MFSA MALTA FINANCIAL SERVICES AUTHORITY

Decentralised Finance (DeFi)

Discussion Paper

Strengthening Malta's Position as a Jurisdiction for Next Generation Financial Services

Date: 12 June 2026
Ref No: 03-2026
Closing Date: 10 July 2026

Table of Contents

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

Table of Abbreviations

AA	Account Abstraction
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
AMLR	Anti-Money Laundering Regulation(s)
ART / ARTs	Asset-Referenced Token(s)
BIS	Bank for International Settlements
CASP / CASPs	Crypto-Asset Service Provider(s)
CeFi	Centralised Finance
DAO / DAOs	Decentralised Autonomous Organisation(s)
DEX / DEXs	Decentralised Exchange(s)
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
DORA	Digital Operational Resilience Act
EOA / EOAs	Externally Owned Account(s)
EMT / EMTs	Electronic Money Token(s)
ESMA	European Securities and Markets Authority
EU	European Union
IOSCO	International Organization of Securities Commissions
Layer 2 / L2	Layer 2 (Blockchain Scaling Solutions)
MFSA	Malta Financial Services Authority
MiCA	Markets in Crypto-Assets Regulation - Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance)
MiFID II	Markets in Financial Instruments Directive II
MTF	Multilateral Trading Facility

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

PSD2	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)
SCC / SCCs	Segregated Cell Company / Companies
SCA / SCAs	Smart Contract Account(s)
TFR	Transfer of Funds Regulation
VFA	Virtual Financial Assets (Act / regime)

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

1 Introduction

1.1 Background

Malta was among the first jurisdictions to establish a comprehensive regulatory framework for the crypto-asset sector. In 2018, the enactment of the Virtual Financial Assets Act, the Malta Digital Innovation Authority Act, and the Innovative Technology Arrangements and Services Act provided legal certainty for activities that had previously operated in a regulatory vacuum, while reflecting a policy commitment to investor protection, market integrity, and financial stability alongside innovation.

This early regulatory engagement has given Malta significant supervisory experience in the crypto-asset space and has supported a smooth transition from the domestic VFA regime to the European Union's Markets in Crypto-Assets Regulation (MiCA), which entered into force on 30 December 2024. MiCA excludes crypto-asset services that are provided in a fully decentralised manner, without any intermediary, from its scope[1].

Decentralised Finance ("DeFi") seeks to provide financial services using distributed ledger technologies in a decentralised manner without the involvement of traditional financial intermediaries[2], typically using smart contracts[3]. DeFi applications facilitate activities such as trading, lending, borrowing, and risk-sharing, replicating functions of the traditional financial system, albeit through a decentralised protocol structure. This type of service provision introduces distinct risks and challenges not currently contemplated by established regulatory approaches, particularly due to the lack of intermediaries that would typically act as regulatory "entry points"[4].

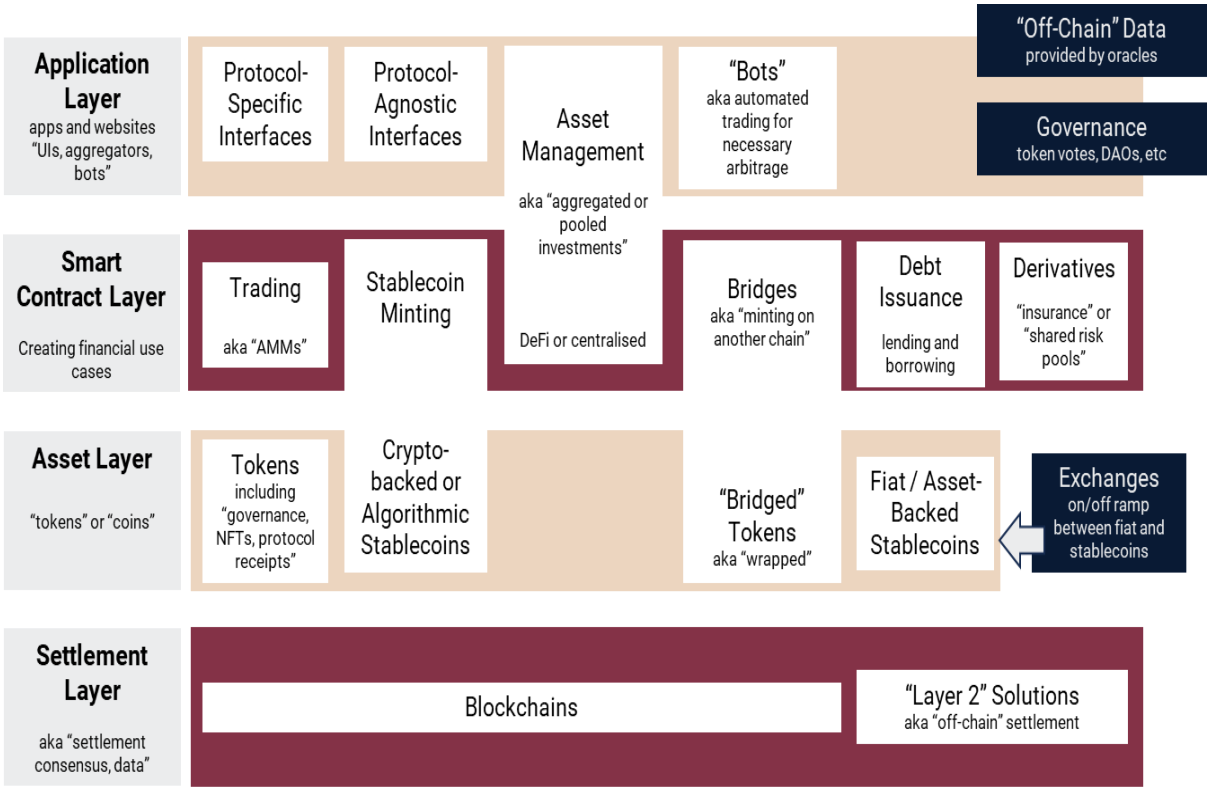
For the purposes of this discussion paper, the DeFi ecosystem is viewed as a layered technology stack comprising four interrelated layers, supported by external, off-chain inputs as illustrated in *Figure 1.1* hereunder. The **settlement layer** consists of blockchains and Layer 2 solutions that record transactions and enable the transfer

