFM, ultimately profiting over USD 7 million to fund luxury purchases, real estate investments, and personal trading. Person X was charged with securities fraud conspiracy, wire fraud conspiracy, and money laundering conspiracy.

The Forsage Case

Person X and three co-founders created and controlled Forsage, a platform marketed as a legitimate DeFi investment opportunity powered by smart contracts. In reality, Forsage was a Ponzi and pyramid scheme operating across Ethereum, Binance Smart Chain, and Tron. Investors were required to buy

[29] https://www.chainalysis.com/blog/crypto-scams-2026/

[30] For further analysis of consumer protection issues in DeFi see the BIS and IOSCO papers: https://www.bis.org/publ/bppdf/bispap156.pdf; https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf

© FATF-OECD 2026

"slots" that generated income through recruitment and profit-sharing, but once payments were made, funds were irreversibly redistributed to earlier participants. Person X and her co-conspirators controlled the top-tier wallets—such as Forsage ID 1—which earned the most and were not required to invest any funds. Although Forsage claimed that income was transparently and entirely distributed to users, part of the smart-contract code (notably the xGold contract) siphoned funds directly to wallets controlled by the founders. Most investors ultimately lost money, while Person X's wallet was the only one to receive over USD 1 million. The conspirators now face fraud charges for misleading investors and operating the scheme through wire communications

Source: INTERPOL, United States

Professional Money Laundering Networks (PMLN) and Transnational Organised Crime

25. A wide range of illicit actors, often linked to transnational criminal organisations, increasingly rely on PMLN to launder funds through DeFi arrangements. These networks employ sophisticated layering techniques designed to obscure transaction trails and bypass centralised exchanges with AML/CFT controls. This typically involves fragmenting funds and moving them across multiple wallets before routing them through DeFi services, such as decentralised exchanges, cross-chain bridges, mixers, and swaps, to create complex, multi-layered obfuscation, often using rapid, automated transactions and chain-hopping. Following prolonged layering, the funds are consolidated and off ramped into fiat currency via centralised exchanges with weak controls or unlicensed OTC brokers and ultimately transferred back to clients through underground banking and informal value transfer systems. [31]

Proliferation financing Networks

26. Sophisticated DPRK state-linked groups have increasingly conducted cyber-enabled attacks on DeFi arrangements and employed complex, multi-layered laundering techniques within the DeFi ecosystem to generate revenue for proliferation financing activities. In April 2026, two major attacks on DeFi platforms attributed to the DPRK accounted for approximately 76% of annual losses from virtual asset-related hacking incidents:[32]

    i. The USD 285 million exploit of Drift Protocol, a major decentralised perpetual futures exchange on Solana, was widely attributed to DPRK-linked actors and executed in about 12 minutes.[33] The attackers used social engineering to obtain pre-authorised multisignature

[31] Addressing APAC's Informal Crypto Market: P2P & OTC Trading - Regulation Asia

[32] https://www.trmlabs.com/resources/blog/north-korea-stole-76-of-all-crypto-hack-value-in-2026-with-just-two-attacks?trk=public_post_comment-text

[33] https://www.trmlabs.com/resources/blog/north-korean-hackers-attack-drift-protocol-in-285-million-heist; https://www.chainalysis.com/blog/lessons-from-the-drift-hack/ ; https://www.elliptic.co/blog/drift-protocol-exploited-for-286-million-in-suspected-dprk-linked-attack

© FATF-OECD 2026

transactions, exploited the removal of a key timelock safeguard, and introduced a fabricated token that was accepted by oracles as valid collateral. This enabled them to inflate the token's value and rapidly extract substantial real assets. The incident highlights critical vulnerabilities in governance, oracle design, and operational security, as well as the growing sophistication of attacks targeting DeFi arrangements.

ii. The KelpDAO exploit resulted in losses of approximately USD 292 million following the exploitation of a single-verifier design flaw in a LayerZero bridge. The attacker manipulated cross-chain validation to drain funds from the protocol. While approximately USD 75 million of the stolen assets were frozen, the remaining proceeds were laundered through THORChain, underscoring vulnerabilities in bridge architecture and the challenges of tracing and recovering cross-chain illicit flows.

27. According to blockchain analytics companies, DPRK-linked hackers have employed a range of tactics to evade controls, including targeting DeFi arrangements that implement no, or limited, AML/CFT measures, conducting frequent, small value, structured and often automated transactions through DeFi arrangements and intentionally comingling illicit funds with large pools of unrelated or legitimate assets to further conceal their origin.[34]

28. There is evidence that Iranian proliferation networks have used certain tools in the DeFi and blockchain ecosystem like bridges, mixers, and cross-chain transfer mechanisms to obscure the movement of funds, although the majority of their activity continues to rely on abusing centralised exchanges and stablecoin-based payment channels.[35]

Ransomware Groups and Hackers

29. The sophistication of ransomware attacks and criminal hacks has grown in recent years, including through the abuse of DeFi arrangements. Ransomware actors primarily demand payment in virtual assets and increasingly use DeFi arrangements, such as decentralised exchanges (DEX), swaps and cross-chain tools, to convert proceeds into other virtual assets and conceal the origin of funds immediately after an attack. They also rely heavily on mixers to further obfuscate subsequent movements of illicit funds. Cybercriminals also exploit vulnerabilities in smart contracts governing DeFi arrangements to steal virtual assets, with the speed of chain-hopping and DeFi-based transactions often enabling laundering before industry or LEAs can respond.

[34] North Korea IT Workers: Inside the DPRK's Crypto Laundering Network

[35] targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

© FATF-OECD 2026

Box 4. Risk Typology – Governance attack

Fraudsters can take advantage of the structure of decentralised autonomous organisations (DAOs) that govern many DeFi arrangements. A DAO allows users who hold governance tokens for the arrangement to vote on critical changes or updates to the protocol. Illicit actors can accumulate governance tokens, sometimes using flash loans, to gain functional control over a legitimate DeFi arrangement's governance mechanism. Once in control, fraudsters can change key smart-contract parameters, redirect funds, or execute malicious proposals to steal assets held within the protocol.

5. Good practices in implementing R.15 to DeFi arrangements

30. This section outlines good practices that jurisdictions may adopt to mitigate the risks identified in previous sections. It covers the detection and identification of controllers of DeFi arrangements, licensing, registration, and supervisory oversight.

31. Regulators and supervisors should distinguish between the decentralised nature of the underlying DeFi technology, which offers opportunities for financial innovation, and the governance of DeFi arrangements, which may in practice be centralised and therefore subject to AML/CFT requirements. Authorities should carefully assess whether a DeFi arrangement is truly decentralised in its governance, or whether it merely purports to be decentralised, while, in reality, control remains concentrated among certain persons.

5.1. Effective risk assessment of DeFi arrangements

32. Most jurisdictions continue to face challenges in adequately identifying and assessing ML/TF/PF risks associated with DeFi (see: section 3.2). Jurisdictions should understand their overall exposure to DeFi activities and conduct a risk assessment of the DeFi sector that is adequate to their national context. This assessment may be integrated into existing national, sectoral, or industry-specific risk assessments, including the VAs and VASPs risk assessment. The risk assessment should identify the nature and materiality of DeFi-related ML/TF/PF risks, including the extent of domestic exposure, cross-border dimensions, and potential vulnerabilities arising from the operation, governance, and use of DeFi arrangements. Jurisdictions can refer to the FATF guidance on risk assessment for general principles that apply also in the context of the DeFi risk assessment.[36]

33. R.15 further requires DeFi arrangements that fall within the scope of the FATF Standards to undertake ML/TF risk assessments at the institutional level and prior to the launch or use of the software or platform. These DeFi arrangements should also take appropriate measures to manage and mitigate

[36] https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Money%20Laundering%20National%20Risk%20Assessment%20Guidance.pdf.coredownload.inline.pdf ; https://www.fatf-gafi.org/en/publications/Methodsandtrends/quick-guide-on-assessing-ML-risks-of-VA-and-VASPs.html

© FATF-OECD 2026

ML/TF/PF risks on an ongoing and forward-looking basis and implement adequate internal controls and risk mitigating measures as part of an effective compliance framework.[37]

Box 5. Conducting a risk assessment of DeFi Arrangements

United States

The United States Illicit Finance Risk Assessment of Decentralized Finance (DeFi)[38], published by the U.S. Department of the Treasury in April 2023, applies a risk-based, function-focused methodology to assess how DeFi activities may be misused for illicit finance. The assessment combines qualitative analysis of known typologies with case studies, blockchain forensics, and consultations with U.S. law-enforcement agencies, regulators, and private-sector experts. Rather than treating DeFi as a single category, it evaluates risks across different DeFi functions (such as decentralised exchanges, lending protocols, bridges, and mixing-like mechanisms), identifies relevant actors who may exercise control or provide services, and maps these activities against stages of the money-laundering lifecycle. The report covers key threat areas including ML, TF ransomware, sanctions evasion, fraud, and theft, while also examining structural vulnerabilities such as pseudonymity, automation, lack of intermediaries, and cross-border reach. Importantly, it distinguishes between the question of whether certain DeFi arrangements may qualify as regulated entities under existing U.S. AML/CFT frameworks and the broader, practical challenges of supervision and enforcement, highlighting both current mitigation measures and policy gaps.