[1] MiCA – Recital 22
[2] ESMA TRV Risk Analysis, 2023. Decentralised Finance in the EU: Developments and risks.
[3] Self-executing codes deployed on a blockchain.
[4] Decentralised finance – a new unregulated non-bank system? Published as part of the ECB Macroprudential Bulletin 18, July 2022.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

of crypto-assets. The **asset layer** comprises the crypto-assets created and used within DeFi systems, including tokens and stablecoins. The **smart contract layer** provides the core operating functionality by encoding rules that govern activities such as trading and lending. The **application layer** consists of user-facing interfaces and tools that facilitate access to DeFi protocols and may be hosted off-chain. Across these layers, DeFi systems also rely on **external, off-chain inputs**, including data feeds from oracles and governance mechanisms such as token-based voting or decentralised autonomous organisations. While not always recorded on-chain, these external, off-chain inputs can be critical to protocol operation and associated risk.

Figure 1.1: The Building Blocks of DeFi



Source: IOSCO DeFi Report – March 2022.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

1.2 Scope

This Discussion Paper sets out a high-level overview of decentralised finance (DeFi), together with a focused consideration of selected areas of potential regulatory relevance. **It does not set out the MFSA's policy position on DeFi; rather, it is intended to stimulate informed dialogue with stakeholders across the public and private sectors, with a view to supporting the development of a proportionate and balanced regulatory approach.**

It is emphasised that the Proposals set out in this Discussion Paper are not binding and are subject to further internal assessment and analysis. Such assessment will be undertaken by the Authority following receipt of stakeholder feedback. It is important that participants in the consultation and broader discussion exercise take these considerations into account.

The Authority notes that certain themes addressed in this Discussion Paper overlap with matters currently being considered by the European Commission in its targeted consultation on the review of MiCA[5]. While this Discussion Paper is intended to support the MFSA's supervisory and policy assessment of DeFi-related developments within the Maltese context, stakeholders are encouraged to engage actively with the European Commission's consultation exercise.

[5] European Commission's targeted consultation on the review of regulation on the MARKETS IN CRYPTO-ASSETS (MICA), link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2 MiCA Implications for Decentralised Finance

The Markets in Crypto-Assets (MiCA) Regulation establishes a uniform legal framework for crypto-assets that were previously unregulated at EU level. MiCA applies to issuers of crypto-assets and to Crypto-Asset Service Providers ('CASPs'), i.e. entities offering services such as custody, exchange, trading platforms, portfolio management, and advisory in relation to crypto-assets. However, MiCA does not apply to crypto-assets that qualify as financial instruments under MiFID II, nor to activities already covered by other EU legislation such as PSD2 for payment services or the Electronic Money Directive for e-money. MiCA also excludes central bank digital currencies (CBDCs), crypto-assets issued by public authorities, and unique non-fungible tokens (NFTs). Stablecoins, including asset-referenced tokens (ARTs) and e-money tokens (EMTs), fall under MiCA but are subject to stricter requirements compared to the general rules for other crypto-assets. The key aims of MiCA are to ensure market integrity, investor protection and financial stability through transparency, disclosures and authorisation requirements for issuers and CASPs.

Under MiCA, crypto-assets are defined broadly as electronic representations of value or rights that are transferable and storable on Distributed Ledger Technology ('DLT').

MiCA categorises crypto-assets into three main groups[6]:

- **Electronic Money Tokens (EMTs):** crypto-assets that purport to maintain a stable value by referencing the value of a single official currency[7];
- **Asset-Referenced Tokens (ARTs):** crypto-assets that are not EMTs and that purport to maintain a stable value by referencing another value or right, or a combination thereof, including one or more official currencies[8].
- **Other Crypto-Assets:** crypto-assets other than EMTs and ARTs. This category covers a wide variety of crypto-assets, including utility tokens and

[6] MiCA – Recital 18
[7] MiCA – Article 3(7)
[8] MiCA – Article 3(6)

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

other digital tokens not covered by EMT/ART definitions (provided they are not MiFID financial instruments)[9].

2.1 Use or incorporation of decentralised products and services by in-scope providers

The Markets in Crypto-Assets (MiCA) Regulation recognises that fully decentralised structures generally fall outside its regulatory perimeter. However, where an authorised CASP integrates decentralised components into the delivery of its services, those components become part of the CASP's regulated activity[10]. As noted in Recital 22 of the Regulation:

"This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation….[11]"

Consequently, the CASP remains responsible for compliance obligations in relation to those features, even if it does not exercise direct technical control over them.

It is reasonable to expect that such decentralised components may operate on a fully autonomous basis and may therefore present inherent risks that the CASP cannot fully mitigate, given its lack of control over them. Whilst CASPs may retain control over their own centralised services, their interaction with decentralised protocols introduces challenges in particular where certain MiCA obligations, such as risk management, operational resilience, and consumer protection, may not be technically enforceable to the same extent across decentralised features.

[9] MiCA – Recital 18
[10] "This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation.....Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation." - MiCA - Recital 22.
[11] MiCA – Recital 22.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

In essence, the establishment of clear governance mechanisms may be difficult to reconcile with the principles of decentralisation, while compliance with MiCA standards and implementation of appropriate monitoring systems for the decentralised aspects of the service may require further clarifications of expectations and, potentially, a degree of regulatory adaptation.

Q1. What challenges are presented in the application of MiCA requirements to services incorporating decentralised components?

Q2. Should CASPs be required to conduct technical and operational due diligence on decentralised systems they integrate (e.g., smart contract audits, governance review, risk assessments)?

Q3. Should the use of certain decentralised protocols be considered incompatible with specific MiCA obligations (e.g., consumer protection, continuity of service)? If so, which ones?

2.2 MiCA - Scope

MiCA excludes fully decentralised models from its regulatory scope, meaning that projects without intermediaries or central control may not need to comply with MiCA. As aforestated, *Recital 22* states that crypto-asset services performed *"in a fully decentralised manner without any intermediary"* should fall outside the scope of MiCA. In essence, services operating on a *truly* decentralised protocol (with no entity in control) are excluded from the Regulation's scope.

However, the determination of whether a DeFi arrangement may be regarded as "fully decentralised" is likely to depend on a case-by-case assessment of the relevant protocol's governance, operational, and control features. ESMA's consultation paper[12] notes that whilst "fully decentralised" DEXs[13] should fall outside MiCA's remit, the scope of this exemption remains unclear and requires a detailed assessment of each system's features. In this regard, the Commission's recent targeted consultation on the review of MiCA highlights a number of indicators that

[12] Section 108 of ESMA's Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper, link.

[13] A decentralised exchange (or DEX) is a peer-to-peer marketplace where transactions occur directly between crypto traders.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

may be relevant in assessing the absence of a full decentralisation. These include:

- The existence of an identifiable intermediary providing a crypto-asset service;
- Presence of control by an identifiable person or group of persons (e.g. via admin keys) over the key functionalities of a DeFi protocol (e.g. upgradeability of protocol);
- Significant concentration of governance power over the key functionalities of a DeFi protocol;
- Custody of user assets by the DeFi protocol;
- The absence of open-source code; and
- The marketing of a DeFi protocol by an identifiable entity or person.

In practice, most systems retain some features that could be considered centralised, even where the protocol is decentralised.

Q4. How should "fully decentralised" be defined for regulatory purposes? Which criteria (technical e.g., protocol architecture, governance e.g., voting power distribution, operational e.g. upgrade mechanisms) should be considered essential?

Q5. Should decentralisation be treated as a spectrum rather than a binary concept? Where would there be value in in developing a harmonised, standardised methodology or scoring framework to assess the degree of decentralisation across systems?

Q6. Which indicators should regulators treat as evidence of continuing central control? (E.g., administrator keys, governance concentration, upgrade rights, or development teams exercising effective influence) Are there others?

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Q7. Should the MFSA issue guidance on assessing decentralisation? If yes, what should such guidance cover (e.g. criteria, scoring methodology, disclosure requirements)?

Stakeholders are also encouraged to consider and respond to the questions raised by the European Commission in its targeted consultation on the review of MiCA, particularly those relating to the assessment of decentralisation and the evolving regulatory treatment of DeFi arrangements.

2.3 Financial Crime Risks and International Standards

In parallel with the regulatory framework established under MiCA, due consideration must be given to international anti-money laundering and counter-terrorist financing (AML/CFT) standards developed by the Financial Action Task Force (FATF). The FATF has consistently emphasised that DeFi arrangements performing functions equivalent to regulated financial services should not fall outside the scope of regulation solely by virtue of their technological architecture. This reflects the FATF's "same risk, same rule" principle, under which persons or entities exercising control or sufficient influence over DeFi protocols may be characterised as Virtual Asset Service Providers (VASPs) and, accordingly, be subject to AML/CFT obligations[14].

DeFi ecosystems may present heightened exposure to financial crime risks due to their global accessibility, pseudonymous participation, and the potential absence of clearly identifiable intermediaries. Key risk vectors include:

- **Money laundering and terrorist financing (ML/TF):** illicit actors may exploit the composability of DeFi protocols to layer transactions across multiple platforms, thereby obscuring the origin and movement of funds;
- **Stablecoin-related risks:** the increasing integration of stablecoins within DeFi has been associated with sanctions evasion and cross-border illicit finance;

[14] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

- **Fraud and market abuse:** practices such as "rug pulls", governance manipulation, and opportunistic liquidity extraction remain prevalent within certain segments of the ecosystem; and
- **Unhosted wallets:** peer-to-peer (P2P) transactions conducted via unhosted wallets may bypass regulated on- and off-ramps, creating challenges for traceability, customer due diligence, and supervisory oversight.

A recent report[15] by the FATF further underscores these risks, highlighting the growing role of stablecoins in illicit finance. As of mid-2025, the stablecoin market exceeded USD 300 billion in capitalisation, with over 250 instruments in circulation. Notably, stablecoins were estimated to account for approximately 84% of illicit virtual asset transaction volume in 2025[16], frequently involving unhosted wallets and sophisticated laundering techniques designed to obscure the origin of funds. The same characteristics that support legitimate use (namely price stability, liquidity, and interoperability) also render stablecoins attractive for misuse by money launderers, terrorist financiers, and state-linked cyber actors adopting stablecoins as a preferred method for laundering proceeds from ransomware, phishing, and other cyber-enabled crimes.

Accordingly, any assessment of DeFi under MiCA should be complemented by an evaluation of AML/CFT exposure, including the extent to which existing international standards may apply to participants within the arrangement, based on both formal roles and their effective control or influence.

Q8. What targeted measures could be adopted to address specific financial crime risks in DeFi (such as the use of stablecoins for illicit finance, transaction layering across protocols, and fraud schemes like "rug pulls") whilst preserving the benefits of decentralisation and innovation within the ecosystem?

[15] FATF (2026), Targeted Report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions, FATF, France, link.
[16] The Chainalysis 2026 Crypto Crime Report; link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

3 Software-based Organisational Models

Distributed ledger technology and autonomous software systems are reshaping how organisational structures are formed, governed, and operated. Among the most prominent manifestations of this evolution are Decentralised Autonomous Organisations (DAOs)[17], which are software-based organisational structures in which governance arrangements, operational rules, and certain decision-making processes are embedded in code and executed, in whole or in part, through distributed ledger infrastructure.