Hong Kong, China

Hong Kong, China, conducts ongoing assessments of the risks associated with decentralised finance (DeFi) through a combination of market monitoring, operational intelligence, and case-based analysis. Given that many DeFi protocols operate without formal incorporation or registration in any single jurisdiction, the Hong Kong Police Force (HKPF) maintains continuous monitoring of developments in the global DeFi ecosystem. This includes analysing widely used DeFi protocols, understanding their governance structures, operational models, and revenue mechanisms, and assessing potential vulnerabilities that may be exploited for illicit finance purposes.

5.2. Defining controllers of DeFi arrangements

34. A key challenge for jurisdictions is determining what constitutes “control or sufficient influence” over a DeFi arrangement. The FATF Guidance clarifies that control should be understood as the ability to take key decisions within

[37] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf

[38] https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

© FATF-OECD 2026

the DeFi arrangement. The controller(s) of a DeFi arrangement may be any person who, in practice, has the authority to determine or materially influence key protocol operations or the delivery of services to users, and/or who derives significant economic benefit from such activities.[39] "Significant economic benefit" does not include broadly distributed returns (e.g. price appreciation or rewards) accruing to token holders who do not exercise control or influence over the arrangement. Controllers may have the ability to:

i. *direct, approve, or influence the execution of protocol-level actions*, including but not limited to the distribution of economic rewards, fees, or emissions to users or participants.

ii. *modify, upgrade, pause, or terminate the protocol or any of its smart-contract components*, whether through upgrade keys, administrative privileges, emergency functions, or governance mechanisms.

iii. *determine, allocate, or manage protocol assets or treasury resources*, including the authority to deploy, re-allocate, or dispose of assets on behalf of the arrangement.

iv. *add, remove, whitelist, or otherwise determine the participants, validators, or other critical users interacting with the DeFi protocol or its components that ultimately facilitate the provision of financial services.*

v. *appoint, remove, or influence persons performing key governance, operational, or administrative roles*, including developers, multisignature signers[40], oracle operators, or governance delegates.

35. Jurisdictions may encounter different challenges in the practical identification of controllers, particularly where influence is exercised indirectly, informally, or, through decentralised governance and technical arrangements. To identify controllers, jurisdictions may draw on a range of complementary sources of information, including:

i. **open source information:** such as publicly available blockchain data, protocol documentation, governance proposals and voting records, published audits, websites, blogs, social media activity, forums, and other online communications that may reveal patterns of influence, decision-making authority, or economic benefit.

ii. **third party information**: including blockchain analytics, forensic analysis, audit reports, transaction-flow mapping, disclosures by service providers (such as front-end operators, custodians, or oracle providers), information obtained through supervisory engagements,

[39] In considering how to approach the question of control of DeFi arrangements, jurisdictions may also refer to IOSCO's Policy Recommendations for DeFi and recommendations on the need to identify 'responsible persons': https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf

[40] Multisignature signers are the individuals or entities that collectively control a blockchain account, smart contract or administrative function through a multisignature wallet. Their approvals (signatures) are required to authorise a transaction or decision within a DeFi arrangement.

© FATF-OECD 2026

and reports from academic, industry, or research organisations, conferences and hackatons.

iii. **intelligence provided by the FIU or LEAs**: including suspicious transaction reports (STRs), investigative findings, seized digital evidence, or communications (for example, instant-messaging chats, emails, or co-ordination channels) that may demonstrate de facto control, co-ordination, or decision-making authority exercised by specific persons or groups within a DeFi arrangement.

5.3. Considerations to determine control in DeFi arrangements

36. The FATF does not prescribe a fixed set of criteria for identifying persons that may exercise control or sufficient influence over a DeFi arrangement but this report offers indicators (see paragraph below) that supervisory authorities can use (in addition to others) to identify controllers of DeFi arrangements established or operating in their territory, which should be applied flexibly based on distinct operational and governance structures.

37. DeFi arrangements can exhibit varying degrees of centralisation in their governance structures. Research suggests that more sophisticated and mature DeFi arrangements in some instances retain identifiable controllers who benefit from the underlying business activity and continue to exercise decision-making authority over time, including in cases where the arrangement transitions toward a Decentralised Autonomous Organisation (DAO) model.[41] The possible indicators provided below are indicative and non-exhaustive.

On-chain indicators of control:

i. **Upgradeability and back-door privileges**: The existence of upgradable contracts, proxy patterns or kill-switch functions, particularly where such powers are retained by a specific person or group, may indicate centralised control. While transparently disclosed emergency functions maintained for safety and security purposes (e.g., protecting assets in response to a cyber-attack) may or may not, in themselves, indicate control, undisclosed or unilateral access rights held by specific persons, which could present material risks if misused (e.g., back-door access), often indicate control.

ii. **Parameter setting:** Rights held by a person or group to unilaterally set or modify key protocol parameters, including risk limits, fees, rewards, collateral factors, or similar economic or operational settings are material indicators of control.

iii. **Oracle control:** the ability to select, configure or change price and other oracle feeds, including switching to manual pricing or overriding oracle inputs, may indicate control.

iv. **Control over protocol-critical smart-contract infrastructure:** Exclusive or dominant control over deployment keys, contract registries, or core contract dependencies (e.g., automated keepers, executor networks,

[41] https://www.bis.org/publ/qtrpdf/r_qt2112b.htm; https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3208~051a880042.en.pdf

© FATF-OECD 2026

settlement contracts) may indicate direct operational influence over protocol integrity and continuity.

v. **Fee flows and profits:** Control may be inferred where specific addresses receive protocol level economic flows such as fees, maximal extractable value (MEV) rebates, liquidation penalties, or token emissions (i.e., newly issued tokens). Such flows can indicate continued influence or control by the recipients.

vi. **Administration / gatekeepers:** Where liquidity pools or protocol functions are permissioned, meaning access is restricted to approved or whitelisted participants, the persons who administer these permissions and determine access rights may be identified as controllers.

vii. **Governance concentration and voting power:** Concentrated governance token holdings, influential delegated voting blocs, or low participation rates that enable a small number of actors to determine governance outcomes may indicate de facto control over strategic decisions, upgrades, and treasury allocations.

Off-chain indicators of control:

viii. **Custody and operations:** Persons designated as signatories for governance or administrative decisions, those controlling upgrade keys, or those co-ordinating or obtaining custodial services for assets on behalf of the arrangement may be reasonably identified as controllers, given their ability to influence critical operational or security-related functions.[42]

ix. **Front-end operation and distribution:** Control over public web front-ends (including mobile apps) and associated content or tools (such as wallets) may indicate centralised influence, as those who operate, maintain or distribute these interfaces can shape how users access and interact with the DeFi arrangement.

x. **Corporate entities:** Companies, foundations, labs, operating companies, or other legal persons that employ core contributors, hold IP rights, manage treasuries or pay service providers may be exercising centralised control. The extent of control depends on their actual independence from the protocol and the degree to which they influence governance, development or operations.

xi. **Control over development, roadmap or off-chain infrastructure:** persons who determine development priorities, control releases, or manage essential off-chain infrastructure (e.g., indexers, data services, automation systems) may exercise substantial influence over the DeFi arrangement's direction and functioning. This indicator may be separate from individual

[42] Examples of such roles include signatories to treasury or reserve wallets holding protocol funds; administrators of multisignature wallets used to execute governance decisions; holders of upgrade keys enabling modification of smart contracts; or entities coordinating custodial arrangements for user or protocol assets. These functions confer practical control over key aspects of the arrangement, including the movement of funds, implementation of protocol changes, and mitigation of security incidents.

© FATF-OECD 2026

developers who contribute to DeFi arrangements' infrastructure without demonstrating real control.

xii. **Branding, communications and user direction:** Control over official branding, public messaging, documentation, risk disclosures or educational materials may indicate influence.

38. Controllers of DeFi arrangements may include persons with different roles and responsibilities within the arrangement. The existence of multiple controllers operating different components of a DeFi arrangement does not in itself remove or dilute AML/CFT obligations. In practice, most DeFi arrangements provide financial services akin to the FATF definition of financial institution and VASP, [43] and any person that maintains control or exercises sufficient influence over the arrangement should be considered as providing or actively facilitating financial services.