DAOs typically utilise smart contracts to automate organisational processes, allocate rights and responsibilities, and facilitate collective decision-making, often through token-based governance mechanisms. Unlike traditional corporate structures, DAOs may operate without conventional boards, management hierarchies, or centralised legal ownership. In practice, however, many DAO arrangements continue to exhibit varying degrees of human coordination, governance concentration, operational centralisation, or reliance on identifiable development teams, treasury managers, front-end operators, or other influential actors.

DAO-type structures are increasingly used across multiple sectors, particularly in digital finance, where they support:

- **Protocol governance arrangements**, which enable token holders to vote on key decisions, such as protocol upgrades, fee structures, interest rates, collateral types and the strategic direction of software protocols. These arrangements can support transparent and community-led governance for lending, trading, and yield platforms such as Aave[18], Uniswap[19] and MakerDAO[20];

[17] Reference may be made to the various publications authored by Dr Max Ganado, Consultant, Ganado Advocates. Dr Ganado has written extensively about these structures and how they may potentially be introduced within the Maltese legal framework.

[18] Aave is a major decentralised lending platform, which enables users to lend and borrow major assets. The token holders govern platform decisions, such as the addition of new assets and the management of platform parameters, e.g. collateralisation ratios.

[19] Uniswap is the largest decentralised exchange on the Ethereum blockchain. The platform launched its token, UNI, in November 2018 and UNI holders can vote or delegate votes that control the protocol's direction, fees and treasury.

[20] Maker is one of the original DAOs in the DeFi ecosystem. As the governance mechanism for the DAI stablecoin (DAI), Maker utilises a DAO framework to vote on aspects such as adjusting the interest rate or the stability fee.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

- **Collective investment and treasury structures**, enabling pooled funds from participants to make venture capital-style investments (e.g. investments in assets such as startups, tokens, or NFTs). Investment decisions are made through participant voting, providing a decentralised alternative to traditional venture capital. Examples include LAO[21] and MetaCartel Ventures;

- **Grant and ecosystem funding structures**, designed to fund open-source projects or other ventures that support the DeFi ecosystem development. Funding decisions are made collectively by DAO participants, promoting transparency and community alignment. Gitcoin[22] DAO is a leading example in the Web3 space.

Notwithstanding their growing prominence, DAOs may be viewed as only one manifestation of a broader class of software-based organisational forms in which software performs material governance, operational, or administrative functions[23]. This wider category may encompass decentralised organisations, tokenised governance structures, hybrid centralised/decentralised enterprises, and autonomous AI-enabled systems. **This suggests that legislative focus may more appropriately be directed toward software-based organisations as a broader legal concept rather than DAOs as a standalone category.**

Accordingly, consideration may be given to whether Maltese law should recognise a broader legal category for **software-based organisational arrangements**, referred to for discussion purposes as **Software-based Organisations ("SBOs")**.

Such a framework would recognise that certain organisational arrangements derive their structure, governance, operational processes, or decision-making architecture materially from software systems, including smart contracts, autonomous code, algorithmic governance mechanisms, or other digital infrastructures. In this respect, academic and policy literature[24] increasingly recognises that software-enabled

[21] The LAO (limited liability autonomous organisation) is structured as a member-directed venture capital fund in the United States. It is registered as a Delaware limited liability company (LLC) and carries out its functions via a DApp and smart contracts.

[22] Gitcoin is an independent platform that funds developers and builders that create opensource applications. Donors can browse projects listed on the platform and choose what they would like to fund. The DAO's governance token, GTC, is used to manage its treasury, grants and disputes.

[23] See UK Law Commission, *Decentralised Autonomous Organisations – Scoping Paper* (11 July 2024), noting that the term "DAO" does not denote a single, clearly defined organisational form and may encompass a broad spectrum of arrangements.

[24] *Foundations of Decentralized Organizations: Blockchain and the Future of Corporate Law* (2026; online edn, Oxford Law Pro), https://doi.org/10.1093/law/9780198946113.001.0001, accessed 24 Apr. 2026. It notes that "DAOs thus have an

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

arrangements may possess a genuine organisational character and should not necessarily be regarded as existing outside conventional legal frameworks merely because their governance is technologically mediated. Legal recognition would therefore derive not from the type of software deployed, but from the extent to which software performs substantive organisational functions warranting an appropriate legal, governance, and accountability framework.

Under such a framework:

- DAOs may be recognised as one category of **Software-based Organisation,** rather than requiring treatment as a standalone legal concept**;**

- **the organisational layer**, i.e. the legal structure through which the software-enabled enterprise is constituted, could address matters of legal personality, governance, registration, accountability, transparency, accounting, continuity, dissolution, and winding-up, thereby establishing clear baseline expectations regarding organisational conduct and responsibility; and

- **the operational software layer**, i.e. the software application, protocol, autonomous system, or digital infrastructure through which services are delivered, would remain subject to applicable sector-specific regulation depending on the function performed, including financial services regulation, AI governance requirements, cybersecurity obligations, consumer protection standards, or other applicable regulatory frameworks.

By distinguishing between organisational constitution and operational execution, such a framework may also facilitate clearer attribution of regulatory responsibilities and legal accountability, an increasingly important consideration in digital finance, where governance opacity, distributed participation, and operational automation can complicate supervisory oversight, liability allocation, and prudential accountability.

The option to establish as a software-based organisation could initially be limited to entities engaged in financial services activities, with the legislative framework designed to allow for its future extension to other sectors.

organizational character. They are more than informal projects and their disavowal of established legal organizational forms does not mean that they exist in a legal vacuum."

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Q9. ***What software-based organisational models are currently emerging in practice (such as DAOs, protocol-governed structures, AI-enabled autonomous systems, tokenised governance entities, or hybrid software enterprises) and to what extent would these models benefit from recognition under a dedicated Software-governed Organisation framework?***

Q10. ***How should regulatory accountability be allocated/structured within Software-governed Organisations where governance, operational execution, or decision-making may be distributed across software protocols, developers, token holders, operators, autonomous agents, or other participants?***

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

4 Segregated Cell Companies (SCCs) in the Context of DeFi

Segregated Cell Companies (SCCs) are corporate structures that permit the creation of multiple internally segregated "cells" within a single legal entity. Each cell maintains its own ring-fenced assets and liabilities which are statutorily and operationally protected from the risks or obligations of other cells and the core entity. Typically used in insurance, investment funds, and structured finance, such vehicles are now attracting attention within the crypto-asset and decentralised finance (DeFi) ecosystem.

The consideration of SCC structures within the context of DeFi reflects, in part, that many DeFi projects are characterised by significant operational centralisation, even where certain technical elements are decentralised. Governance keys, protocol upgrade mechanisms, treasury management, and control over user-facing interfaces are often retained by identifiable persons or entities. As a result, DeFi projects seeking clearer allocation of rights and liabilities, legal structuring of risk, or alignment with regulatory expectations may consider SCC-type structures as a means of complementing their technical modularity with a robust legal framework.

Q11. Should a framework for SCCs in the context of DeFi be introduced under the Maltese legislative framework?

4.1 SCC Model Overview and Its Relevance to DeFi

At its core, an SCC consists of a single incorporated entity hosting multiple internal cells, each with its own statutorily separated balance sheet. For DeFi operators, whose protocols often comprise several interconnected modules, this structure can offer a legal solution that aligns with the modular architecture of on-chain ecosystems. Many DeFi systems operate as complex, interdependent systems of smart contracts, where risks in one module can propagate into another unless clear legal or technical boundaries are established. Whilst legal segregation cannot substitute technical isolation, cell-level separation within an SCC can help provide a clearer mechanism for distinguishing between different operational layers, particularly where those layers entail distinct governance, disclosure, or compliance obligations.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

In cases where DeFi activities are not fully decentralised and identifiable persons retain influence or operational control, SCCs offer a practical means to allocate functions and accountability, ring-fence risks, and delineate supervisory responsibilities provided that each cell's activities can be separately scoped, controlled and evidenced. A single DeFi organisation could assign each functional or economic component of the ecosystem to a dedicated cell, broadly reflecting the isolation of smart-contract modules on-chain. For instance, where a project undertakes multiple activities such as token issuance, automated market making, cross-chain operations, or provision of interfaces, SCCs may allow each to be situated within a cell with its own operational procedures and compliance responsibilities. This approach can help differentiate regulated activities from non-regulated features and enable more granular governance and audit processes, provided that inter-cell dependencies, shared resources, and consolidated-level obligations are appropriately identified and managed.

Q12. To what extent are SCCs currently being considered or utilised by DeFi operators as an organisational mechanism for managing discrete lines of activity or treasury resources? Please identify any observed use cases, barriers to adoption, or jurisdictional considerations.

Q13. Which DeFi operations or functions do you consider most suitable for structuring at cell-level within an SCC?

4.2 Contagion Mitigation and Containment of Smart-Contract Failures

DeFi offers services that are economically comparable to those provided by traditional finance and is therefore exposed to analogous financial stability vulnerabilities. The core mechanisms giving rise to these vulnerabilities (such as leverage, liquidity mismatches and their interaction through profit-seeking and risk-management practices) are well-documented in the established financial system[25]. Furthermore, DeFi protocols may be interdependent[26] such that a failure in one

[25] DeFi risks and the decentralisation illusion, Bank for International Settlements (BIS) Quarterly Review, December 2021, link.
[26] DeFi composability is the ability of different decentralised finance protocols and applications to interact with and build upon one another. This allows developers to stack, combine, and integrate existing services to create more complex financial products and services without starting from scratch.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

module (e.g. a bridge compromise that drains liquidity, flaws in token mechanics, an oracle malfunction) can propagate across multiple interconnected protocols or user positions.

By confining each activity to distinct cells, SCC structures may act as a legal and balance-sheet containment mechanism, helping to ensure that liabilities arising from a malfunction in one protocol-related activity does not automatically affect other services hosted by the entity. While such legal segregation, which may be viewed as a 'circuit breaker', cannot prevent on-chain technical contagion, it may limit off-chain legal and financial spillovers, particularly where a DeFi ecosystem appears unified to the user perspective but internally relies on several risk-critical smart contracts, operational components, or governance functions.

Q14. To what extent could SCC-based legal and balance-sheet segregation, when combined with DeFi's modular and composable architecture, contribute to limiting off-chain financial and legal spillovers arising from failures in individual protocol components?

Q15. Which types of DeFi failure scenarios do you consider most amenable to mitigation through cell-level segregation within an SCC structure?

4.3 Governance, Regulatory Attribution, and Interaction with MiCA

Under MiCA, persons who provide crypto-asset services "on a professional basis"[27],generally fall within the scope of a Crypto-Asset Services Provider (CASP). MiCA takes a functional approach. Where identifiable natural or legal persons provide, control or materially influence the provision of crypto-asset services, they may be treated as within scope[28]. In the context of decentralised finance (DeFi), automation via smart contracts does not necessarily eliminate the presence of identifiable responsible persons. Even where protocol execution is autonomous, operational levers such as key management, parameter modification rights, treasury deployment, fee-setting, or control over user-facing interfaces often remain vested in specific individuals or concentrated governance holders. The International

[27] MiCA – Recital 21
[28] MiCA – Recital 22

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Organization of Securities Commissions (IOSCO) has also noted that such retained influence over critical functions may amount to *de facto* control and may therefore trigger regulatory responsibility notwithstanding claims of technological decentralisation or protocol autonomy.[29]

The Segregated Cell Company (SCC) framework offers a structure to transparently allocate responsibility for these functions. By placing discrete operational components of a DeFi ecosystem such as token issuance, liquidity management, bridging, oracle provisioning, custody, or order routing, within a dedicated cell, an SCC can enable explicit governance mapping and clearer attribution of regulatory obligations. This can help supervisors determine which individuals or entities within the SCC's governance arrangements exercise meaningful control over a given service and therefore could qualify as CASPs. Governance arrangements can be defined at cell level, including decision-making rights, accountability structures, and documented interfaces with decentralised or community-driven processes.