39. Controllers may include developers, governance token holders, core maintainers, front-end operators, investors, oracle (and other data) providers, foundation or corporate entities. This list is non-exhaustive, and controllers can potentially overlap and fall into multiple categories depending on the specific characteristics of the DeFi arrangement. Jurisdictions should adopt a functional approach to the identification of controllers in the DeFi context, assessing who effectively controls or influences different aspects of the arrangement. For example, in certain jurisdictions, entities operating websites or interfaces that facilitate user interaction with DeFi protocols may fall within the regulatory perimeter where they provide or "arrange" VA services, even in the absence of direct control over the underlying smart contracts. Other jurisdictions may take a different approach.

[43] Certain DeFi arrangements do not provide financial services and therefore fall outside the scope of the FATF Standards. These typically include protocols or platforms that support infrastructure, governance, or data functions rather than facilitating the transfer, exchange, or custody of assets. For example, decentralised governance platforms that enable token holders to vote on protocol changes, blockchain oracles that supply external data to smart contracts, and developer tools or protocol interfaces that allow users to interact with blockchain networks do not, in themselves, constitute financial services.

© FATF-OECD 2026

Box 6. Japan's efforts to develop an appropriate and proportionate regulatory framework to control DeFi arrangements

The JFSA held discussions on regulatory approaches to crypto-asset systems through a Working Group (WG) on Crypto-asset Systems of the Financial System Council, with the participation of private-sector experts. In the course of these discussions, the JFSA referred to DeFi. The WG report published in December 2025 noted that entities providing user interfaces (UIs), such as applications that connect users to decentralised exchanges (DEXs), to residents in Japan may need to be subject to regulation proportionate to risks. Such regulation could include obligations to provide clear explanations of the risks associated with the connected services, as well as AML/CFT requirements, including customer due diligence obligations under Japan's AML/CFT Act.

Furthermore, the report indicates that while the development and deployment of DEX protocols may fall outside the scope of the current legal framework, DEXs have deficiencies or vulnerabilities in their protocols and also carry a risk of being used for money laundering. It notes that proportionate, technology-specific risk-mitigation measures—distinct from those applicable to existing exchange service providers—should continue to be explored, with due regard to international regulatory discussions. Building on the directions set out in the report, the JFSA has been further deepening its considerations while strengthening engagement with DeFi-related stakeholders, holding ad-hoc roundtables with private sector firms and other relevant participants.

Source: Japan

5.4. Assessment of control over DeFi arrangements

40. Although many DeFi arrangements present themselves as decentralised, a number of them may have controllers who maintain decision-making authority over key aspects of their operations.[44] Supervisory authorities should therefore remain vigilant and focus on the functions performed by DeFi arrangements and the underlying business rationale, rather than how they are labelled or marketed. Where a DeFi arrangement effectively provides business services similar to those of financial institutions or VASPs, controllers may exercise operational management and derive economic benefit from its activities. In such cases, the arrangement should fall within the scope of the jurisdiction's regulatory and supervisory framework.

41. Supervisors should particularly be mindful of the following scenarios in which control could be retained within purportedly decentralised DeFi arrangements:

[44] https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3208~051a880042.en.pdf ; 2024-2nd-global-cryptoasset-regulatory-landscape-study.pdf; Ecosystem Map | DeFi Navigator

© FATF-OECD 2026

i. *Governance transferred from a legal entity to a DAO*: Where a project migrates governance from a company or foundation to a DAO, the transfer may be nominal rather than substantive. Authorities should look for indicators of continued control, including the founding members retaining governance tokens or special voting privileges, submitting most governance proposals, maintaining de facto operational control over the DAO, or benefitting from most fee flows and profits.

ii. *Governance tokens distribution*: concentration of governance tokens in a small number of wallets (e.g., a protocol in which fewer than 1% of wallets hold a controlling majority of voting power) may indicate control over the DeFi arrangement. Supervisors should carefully assess the practical privileges and influence associated with the governance tokens, such as voting weight, proposal rights, veto powers, and upgrade authority, to determine whether token concentration translates into meaningful decision-making control in practice. Persons may also exercise control or sufficient influence over a DeFi arrangement by holding governance tokens across multiple seemingly unrelated wallets. When assessing governance structures, supervisors should therefore consider potential wallet clustering and behavioural patterns that may indicate consolidated control.

iii. *Delegation of voting rights and voting patterns*: small or inactive governance token holders may delegate their voting rights to other participants, thereby bolstering other token holders' influence over the arrangement. While delegation is often presented as a mechanism to increase participation and improve governance efficiency, it can also significantly concentrate effective control, amplifying the influence of large token holders and obscuring the extent of consolidated influence. Delegation of voting rights may be complex and opaque, and authorities should carefully assess specific circumstances to determine whether it may confer effective control.

© FATF-OECD 2026

Box 7. Example of control in DeFi arrangements

Ooki DAO – United States[45]

The Commodity Futures Trading Commission (CFTC) charged Ooki Decentralised autonomous organisation (DAO) in an administrative order against Ooki DAO's predecessor LLC (bZeroX).

1. *Use of DAO structure to avoid oversight*: bZeroX LLC transferred control of the software to a DAO. The founders explicitly advertised the move to the bZeroX community as a way to avoid complying with the Commodity Exchange Act (CEA) and potential enforcement actions, but control was actually retained by a few persons.
2. *Founders' influence through governance tokens*: Formally, voting rights and admin keys were distributed among holders of a specific governance token. Individuals with these tokens included the founders, who could propose and vote on protocol changes and influence key financial operations. Ooki DAO lacked formal centralised leadership, however, de facto the founders continued to exercise control through governance tokens.

In June 2023, a federal judge ruled in favour of the CFTC and held that Ooki DAO is a "person" under the CEA, with token holders effectively exercising collective managerial authority even though no central executive team directed the operations. The Court order required Ooki DAO to pay a civil monetary penalty of over USD 643,000. However, the decision was a default judgment as Ooki DAO did not appear before the court and therefore carries limited precedent under U.S. law.

5.5. Truly decentralised DeFi arrangements

42. While some DeFi arrangements have centralised elements, other DeFi arrangements may be highly decentralised, with no person exercising control or sufficient influence over their operations. These DeFi arrangements do not fall within the scope of the FATF Standards. Supervisors should assess the control structure of a DeFi arrangement using a range of criteria[46] before determining whether the arrangement is truly decentralised. Authorities should not rely solely on information provided by the DeFi arrangement itself or on marketing terms used to describe its degree of decentralisation but should conduct an independent analysis to understand different types of control structures that may exist within the arrangement, (e.g., operational, governance, etc.).
43. Regulatory and supervisory authorities will not be able to mitigate the risks posed by truly decentralised DeFi arrangements through the direct imposition of AML/CFT requirements. Instead they should consider broader, risk-based

[45] https://www.taxnotes.com/research/federal/court-documents/court-opinions-and-orders/court-orders-shutdown-blockchain-based-software-operator/7jhws

[46] Please refer to the considerations set out in Section 5.3 of this report.

© FATF-OECD 2026

and holistic mitigating measures, including issuing guidance to regulated entities on the risks of interacting with such arrangements, and clarifying whether, and under which conditions (e.g., the application of enhanced AML/CFT controls), engagement with these arrangements may be appropriate. Regulated entities that interact with the DeFi ecosystem may include:

i. *Stablecoin issuers* that retain the ability to freeze and burn stablecoins used in truly decentralised DeFi protocols.

ii. *VASPs that provide on- and off-ramps*[47] into the DeFi ecosystem, and have KYC and CDD responsibilities, as well as the obligation to submit STRs for suspicious transactions.

iii. *front-end platforms*[48] used to access the underlying DeFi arrangement that may have identifiable controllers and AML/CFT obligations.

iv. *Financial institutions* interacting with the DeFi arrangement.

44. In parallel, regulatory and supervisory authorities are also encouraged to engage extensively with the private sector to consider innovative AML/CFT solutions that could be applied also in the context of truly decentralised DeFi arrangements, including leveraging cryptographic and digital identity technologies, as well as blockchain analytics.

5.6. Licensing and/or registration requirements for centralised DeFi arrangements

Centralised DeFi arrangements

45. Jurisdictions should impose licensing or registration requirements on centralised DeFi arrangements to be compliant with R.15.[49]

i. At a minimum, DeFi arrangements that are controlled by legal persons should be required to be licensed or registered in the jurisdiction(s) where they are created.

ii. In cases where the controller or person exercising sufficient influence over the DeFi arrangement is a natural person, such person should be required to be licensed or registered in the jurisdiction where their place of business or residence is located.