The SCC model may also streamline compliance with MiCA's differentiated requirements. When a cell carries out an activity listed in Article 3(1)(16) of MiCA, such as custody, transfer, exchange, or order transmission, the cell (or the SCC as a whole) may require authorisation. Separating activities through cells can ensure that compliance obligations (e.g., own-fund requirements, risk management, safeguarding of client assets, disclosure obligations) attach specifically to the cell performing the regulated function, rather than being diluted across the entire structure. However, prudential, conduct and safeguarding obligations are imposed on the authorised entity. Internal cell delineation should be reflected in governance, risk and control documentation but does not replace entity-level accountability. This compartmentalisation may therefore improve clarity and proportionality in implementation whilst providing supervisors with a clearer view of risk concentration.

Further, cell-level structuring may support compliance with related frameworks such as the Transfer of Funds Regulation (TFR) for AML/CFT travel-rule obligations[30], and operational-resilience expectations under the Digital Operational Resilience Act

[29] IOSCO, *Decentralized Finance (DeFi) Report* (2022), Box 1 "Decentralization" (noting that DeFi protocols frequently retain centralised influence or decision-making power despite decentralisation claims), link.
[30] FATF (2012-2025), International Standards on Combating Money Laundering and Financing of Terrorism & Proliferation, FATF, Paris, France, link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

(DORA). By isolating riskier or more centralised functions in specific cells, operators can target safeguards in a proportionate manner, whilst providing transparent disclosure to users regarding which parts of a protocol fall under regulated oversight.

However, using an SCC structure may affect a project's ability to rely on claims of decentralisation. The existence of a central entity, delineated governance bodies, and cell-specific operational control could be interpreted as evidence of centralisation, thus potentially reducing eligibility for any decentralisation-based exclusions contemplated under MiCA.

Q16. To what extent can SCC-based structuring improve governance clarity, auditability, and regulatory attribution in complex or multi-module DeFi ecosystems?

Q17. Should MiCA authorisation and supervisory oversight apply at the SCC (entity) level, with cell-level responsibilities reflected in the operational model, or should certain high-risk cells be subject to explicit, cell-specific conditions or approvals? What criteria should determine this allocation? (e.g. nature of the crypto-asset service, client-asset exposure/custody, leverage or liquidity risk, oracle/bridge dependence, cross-cell interdependencies?)

Q18. Could the use of SCCs inadvertently weaken legitimate decentralisation characteristics, and if so, how should regulators evaluate this trade-off?

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

5 Guardian Agents[31]

Decentralised Finance (DeFi) challenges the foundational assumptions of financial regulation by disaggregating functions traditionally performed by licensed intermediaries and reallocating them to software, incentives, and distributed governance arrangements. Whilst this architecture can reduce reliance on centralised institutions, it does not eliminate the need for oversight, risk containment, or accountability. Instead, these functions are re-embedded within the protocol architecture itself, often through a combination of automated rules, governance mechanisms, and constrained human intervention.

Guardian Agents may represent one such embedded mechanism and are increasingly relevant to regulators seeking to understand how control, responsibility, and intervention operate in DeFi ecosystems, particularly where protocols are designed to operate without continuous human discretion.

In this context, Guardian Agents can be understood as protocol-level mechanisms, whether fully automated, semi-automated or subject to tightly constrained human activation, that are designed to monitor, evaluate, and constrain the behaviour of other autonomous systems to ensure compliance with predefined objectives and risk tolerances. They do not exercise open-ended discretion but rather apply pre-defined parameters to trigger corrective or protective actions, such as pausing certain functions, imposing limits, or activating fail-safe responses.

From a regulatory perspective, Guardian Agents are strategically important because they provide insight into how DeFi protocols internalise risk management, contingency planning, and crisis response without the direct involvement of the regulator. Understanding Guardian Agents is therefore essential not only for evaluating protocol resilience, but also for assessing whether DeFi systems can produce outcomes functionally analogous to those pursued by regulation, such as consumer protection, market integrity, financial crime compliance and financial stability.

[31] Reference may be made to: Gauci, Ian, Rethinking DeFi Regulation: A Functional Model for Supervisory Design Under EU Law (July 05, 2025).

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Q19. To what extent can Guardian Agents be considered functional equivalents of certain regulated financial safeguards? (e.g. risk limits, circuit breakers, fail-safe mechanisms), and what material limitations should regulators consider when assessing such equivalence?)

Q20. (a) Should the presence, design, and effectiveness of Guardian Agents influence a regulator's assessment of DeFi-related operational, contagion, or systemic risk? If so, how should such mechanisms be evaluated in practice?

(b) Should guidance be developed to outline best-practice design principles for Guardian Agents (e.g. transparency, auditability), and if so, should such guidance be purely descriptive or incorporated in supervisory risk assessments?

5.1 Roles, Scope, and Constraints of Guardian Agents

From a regulatory perspective, the defining characteristic of Guardian Agents is not merely that they exist, but how their authority is designed, governed and constrained. In DeFi protocols, guardians may hold powers ranging from runtime monitoring and alerting to emergency contract suspension, rate-limiting or throttling, parameter adjustment or oracle substitution. These powers are typically justified as necessary for rapid response to exploits, market dislocations, or unforeseen interactions between protocols - risks that are magnified in highly composable DeFi environments. In line with McMullen's framing of "guardian agents", such mechanisms can evolve across phases, from quality control (*ex-post* output checks), to observation (explainability and continuous supervision), and ultimately to protection roles based on pre-defined, bounded interventions when exceptional conditions are met.[32] This highlights that guardians can, depending on their design, hold **active intervention authority** beyond passive monitoring.