---

[47] On- and off-ramps refer to services that enable movement between the traditional financial system and the virtual assets ecosystem. An on-ramp allows users to convert fiat currency (e.g., EUR, USD) into virtual assets, or virtual assets into another virtual asset, serving as an entry point into the virtual asset environment. Conversely, an off-ramp enables users to convert virtual assets back into fiat currency, providing an exit route from the virtual assets ecosystem and ensuring users can redeem virtual assets for spendable, real-world currency. https://www.coinbase.com/en-fr/learn/crypto-basics/what-are-fiat-on-ramps-and-off-ramps

[48] Authorities should be able to determine how to treat front-end providers at their own discretion, either as a compenent of a DeFi arrangement or as an independent function.

[49] Paragraph 3, Interpretative Note of Recommendation 15 FATF Recommendations 2012.pdf.coredownload.inline.pdf

© FATF-OECD 2026

iii. Jurisdictions may also require persons controlling DeFi arrangements that provide, facilitate or promote products and services to customers within their jurisdiction to be licensed or registered.[50]

Centralised DeFi arrangements where controllers cannot be readily identified

46. While supervisory authorities may be able to determine that a DeFi arrangement has controllers, for example through the analysis of governance-token voting rights, associated wallet behaviour and other factors, the process of identifying those persons may still be difficult due to the pseudonymous nature of the blockchain ecosystem. To mitigate these issues, supervisory authorities should collaborate as closely as possible with other entities that may hold additional information on the identity and role of controllers, including:

    i. relevant domestic authorities, including FIU and LEAs.

    ii. Foreign counterparts by leveraging established international co-operation mechanisms.[51]

    iii. Private sector, including blockchain analytics companies, who may be able to collect further identifiers leveraging technological tools.

47. Where possible, supervisory authorities should engage with DeFi arrangements to request information on persons exercising control, particularly where such controllers cannot be readily identified despite being subject to licensing or registration obligations under R.15.

48. Supervisory authorities should adopt a risk-based approach to the identification of controllers, prioritising their efforts based on materiality of, and risks posed by, the DeFi arrangement within their jurisdiction. Supervisors should explore all reasonable avenues[52] to identify the persons exercising control. If, after undertaking such efforts, supervisory authorities are still unable to identify the controllers, they may apply similar risk-mitigating measures as those recommended for truly decentralised DeFi arrangements.

49. Supervisors should undertake ongoing efforts to identify controllers and effectively implement regulatory measures for centralised DeFi arrangements in line with the FATF Standards, particularly where these arrangements present higher risks. Examples of such efforts can include but are not limited to:

    i. Conducting **continuous blockchain analytics**, including transaction tracing, wallet clustering, and network analysis to identify linkages between addresses and potential controllers.

[50] The FATF has analysed the risks and regulatory challenges linked to Offshore VASPs (including relevant DeFi arrangements) in March 2026 https://www.fatf-gafi.org/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html

[51] Please refer to the information included in sections 6.1. of this report.

[52] Depending on the risk and context of the jurisdiction, "reasonable avenues" may include the actions set out in paragraph 47, as well as co-operation with the entities identified in paragraph 44.

© FATF-OECD 2026

ii. Monitoring **governance and operational control** points, such as voting activity, proposal initiation, multisignature signatories, treasury wallet management, and the use of upgrade or admin keys.

iii. Leveraging **regulated entities** as information gateways, including by requiring VASPs and financial institutions to collect, analyse, and report information on interactions with DeFi arrangements.

iv. Using **supervisory and financial intelligence tools**, including STRs, supervisory reporting, and data from fiat on/off-ramps to support attribution efforts.

v. Maintaining **ongoing monitoring frameworks**, ensuring that identification efforts are continuous and adapted as new information, tools or risks emerge.

vi. **Documenting and periodically reassessing efforts**, including maintaining records of investigative steps taken, outcomes, and updated risk assessments over time.

Box 8. Imposing licensing and registration requirements to DeFi arrangements

1. Jurisdictions should ensure that perimeter-review processes are designed to be able to identify DeFi arrangements operating within their territory, using, when relevant, the same methods and tactics to detect non-resident ("offshore") VASPs.[53] These may include: web-scraping and open-source information to identify any advertising, promotional communication or other solicitations for business; information from the general public, obliged entities (e.g., VASPs) and industry circles; FIU or other information from reporting institutions, such as STRs or investigative leads; law enforcement or intelligence reports, including information from international co-operation (e.g., tips from international counterparts).
2. Where a DeFi arrangement is identified, supervisory authorities should conduct a holistic "control assessment" to determine whether the arrangement is genuinely decentralised. This assessment may be informed by the indicators set out in section 5.3 of this report, as well as any additional criteria determined by the Supervisory Authority.
3. Where an arrangement is found to be centralised and to have persons exercising control or sufficient influence over its operations, supervisors should allocate appropriate resources to conduct a comprehensive analysis of the arrangement's control structure.
    a. Where the controller(s) can be identified, the DeFi arrangement should be brought within the supervisory perimeter as a VASP or a financial institution consistent with the activities conducted and the jurisdiction's regulatory framework.

[53] Section 3.1 of the oVASP report : https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf

© FATF-OECD 2026

b. Where the controller(s) cannot be identified after all reasonable avenues have been explored, supervisory authorities may consider alternative mitigating measures similar to those applied for truly decentralised DeFi arrangements. Supervisors should take ongoing efforts to identify controllers and effectively implement regulatory measures for such DeFi arrangements in line with the FATF Standards, particularly where these arrangements present higher risks.

4. Where arrangements are truly decentralised, they do not fall within the scope of the FATF Standards; however, jurisdictions should still adopt a risk-based approach and consider what alternative measures can be implemented to mitigate the illicit finance risks posed by these arrangements.

5.7. Supervisory practices

50. Jurisdictions should consider the following supervisory practices when shaping their approach to the unique characteristics of the DeFi ecosystem and mitigating associated illicit finance risks. Countries should avoid adopting a tick-box approach, as DeFi arrangements often exhibit highly variable and distinctive features. Supervisory measures should instead be proportionate, risk-based, and tailored to the specific risks and contextual factors presented by each DeFi arrangement. It is also critical that supervisors issue clear guidance on existing requirements (including that DeFi arrangements should be subject to licensing or registration when controllers exist) so that obliged entities fully understand jurisdictions' expectations.

51. *Establish clear standards for smart contract audits*: Jurisdictions may consider establishing robust and transparent standards for smart-contract audits to ensure that reviews of DeFi arrangements are comprehensive, independent, and aligned with recognised security best practices. Jurisdictions may also consider making audits mandatory for certain categories of DeFi arrangements, particularly those handling significant user funds, employing complex cross-chain bridges, or relying on high-risk architectural components (e.g., multi signature administrative keys, proxy patterns).

52. *Require, or at least encourage, embedded AML/CFT controls at protocol and/or interface layer:* Jurisdictions may consider requiring or at least encouraging DeFi arrangements to embed AML/CFT controls directly within their smart contracts interface layer or as an external wrapper. These may include, for example, automated freezing mechanisms for addresses associated with sanctioned persons, on-chain risk-scoring logic, controls that delay or block high-risk transactions pending verification, or requirements for verifiable credentials (e.g., proof-of-KYC) before executing certain high-risk functions. Such embedded controls can help mitigate illicit finance without disproportionally hindering distinctive and innovative features of the DeFi ecosystem.

© FATF-OECD 2026

Box 9. France working group on smart contract certification

In January 2024, the Autorité de contrôle prudentiel et de résolution (ACPR) and the Autorité des Marchés Financiers (AMF) jointly established a working group under the ACPR-AMF Fintech Forum to examine smart contract certification within the broader context of potential future DeFi regulation. The group focused on defining possible certification standards and audit methodologies. Its findings were published in February 2025 in a report available on the ACPR and AMF websites.

The report explores how certification could reduce user risks, enhance trust and possibly inform future regulatory frameworks. It provides high-level principles, views from working group members, and explores regulatory options around the certification of smart contracts, highlighting that trust and resilience in DeFi ecosystems require certification based on clear, measurable standards, including on compliance.

The report mentions that measures to combat ML/TF/PF could be technically embedded directly into specific smart contracts, thereby facilitating their use by entities subject to AML/CFT regulation, including crypto-asset service providers and other financial institutions. For example, smart contracts could incorporate regularly updated lists of addresses with which interactions are prohibited. In addition, elements of zero-knowledge proof (ZKP)–based customer verification could be integrated to ensure that access to certain smart-contract functionalities is restricted to users who have undergone enhanced identity or due-diligence checks. The study highlighted that a smart contract certification could assess areas such as security and code quality, governance and upgradeability, execution environment, transparency and access control, lifecycle management and user protection.

Source: France

53. *Issue best practices for transparent and responsible emergency controls*: Jurisdictions may consider issuing a set of best practices related to the design and use of emergency controls (e.g., pause functions, circuit-breakers) within DeFi arrangements. These guidelines should clarify how such controls can be implemented transparently, with appropriate governance safeguards and accountability, to mitigate severe risks such as cyberattacks, protocol exploits, or large-scale laundering, while preserving the arrangement's decentralised characteristics to the greatest extent possible.
54. *Enhance oversight of front-end providers and oracle operators*: Jurisdictions may consider enhancing oversight of key off-chain infrastructure providers, particularly front-end interfaces and oracle operators, as these components exert significant influence over user interactions and protocol behavior. Supervisors may encourage or require such providers to adopt measures that reduce illicit activity, such as automated screening, risk-scoring, geo-blocking based on sanctions, or improved transparency around oracle data sourcing and manipulation-resistance.
55. *Conduct blockchain monitoring of high risk DeFi arrangements*: Jurisdictions may consider deploying blockchain-analytics capabilities to monitor DeFi arrangements operating in their territory. This may involve tracking suspicious flows, identifying patterns consistent with illicit finance, and conducting ongoing risk assessments based on transaction data. Jurisdictions

© FATF-OECD 2026

may also consider sharing relevant findings with regulated financial institutions and VASPs that interact with these arrangements to support stronger detection of illicit funds.

56. *Promote transparency in DeFi governance structures*: Jurisdictions may consider introducing measures to ensure that DeFi arrangements maintain transparent and easily identifiable governance structures. This can help reduce the risk of governance obfuscation, concentration of control, or covert influence by illicit actors. Measures may include encouraging public disclosure of governance processes, ensuring clarity around voting rights and delegation, and promoting transparency regarding persons that influence upgrades, parameter changes, or protocol operations.

57. *Regulatory sandboxing*: Regulatory sandboxes are schemes established by competent authorities that allow regulated and unregulated entities to test innovative products or services under defined guardrails. Jurisdictions may consider establishing regulatory sandboxes for DeFi arrangements to trial supervisory approaches in a controlled, risk-managed environment. Regulatory sandboxes can be resource-intensive for both the public and private sector and may not be the most appropriate tool in all scenarios.[54]

Box 10. Regulatory sandboxes for DeFi arrangements

Bermuda

DerivaDex Bermuda 1 Class T (Sandbox) – small scale limited operation with continuous oversight from Prudential, Cyber risk and AML on their risk and governance and evolution of the Company. Operating volume – as the Company has recently started operations, with license restricted to 1,000 active users. The Company doesn't hold client funds. The only DeFi arrangement currently operating out of the jurisdiction sought licensing and the governance structure is known to the Authority.

The single DeFi arrangement operating has implemented, through an Outsourcing arrangement, KYC/CDD verification services, AML checks, Proof of address verification, Crypto AML checks, Identity document authentication, Face match verification, Ongoing AML monitoring.

Source: Bermuda

5.8. Interaction between DeFi arrangements and regulated financial institutions and VASPs

58. Jurisdictions should ensure that financial crime risks associated with the DeFi ecosystem are sufficiently understood by obliged entities, including financial institutions and VASPs. The financial sector is increasingly interested in interacting with DeFi arrangements, both within permissioned and

[54] Building A Regulatory Sandbox | Digital Finance Inclusion; Regulatory sandbox toolkit | OECD; How Regulatory Sandboxes Foster Innovation and Compliance in Crypto

© FATF-OECD 2026

permissionless environments, to take advantage of operational benefits, including automated settlement, cross-border outreach, 24/7 availability, and generally higher yields. As regulated financial institutions, VASPs and DeFi arrangements become more interconnected, developments within the DeFi ecosystem can have broader implications for AML/CFT compliance, potentially heightening ML/TF/PF vulnerabilities across the broader virtual assets and financial system.

59. Financial institutions and VASPs interacting with DeFi arrangements should be required to undertake a risk assessment of the products and take appropriate measures to manage and mitigate the risks posed by these arrangements, in line with R.15 paragraph 1. When financial institutions and VASPs offer services to DeFi arrangements, they should also comply with Recommendations 10 (Customer Due Diligence when the DeFi arrangement is seeking to become a client or is already a client) and Recommendation 13 (when the DeFi arrangement is seeking to establish a correspondent banking relationship), and they should refrain from interacting with DeFi arrangements if these specific obligations under the FATF standards cannot be fulfilled. They also have a general obligation to maintain the integrity of their AML/CFT frameworks and to ensure the effective application of preventive measures within their ecosystems. Financial institutions and VASPs should assess DeFi arrangements in a risk-based and proportionate manner and implement appropriate mitigating measures in different scenarios:

    i. Centralised DeFi arrangements: Financial institutions and VASPs should conduct CDD on the DeFi arrangement, in line with the FATF Standards on correspondent banking, including determining whether the arrangement is licensed or registered and subject to adequate supervision. Financial institutions and VASPs should perform adequate due diligence or ensure that the arrangement has implemented AML/CFT controls, in line with Recommendations 10 and 13.[55]

    ii. Centralised DeFi arrangements where controllers cannot be readily identified and truly decentralised DeFi arrangements: Financial institutions and VASPs should apply appropriate AML/CFT measures to the underlying customers of the DeFi arrangement, including identity verification, and, where appropriate, ongoing monitoring of the protocol's integrity and security. Financial institutions and VASPs remain responsible for ensuring that their interactions with such arrangements are compliant with AML/CFT requirements. Supervisors should provide further guidance to obliged entities, taking into account jurisdictional risks as well as sector- and entity-specific considerations.

60. Financial institutions and VASPs' interactions with DeFi arrangements should be matched with robust risk-mitigation measures. DeFi arrangements that allow unrestricted user access without any AML/CFT controls may be

[55] Some DeFi arrangements have established permissioned environments to interact with regulated financial institutions while meeting regulatory expectations. Financial institutions should assess the sophistication of AML/CFT controls implemented by these DeFi arrangements and ensure that these are compatible with their own AML/CFT programs.

© FATF-OECD 2026

considered higher risk, as they can facilitate direct interaction with potentially illicit actors. Financial institutions and VASPs should carefully assess whether they can implement adequate AML/CFT mitigating measures within their own compliance framework to interact with such arrangements without breaching their compliance obligations.

61. While understanding a DeFi arrangement's governance structure, audits, and cybersecurity controls is good practice, obliged entities should prioritise assessing the adequacy and effectiveness of the AML/CFT controls implemented by the arrangement and establish robust frameworks to effectively identify and verify the identity of its underlying users. They should also apply additional mitigating measures (e.g., real-time monitoring through blockchain analytics tools) as appropriate.

62. Regulatory and supervisory authorities may consider adopting a tailored and more flexible approach where truly decentralised DeFi arrangements incorporate effective AML/CFT risk-mitigation measures at the protocol level. Such measures may include reliance on third-party KYC/CDD providers, embedded KYC/CDD solutions, and the use of allow-lists or block-lists at the smart contract or front-end level. In such cases, the residual risk associated with the DeFi arrangement may be lower, and the AML/CFT controls applied by financial institutions and VASPs to the underlying customers of the DeFi arrangement may be calibrated, provided that risks are mitigated effectively and on an ongoing basis.

© FATF-OECD 2026

Box 11. Case studies: Financial institutions and VASPs interaction with DeFi arrangements

Domestic co-operation between financial regulator and law enforcement to support robust supervision

The UK adopts a multi-agency co-operation approach at the domestic level to address emerging risks associated with DeFi, particularly where these activities intersect with traditional financial services and the broader virtual asset ecosystem. The Financial Conduct Authority (FCA), as the regulator of VASPs, works closely with law enforcement agencies such as the National Economic Crime Centre through regular meetings and information-sharing forums covering ML/TF/PF risks.

These mechanisms enable law enforcement to inform the FCA of new business models involving regulated financial institutions, VASPs, and DeFi. In response, the FCA has undertaken targeted supervisory activities to assess the application and effectiveness of financial crime controls on new products that were not covered at the time of authorisation.

These supervisory efforts include reviews of on- and off-ramping arrangements, product risk assessments (including links between fiat and virtual assets), wallet management practices, customer onboarding processes, CDD/EDD measures, and compliance with travel rule and sanctions requirements. This work has allowed the FCA to identify gaps and require improvements where necessary.