The scope of guardian authority directly affects the risk profile of a DeFi system. Narrowly scoped guardianship may be insufficient to contain cascading technical or

[32] Meet Your Guardian Agent Overseeing AI by Leigh McMullen, link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

economic failures, whilst broadly scoped authority may amount to effective control over a critical function without corresponding accountability. The constraints on guardian authority are therefore particularly relevant. Many protocols present guardianship as transitional, with powers expected to diminish over time as systems mature. Others retain permanent guardianship as a safeguard against unknown or future risks.

From a supervisory standpoint, distinguishing between temporary risk-mitigation measures and enduring control structures is critical to understanding where responsibility ultimately resides.

Q21. How should regulators assess the materiality of guardian powers when determining whether a DeFi protocol is effectively decentralised? At what point does guardian authority (by virtue of its scope, duration, frequency of use, or governance) constitute ongoing or effective control that may warrant regulatory treatment?

5.2 Guardian Agents as embedded Risk Management and Market Integrity Tools

In traditional financial systems, risk management and market integrity are supported by layered institutional arrangements, including prudential requirements, financial crime compliance requirements, circuit breakers, supervisory interventions, and legal remedies. DeFi lacks many of these *ex-post* enforcement mechanisms, placing greater weight on *ex-ante* design-embedded technical controls. Guardian Agents serve as one of the primary means by which DeFi protocols seek to replicate, at protocol level, the stabilising functions of these arrangements in regulated markets, including loss-containment, continuity of service, and the prevention of disorderly failure.

At the same time, reliance on Guardian Agents introduces new regulatory concerns. Depending on their scope and governance, Guardian Agents may redistribute losses, alter contractual outcomes, or override user expectations in ways that are functionally analogous to discretionary supervisory or resolution actions—yet without explicit legal mandates, procedural safeguards or avenues for redress. Moreover, the expectation of guardian intervention may weaken market discipline,

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

encouraging greater risk-taking by developers or users who assume that extreme outcomes will be mitigated.

Q22. To what extent do Guardian Agents meaningfully contribute to market integrity and financial stability in DeFi, and under what conditions might they primarily protect protocol insiders and incumbents? How should regulators evaluate the trade-off between rapid intervention and predictable, rule-based outcomes in DeFi?

5.3 Governance and Accountability

A central regulatory challenge posed by Guardian Agents is accountability and attribution. Whilst DeFi systems are often described as trustless, Guardian Agents necessarily require some degree of trust—whether in code, governance processes, or identifiable actors. For regulators, the question is not whether trust exists, but how trust, authority and responsibility are structured, how they are constrained, and whether they are legible to supervisors, users, and other external stakeholders.

Guardian Agents may derive operational legitimacy from governance mechanisms (such as on-chain voting), reputational frameworks within developer communities, or constraints encoded directly into smart contracts. However, none of these mechanisms cleanly align with established regulatory accountability frameworks. Token-based governance may concentrate effective influence among large or coordinated holders, whilst code-based constraints may operate as intended under normal conditions but fail in novel or extreme scenarios. The absence of legal obligations further complicates questions of redress, liability and enforcement.

Nevertheless, Guardian Agents may also provide regulators with clearer points of regulatory engagement than fully autonomous systems. Where guardian actions are transparent, auditable, and attributable (whether to specific blockchain addresses, multi-signature arrangements, or identifiable governance bodies), they may offer a practical basis for dialogue, the development of standards or expectations, and potentially coordinated responses during periods of market stress, without implying delegation of public authority or supervisory functions to the protocol itself.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Q23. What forms of accountability should regulators expect of Guardian Agents, given their functional role in DeFi systems? To what extent can transparency, on-chain auditability, and verifiable governance processes substitute, even partially, for traditional legal accountability and enforcement obligations?

5.4 Guardian Agents in the Regulatory Trajectory of DeFi

As DeFi continues to evolve, Guardian Agents may increasingly play a pivotal role in shaping its regulatory trajectory. Protocols that incorporate credible, transparent and well-governed guardianship mechanisms may be perceived as more resilient and more compatible with policy objectives (e.g. consumer protection, market integrity), potentially reducing pressure for broad and/or blunt regulatory intervention. Conversely, opaque or overpowered guardian structures may reinforce concerns that DeFi replicates the risks of traditional finance without commensurate safeguards, accountability or redress.

Looking ahead, Guardian Agents may also become conduits for regulatory alignment-by-design. Industry practices and soft-law principles or guidelines for guardian transparency, scope limitation (i.e. bounded authority and triggers), and emergency procedures could emerge organically within the industry or be encouraged through supervisory guidance and expectations. Such developments would not amount to direct regulation of code, but rather to the articulation of outcomes-based expectations around responsible protocol design.

For financial authorities, the important question is how to engage with Guardian Agents as risk-mitigating design features without undermining decentralisation claims or assuming *de facto* responsibility for private systems. A functional approach, that is by focusing on who can intervene, under what conditions, and with what effects, may offer a path to assess responsibility and supervisory touchpoints while respecting architectural autonomy. Guardian Agents highlight both the limits of purely automated finance and the opportunities for new, hybrid forms of oversight that sit between markets and the state.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Q24. ***Should the MFSA consider introducing a principles-based framework or guidance addressing the design, governance, and transparency of Guardian Agents within DeFi systems?***

Q25. ***How should regulatory engagement with Guardian Agents differ from the supervision of traditional financial intermediaries, given their embedded, protocol-level role and potential absence of independent legal personality? Which supervisory tools (e.g. disclosure expectation, design principles, incident reporting, governance reviews) are most appropriate for such mechanisms, and which traditional tools may be unsuitable or disproportionate?***

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

6 Account Abstraction

Blockchain systems have traditionally relied on Externally Owned Accounts (EOAs), which are addresses controlled directly by private cryptographic keys, held by users or custodians, used to authorise all transactions. Accordingly, EOAs have two significant limitations:

i. they require transaction fees (i.e. gas fees) to be paid exclusively in the network's native token; and

ii. they rely entirely on possession of the private key to initiate transactions and recover access, offering no native support for programmable controls, recovery logic, or conditional execution, as EOAs cannot contain executable code.