Overall, the case demonstrates how effective multi-agency co-operation can support early intervention outside the regular supervisory cycle and foster a shared understanding among competent authorities of ML/TF risks associated with emerging DeFi-related products.

Source: United Kingdom

Monetary Authority of Singapore (MAS) Supervisory Practices

MAS engages with Digital Payment Token Service Providers (DPTSPs) to evaluate their DeFi exposure on a bilateral basis, as part of the supervisory and licensing process. At the minimum:

1. If a DPTSP provides services to customers engaged in DeFi-related activities, the customer's source of wealth and any other material nexus to these activities should be considered as part of the DPTSP's customer risk assessment. Where appropriate, the VASP should apply enhanced due diligence (EDD), including strengthened ongoing monitoring. DPTSPs should fully consider the nature and risk profile of the customer's DeFi-related activities and ensure that their risk assessment is comprehensive and proportionate.

2. If the DPTSP partners with a DeFi platform to provide customer services, the DPTSP should conduct a risk assessment on the ML/TF risks associated with the provision of services through the DeFi platform, as well as due diligence on the DeFi platform to assess (i) the robustness of the DeFi platform's AML/CFT/CPF risk control framework; and (ii) the DeFi platform's alignment with the DPTSPs own AML/CFT/CPF framework and regulatory requirements.

Source: Singapore

© FATF-OECD 2026

6. Enforcement and other actions to mitigate risks associated with DeFi arrangements

63. The FATF has published guidance on how authorities can investigate and confiscate virtual assets, including stablecoins, which is also relevant for DeFi arrangements.[56] In the specific case of DeFi, authorities may face additional challenges arising from their unique characteristics.[57] DeFi-related investigations often encounter complex obfuscation techniques, including chain-hopping, cross-chain swaps, and micro-structuring. Jurisdictions should establish robust interagency mechanisms that facilitate joint operational analysis and rapid response, and should use Public-Private Partnerships (PPPs) to integrate real-time blockchain analytics and advanced tracing tools into LEAs operations.

6.1. Use of blockchain analytics tools in DeFi-related investigations

64. LEAs should leverage blockchain analytics tools to support investigations involving DeFi protocols. These tools enable the tracing of fund movements across multiple blockchains and assets, including through mixers, bridges, and complex smart contract interactions, allowing investigators to reconstruct transaction flows. They also provide visualisation capabilities to map relationships between wallets, entities, and protocols, alongside detailed smart contract analysis to understand how funds move within DeFi environments. In addition, automated detection of suspicious patterns, such as layering or peeling, combined with advanced attribution techniques, can support the identification of entities controlling wallets and their potential links to illicit activity.

65. While blockchain analytics tools can support investigations into DeFi arrangements, jurisdictions should be aware that their effectiveness may be limited as DeFi platforms become more technically sophisticated. For example, the migration of DeFi activity from public blockchains to specialised Layer 1 networks, many of which are not yet supported by mainstream analytics tools, as well as the pooling of deposits from multiple users within a single smart contract, can reduce transparency and make it more difficult to attribute transactions to individual users.

[56] Asset-Recovery-Guidance-Best-Practices.pdf.coredownload.pdf;

https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html; https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

[57] Please refer to the information included in section 2.1. of this report.

© FATF-OECD 2026

Box 12. Hong Kong, China: Investigating DeFi arrangements

Within Hong Kong Police Forces (HKPF), a dedicated cryptocurrency investigation team conducts investigations and regularly analyses the use of DeFi protocols in criminal activities. Through these investigations, authorities identify typologies involving decentralised exchanges, cross-chain swaps, liquidity pools, and other DeFi mechanisms that may be used to facilitate fraud, hacking, or the laundering of criminal proceeds. HKPF also operates a cryptocurrency stop-payment co-ordination mechanism to facilitate the rapid containment of illicit virtual assets. When crime proceeds are traced to DeFi-related activities, HKPF may engage relevant platforms to obtain digital footprint information and, where feasible, assist in preventing the dissipation of assets associated with criminal activity.

In addition, HKPF have handled multiple incidents involving attacks on DeFi-related platforms and Web3 infrastructure. These investigations involve identifying the causes of security vulnerabilities, providing security advice to affected entities, and co-ordinating rapid response actions to mitigate losses. Such actions have, in some cases, enabled the containment of stolen virtual assets shortly after the incidents occurred.

Source: Hong Kong, China

6.2. Co-ordination with other competent authorities

66. LEAs should closely collaborate with supervisory authorities, FIUs and other relevant competent bodies. Rather than relying solely on traditional MoUs, domestic co-operation should be operationalized through actionable frameworks. This includes:

    i. *Establishing joint standard operating procedures (SOPs)* for emergency asset freezing, providing cross-agency access to proprietary blockchain analytics platforms, and facilitating temporary personnel secondments between supervisory and LEAs to build lasting institutional capacity and real-time operational synergy.

    ii. *Specialised, multi-disciplinary joint task forces* can support investigations given the highly technical and borderless nature of DeFi arrangements. These task forces should integrate the distinct expertise of FIUs, cybercrime divisions of LEAs, and financial supervisors. Pooling resources such as advanced blockchain analytics tools, cyber-forensic capabilities, and traditional financial intelligence allows authorities to conduct parallel investigations and prevents the loss of digital evidence.

6.3. Freezing and Recovery of Illicit Funds

67. Freezing and recovering funds linked to illicit activity in DeFi present both operational and regulatory challenges. Criminals frequently exploit DeFi's composability and pseudonymity to layer transactions or route them through mixers, cross-chain bridges, and DEXs before authorities can intervene. These

© FATF-OECD 2026

dynamics make traditional asset-seizure approaches harder to apply, especially in the absence of centralized intermediaries.

68. An effective approach to mitigate these risks under the existing regulatory framework is to focus efforts on adjacent components of the broader virtual assets' ecosystem that are capable of applying freezing or rejecting mechanisms, as well as unique intermediaries within the DeFi ecosystem, including:

    i. *Fiat-backed stablecoin issuers* that have the ability to freeze, block, burn or reissue tokens associated with criminal activities play a particularly relevant role, given that stablecoins represent 90% of VAs in the DeFi ecosystem.[58] To facilitate co-ordination, competent authorities should actively leverage established global networks, such as the INTERPOL I-24/7 secure communication channel which allows LEAs to swiftly co-ordinate with stablecoin issuer's home jurisdiction and execute emergency asset freezing requests before illicit funds are dissipated or off-ramped. Jurisdictions should also consider integrating INTERPOL's tailored Notices into their cross-border investigative workflows.

    ii. *VASPs acting as custodial endpoints* can freeze illicit assets that have been laundered through DeFi arrangements immediately upon receiving a lawful order, such as a subpoena, seizure warrant or freezing instruction. VASPs can be critical choke points for asset recovery, as illicit actors abusing DeFi arrangements often will use a fiat off-ramp.

    iii. *DeFi front-ends* that integrate certain compliance tools may be able to automatically reject assets associated with illicit actors by leveraging blockchain analytics, risk ratings, and other red flag indicators. These rejections may prevent the illicit actors that may be using the front-end from accessing a DEX, bridge, or other DeFi arrangement. The front-end operator may then be able to contact the relevant authorities to share information on the rejected transactions.

69. Criminal actors are increasingly targeting DeFi arrangements through sophisticated hacks. In response, many protocols rely on individuals who hold admin keys or participate in multisignature control structures who can take emergency actions, such as disabling front-end interfaces, pausing contract functionality, freezing specific vaults, pools or modules and adjusting system parameters to prevent the attacker from completing the exploit. LEAs should proactively identify and engage with these key individuals operating in their jurisdiction, so that effective measures can be co-ordinated quickly to preserve funds before they are moved out of the protocol.

[58] For further information on how stablecoin issuers can freeze and burn stablecoins please see: targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

© FATF-OECD 2026

7. International co-operation

7.1. Cross-border information sharing

70. Cross-border information sharing is fundamental to identify centralised DeFi arrangements that may be operating without the appropriate registration or licence. Effective cross-border co-operation also supports a deeper understanding of the risks posed by truly decentralised DeFi arrangements that may be abused by illicit actors, including the potential cascading effects on regulated entities. Authorities should leverage to the largest extent possible existing international co-operation mechanisms, like IOSCO's Multilateral Memorandum of Understanding (MMoU), to share data on emerging risks, investigative findings and enforcement actions.[59]

71. Effective **information sharing between FIUs** also plays a key role in identifying cross-border DeFi-related risks. Experiences from the FATF Global Network indicate that exchanges of operational and strategic analysis can support the detection of emerging misuse of DeFi arrangements and tracing efforts. Jurisdictions have reported using the following channels to exchange information:

    i. Egmont Secure Web[60]

    ii. "Next-Generation" FIU.net[61]

72. **Supervisory authorities** should cooperate to the greatest extent possible to exchange information on the persons who control or exercise sufficient influence over DeFi arrangements, since these may be anywhere in the world, and information on their identity may not be available in the jurisdiction where the controller(s) of the DeFi arrangement operate. Supervisory authorities should also share to the extent possible information about DeFi arrangements, including technical, operational and governance structures, in order to foster a consistent analysis of cross-border DeFi arrangements. Supervisory authorities are encouraged to publish analysis of DeFi arrangements and the broader DeFi ecosystem in line with the relevant information sharing and privacy regulations.

73. Finally, private sector entities should share information among themselves across borders, in accordance with applicable information-sharing frameworks, to better identify and disrupt illicit flows within the DeFi ecosystem. Certain financial institutions or VASPs may have access to unique and valuable data, both on emerging patterns of misuse of DeFi arrangements and on persons that control or exercise sufficient influence over DeFi arrangements, that may not be available to regulated entities in other jurisdictions. The timely cross-border sharing of such non-proprietary information can enhance the ability of global compliance teams to detect risks and strengthen their ML/TF mitigation measures.

---

[59] FR14/23 Final Report with Policy Recommendations for Decentralized Finance (DeFi)

[60] Organization and Structure - Egmont Group

[61] 'Next-Generation' FIU.net - European Commission

© FATF-OECD 2026

7.2. Cross-border investigations

74. **Cross-border co-operation between LEAs**: Given the borderless nature of DeFi and the lack of geographic restrictions, cross-border co-operation between LEAs is essential. The use of traditional mechanisms such as Mutual Legal Assistance (MLA) is essential for evidence gathering, but their standard processing timelines may sometimes not fully align with the instantaneous nature of decentralised value transfers. To complement these formal channels and address the critical urgency of active investigations, jurisdictions are encouraged to establish expedited, secure frameworks for the immediate sharing of advanced blockchain analytics intelligence among FIUs and cybercrime divisions. This rapid exchange is critical to successfully trace multi-hop transactions before the investigation goes cold and traditional mechanisms can complement the investigation with additional evidence.

Box 13. United States: The Samourai case

In November 2025, the U.S. Department of Justice sentenced Keonne Rodriguez and William Lonergan Hill, the co-founders of Samourai Wallet, a DeFi mixer that facilitated over USD 237 million in illegal transactions. The criminal proceeds laundered through Samourai came from, among other things, drug trafficking, darknet marketplaces, cyber-intrusions, frauds, sanctioned jurisdictions, murder-for-hire schemes, and a child pornography website. Rodriguez and Hill actively promoted Samourai to criminals, including via claims that Samourai would make virtual assets "untraceable, clean" on a darknet forum. Rodriguez and Hill were sentenced to five and four years in prison, respectively, and have paid more than USD 6 million in forfeited fees.

In this case, assistance was provided by Europol, the Portuguese Judicial Police and the Icelandic Police, among others, during the investigation. Based on a U.S. MLA request, the Icelandic authorities obtained information from the server Samourai was using for its operations, which was located in Iceland, providing transaction data to U.S. law enforcement counterparts that proved critical to advancing the case. In addition, Hill was secured via a July 2024 extradition from Portugal, and the Portuguese authorities were instrumental in obtaining additional useful evidence from Hill's residence in Portugal. French authorities also provided valuable assistance through MLA channels. This case demonstrated the necessity of working with foreign partners early in complex cases to identify relevant digitised data and suspects who may often be operating across multiple jurisdictions.

Source: United States

© FATF-OECD 2026

7.3. Public-private co-operation

75. Public-Private Partnerships (PPPs) play a pivotal role in addressing ML/TF/PF risks arising from DeFi by enabling structured information sharing, joint operational analysis and a shared understanding of emerging risks and regulatory requirements between public authorities and private sector participants. Jurisdictions should, in line with their risk and context, establish appropriate communication channels to engage with DeFi arrangements, when possible, as well as with VASPs, blockchain analytics firms, and financial institutions to strengthen collaboration across the ecosystem.

76. PPPs are particularly valuable in helping authorities respond to regulatory, supervisory and enforcement challenges. They can support authorities in identifying the characteristics, governance features and control structures of DeFi arrangements as well as in developing a deeper understanding of how protocols and smart contracts are programmed and deployed. PPPs also play a key role in promoting the development and adoption of AML/CFT measures and decentralised identity solutions to strengthen user identification and reduce anonymity-related risks. In addition, they facilitate tactical information sharing, enable the development of typologies of illicit activity and emerging trends, strengthen intelligence collection and enhance incident response to hacks and exploits. Finally, PPPs can support industry standardisation initiatives, including those led by international organisations (e.g. IEEE, ISO) and industry consortia, contributing to improved security, interoperability, and compliance in the DeFi ecosystem.

Box 14. United Kingdom: Regulatory thematic workshops with the private sector to promote understanding of risks and compliance in DeFi

As part of its VA regulatory regulatory regime, the UK Financial Conduct Authority (FCA) has increased engagement with private sector stakeholders to discuss risks posed by DeFi and potential compliance tools for risk mitigation through a series of thematic workshops, involving financial institutions, VASPs, DeFi arrangements as well as compliance expertise on ML/TF/PF and technological issues.

The workshops focused not only on the current and emerging ML/TF/PF risks and relevant risk mitigation practices adopted by the industry, but also on the technology risks posed by DeFi, including vulnerabilities in open codes protocols and smart contracts that may be exploited by hackers. Through these discussions, industry participants shared their experience of the limitations of blockchain analytics and the potential for technical solutions like built-in freeze functionality at the protocol level, and the use of zero-knowledge proof-based 'Know Your Customer' checks. The workshops allowed the FCA to refresh its assessment of illicit finance risks and mitigations and reflect industry inputs into regulatory guidance.

Source: United Kingdom

© FATF-OECD 2026

Box 15. Singapore: Global Layer One (GL1)

Global Layer One (GL1) is a public-private initiative, supported by MAS, that convenes global financial institutions, VASPs, entities involved in the DeFi ecosystem and policymakers to advance asset tokenisation through open and interoperable network standards. GL1 is developing reference architectures for incorporating regulatory compliance controls directly into on-chain transaction logic. These designs aim to support compliance with relevant regulatory obligations, including AML/CFT/CPF requirements, through modular compliance components that allow different actors to perform distinct roles across the compliance value chain. The framework explores the use of verifiable credentials and identity-linked attestations that may enable AML/CFT/CPF checks to be embedded into programmable transaction conditions. This approach seeks to allow regulated participants to demonstrate compliance with applicable regulatory requirements while maintaining interoperability across jurisdictions and tokenised asset networks.

While MAS contributes to GL1, participation in or use of the framework does not in itself constitute supervisory endorsement. Regulated financial institutions remain subject to MAS' supervisory oversight, and compliance with AML/CFT/CPF obligations is evaluated holistically, taking into account a range of governance, operational, and risk management controls beyond on-chain compliance mechanisms.

Source: Singapore

Conclusion

77. DeFi has continued to grow rapidly in the past few years, and it has the potential to play an important role in the global financial system of the future. Its technological features, such as automation, composability, 24/7 availability, and cross-border reach, create both opportunities for financial innovation and substantial ML/TF/PF risks. These risks are amplified by widespread misconceptions about "decentralisation", persistent regulatory gaps, and the increasing misuse of DeFi arrangements by cybercriminals, fraudsters, professional money launderers and proliferation financing networks, including through the abuse of advanced AI tools.

78. The FATF Standards already provide the framework to address these risks, but implementation remains significantly insufficient. Most jurisdictions have not yet identified DeFi arrangements operating in their territory, have not assessed their risks, and have not applied R.15 to arrangements that qualify as VASPs. A core challenge is determining who exercises control or sufficient influence over DeFi arrangements. The report provides examples of criteria that can be used by jurisdictions to conduct a holistic determination and presents examples and case studies of control and 'sufficient influence' in practice.

79. Jurisdictions should adopt a functional, risk-based approach to identifying controllers, applying licensing/registration requirements, and supervising

© FATF-OECD 2026

DeFi arrangements. Authorities should strengthen investigative and enforcement capabilities, including blockchain analytics, operational co-operation, and public-private partnerships, to respond effectively to increasingly sophisticated DeFi-enabled illicit finance. For arrangements that are truly decentralised and fall outside the scope of the Standards, jurisdictions should leverage alternative risk-mitigation measures targeting adjacent regulatory access points such as stablecoin issuers, VASPs, and application-layer interfaces. These alternative risk-mitigation measures may be calibrated where truly decentralised arrangements implement adequate risk-mitigation measures.

80. Jurisdictions within the FATF Global Network should proactively monitor the potential growth of truly decentralised DeFi arrangements. At the same time, they should apply appropriate risk-mitigating measures to regulated entities that interact with such arrangements, as outlined in section 5.5 of this report.

81. The FATF should continue to monitor market developments and risks associated with the DeFi ecosystem, especially truly decentralised DeFi arrangements, to ensure that the FATF standards remain relevant.

82. Ultimately, effective mitigation of DeFi-related risks will require co-ordinated global action, transparent governance practices, innovative compliance solutions, and sustained engagement between regulators, law-enforcement agencies, and the private sector. Without such measures, the rapid evolution of DeFi, which has potential benefits for payments modernisation, can risk creating growing regulatory asymmetries, enabling jurisdictional arbitrage, and facilitating illicit finance at scale.

Recommendations to mitigate the risk stemming from DeFi arrangements

1.1. ***For jurisdictions***

1) Proportionate to the risk and context, conduct a risk assessment of the risks linked to the DeFi ecosystem , which may be incorporated into the national, sectoral, or industry-specific risk assessments, or into the jurisdiction's VAs and VASPs risk assessment. This assessment should identify the materiality and nature of DeFi-related ML/TF/PF risks, including the extent of domestic exposure, cross-border dimensions, and potential vulnerabilities arising from the operation, governance, and usage of DeFi arrangements.

2) Based on the risk assessment, implement proportionate mitigating measures. These may include requiring centralised DeFi arrangements and encouraging Decentralised DeFi arrangements to embed AML/CFT controls at the smart contract and/or user interface levels; requiring other entities interacting with the DeFi ecosystem, such as financial institutions and VASPs, to apply additional AML/CFT controls to mitigate risks arising from the DeFi arrangement's underlying users; and, in higher risk scenarios, where DeFi arrangements refuse to cooperate with public authorities, as a last resort, prohibiting them from operating in the territory (blacklisting).

3) Engage with industry participants, including DeFi arrangements, VASPs, blockchain-analytics companies and other service providers interacting with DeFi arrangements to identify innovative solutions and tools to enhance the implementation of effective AML/CFT controls within the DeFi ecosystem

© FATF-OECD 2026

without disproportionally hindering innovation (e.g., digital identity, embedded KYC/CDD programs).

4) Establish appropriate criteria for determining control or sufficient influence in the context of DeFi and, where such control is identified, apply AML/CFT measures to these arrangements. Conduct targeted industry outreach (including participation in relevant industry events) to ensure that centralised DeFi arrangements are aware of applicable requirements.
    - Where controllers exist but cannot be identified, and the DeFi arrangement cannot ensure that its operations comply with AML/CFT requirements, supervisors should treat it as unregulated and apply the same mitigating measures used for truly decentralised arrangements, while continuing to make enquiries and, where appropriate and possible, applying proportionate sanctions.
5) Establish clear regulatory pathways that enable regulated institutions to interact with DeFi arrangements while preserving the integrity of their AML/CFT compliance frameworks and that of the broader financial system. Regulated institutions should implement appropriate AML/CFT measures to mitigate the risks posed by DeFi arrangements and effectively apply controls to the underlying customers of such arrangements in line with Recommendations 10. These measures should be proportionate to the risks identified and take into account any mitigating measures implemented by the DeFi arrangement, such as embedded AML/CFT controls at the smart contract level or reliance on third-party AML/CFT service providers.
6) When appropriate based on risk and context, develop structured and accessible regulatory engagement mechanisms, such as pre-application meetings, innovation hubs, regulatory sandboxes, and technical workshops, to provide DeFi arrangements with clarity on compliance expectations before they enter the market.
7) Establish mechanisms to identify high-risk or non-compliant DeFi arrangements. These mechanisms may include public registries, supervisory notices, or risk-rating disclosures, which can help guide market participants, incentivise responsible behaviour, and enhance overall market integrity.
8) Enhance oversight of key off-chain infrastructure providers that serve as regulatory access points within the DeFi ecosystem, such as front-end operators, and encourage them to adopt tailored measures to hinder illicit activity.
9) Consider requiring or encouraging all types of DeFi arrangements operating within the jurisdiction to designate a responsible person for timely engagement with competent authorities, particularly in the context of law-enforcement investigations, to address the current lack of efficient co-operation mechanisms.
10) Strengthen interagency co-ordination and operational capacity for DeFi-related investigations by establishing robust mechanisms for joint analysis and rapid response, and by leveraging Public-Private Partnerships to integrate real-time blockchain analytics and advanced tracing tools.

© FATF-OECD 2026

1.2. For the private sector

For DeFi arrangements

11) Centralised DeFi arrangements and those that are centralised in practice, but where controllers cannot be readily identified, should fully comply with the requirements of Recommendation 15.

12) Centralised DeFi arrangements should prioritise investment in the development of innovative tools that enable the effective implementation of AML/CFT measures and strengthen technological capacities to support the prompt identification, seizing, and freezing of illicit assets.

13) DeFi arrangements that are truly decentralised and fall outside the scope of the FATF Standards are encouraged to understand their ML/TF risks and to integrate proportionate AML/CFT controls into their operational frameworks, as appropriate, in order to support the overall integrity of the financial system.

14) All DeFi arrangements should:

    i. Collaborate to the greatest extent possible with competent authorities in the context of AML/CFT investigations and designate a dedicated point of contact (PoC) to maintain formal communication channels with law enforcement authorities and FIUs. The PoC may be the controller of the DeFi arrangement in centralised DeFi arrangements, or the persons responsible for the creation of the arrangement in truly decentralised DeFi arrangements (e.g., developers).

    ii. Draft and make readily available to competent authorities documentation that clearly sets out the control and decision-making structures within the DeFi arrangement. Such documentation should identify the persons exercising operational influence, governance authority, or protocol-level controls. It should also include contact points for competent authorities.

        - For DeFi arrangements that are truly decentralised, the persons responsible for the creation of the arrangement should also be responsible for explaining the governance and operational model, including the features that substantiate claims of decentralisation.

    iii. Conduct regular audits related to protocol cybersecurity and ensure ongoing monitoring of suspicious trends and potential exploits to better prevent theft and abuse by illicit actors.

For Financial Institutions and VASPs

15) Implement Recommendation 13 when establishing business relationships with centralised DeFi arrangements and those that are centralised in practice, but where controllers cannot be readily identified. Where controllers cannot ultimately be identified, after all reasonable avenues have been explored, apply the same risk mitigating measures as those applicable to truly decentralised DeFi arrangements.

16) Interact with DeFi arrangements that are not subject to regulation in line with appropriate AML/CFT measures to mitigate risks arising from their

© FATF-OECD 2026

customers, including customer due diligence (e.g. verification of the identity of underlying customers) and ongoing monitoring of the integrity and security of the protocol.

17) Share information with other private sector entities, including across jurisdictions, to improve the identification and disruption of illicit flows within the DeFi ecosystem, in compliance with applicable legal and regulatory frameworks.

Annex A: Overview of FATF work on VAs and VASPs

2018	• Recommendation 15 amended including addition of new definitions "virtual asset" and "virtual asset service provider".
2019	• Adoption of Interpretive Note to R.15 • Creation of the FATF Virtual Assets Contact Group (VACG) • Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021)
2020	• 12 month review of the new FATF Standards: 1st12-month review • Report to the G20: FATF Report to the G20 on So-called Stablecoins • Risk indicators: List of Red Flag Indicators of ML/TF through VAs
2021	• Updated guidance[62]: Updated Guidance for a Risk-Based Approach to VA and VASPs • 24 month review of the FATF Standards: 2nd12-month review
2022	• Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2023	• Report on ransomware, with focus on VA risks and trends: Countering Ransomware Financing • Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2024	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity
2025	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity • Best Practices in Travel Rule Supervision • Quick guide on assessing the Money Laundering risks of virtual assets (VA) and virtual asset service providers (VASP)
2026	• Targeted report on Stablecoins and Unhosted Wallets - Peer-to-Peer Transactions • Understanding and Mitigating the Risks of Off-shore Virtual Asset Service Providers • 7th Targeted Update on the Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers

[62] The 2021 updated Guidance included updates focusing on the following six key areas: clarification of the definitions of VAs and VASPs; guidance on how the FATF Standards apply to stablecoins; additional guidance on the risks and the tools available to jurisdictions to address the ML/TF risks for peer-to-peer transactions; updated guidance on the licensing and registration of VASPs; additional guidance for the public and private sectors on the implementation of the Travel Rule; and principles of information-sharing and co-operation amongst VASP supervisors.

© FATF-OECD 2026

July 2026

www.fatf-gafi.org