Account abstraction (AA) refers to an evolution in account architecture whereby instead of relying solely on a private key, a user's account may be implemented as a Smart Contract Account (SCA) deployed directly on the blockchain. Under AA, the logic governing transaction authorisation, validation, and execution is fully programmable. Unlike EOAs, the authorisation of a transaction can be logically and temporarily separated from its execution and fee payment, allowing for greater flexibility in how transactions are initiated, validated and funded.

In practice, AA allows accounts to, *inter alia*:

- define custom validation rules for transactions (e.g. spending limits, multi-factor or multi-signature authentication);
- batch, delegate, or schedule transactions;
- incorporate recovery, pause, or emergency mechanisms; and
- enable alternative arrangements for transaction fee payment, including the ability for users to pay fees in tokens other than the blockchain's native asset.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Furthermore, Account Abstraction introduces additional actors into the transaction lifecycle, facilitating alternative fee and execution arrangements, and effectively decoupling the user experience from underlying network mechanics. These actors include:

- **Paymasters**: smart contracts that may sponsor, subsidise, or condition the payment of transaction fees on behalf of users, for example by covering gas costs for specific transactions or accepting fees in tokens other than the native blockchain asset;[33] and

- **Bundlers**: off-chain service providers or software applications that aggregate multiple transactions from various SCAs, packaging them into a single, standard blockchain transaction, which is then submitted to the network for validation[34].

6.1 Account Abstraction and DeFi

AA is particularly relevant in the context of decentralised finance because it changes how users, software and intermediaries interact with DeFi protocols, transforming wallets from largely passive key-holding tools into active, programmable control layers. This impact can be synthesised into three key changes:

i. **Logic-driven interaction**: AA enables transactions to be executed automatically based on predefined rules (e.g., scheduled payments, automated portfolio management, or conditional execution), reducing the need for contemporaneous, manual user action for every transaction. This programmability allows DeFi interactions to be policy-driven rather than key-driven, with transaction behaviour determined *ex ante* by encoded logic rather than ad hoc user approvals;

ii. **Delegated and agent-based activity**: AA permits software agents, including algorithmic and AI-based agents, to interact with crypto-assets within strictly defined and auditable parameters. Instead of granting unrestricted private-

[33] Visa, "What is Account Abstraction?" (2023) - Exploring new techniques for blockchain payment processing. (link).
[34] Ibid.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

key access, SCAs allow granular delegation subject to predetermined spending caps, circuit breakers, time-locks, or multi-factor validation for higher-risk actions. This supports the automation of complex DeFi strategies while reducing single-key risk and improving the traceability of delegated authority; and

iii. **Emergence of new technical roles**: AA introduces new actors into the transaction lifecycle, such as the abovementioned paymasters and bundlers. While these roles may be purely technical in certain implementations, their operation may be commercial in nature and involve some degree of influence over transaction ordering, fee payment, or execution conditions, whether directly or indirectly, over wallet transactions questions may arise as to the allocation of control, responsibility, and potential regulatory qualification under existing EU frameworks.

Taken together, these developments may materially reshape how DeFi operates in practice, even where underlying protocols remain decentralised and permissionless. By shifting control and decision-making to the wallet layer, AA introduces new governance, accountability, and risk-management considerations that sit upstream of DeFi protocols themselves.

Through this discussion paper, the MFSA seeks to initiate a preliminary dialogue on how AA affects the allocation of control, responsibility, and regulatory obligations under existing EU frameworks, including but not limited to MiCA, the payments framework, and broader governance expectations applicable to authorised entities and service providers.

6.2 Preliminary considerations under MiCA

The Markets in Crypto-Assets Regulation (MiCA) was drafted with a technology-neutral and activity-based approach, and regulates persons who issue, offer or provide crypto-asset services, rather than specific technical architectures. Accordingly, the use of smart contracts instead of EOAs does not, in itself, determine whether an activity falls within the scope of MiCA. What matters is whether identifiable natural or legal persons perform, provide or control services functionally captured by MiCA's CASP perimeter (e.g. custody and administration, exchange,

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

execution, transfer, advice, portfolio management, operation of a trading platform, placing), regardless of the underlying code implementation.

In line with the Regulation, and noting that Recital 22 excludes from MiCA's remit crypto-asset services which are offered in a "*fully decentralised manner without any intermediaries"*, the key regulatory question is whether a person or entity:

- provides a crypto-asset service on a professional basis;
- acts on behalf of users in relation to such services; or
- provides a service, exercises control or material influence over crypto-assets or their administration (i.e. has "means of access" to the crypto assets[35])[36].

From this perspective, AA does not automatically imply the provision of custody or administration services. MiCA looks to assess who can ultimately exercise control or intervene over assets or services performance. However, AA, as outlined above, introduces two main areas where MiCA-relevant control may arise:

i. **Custody of crypto-assets**: in AA implementations, such means of access or control could potentially arise: (a) where a commercial entity or professional recovery service acts as a "guardian" for a user's SCA, by holding sufficient signature weight in a multi-signature or social-recovery setup, thereby enabling unilateral or joint control over the SCA (e.g. recovery, emergency pause etc.). In this event, that entity possesses a technical means of access to exercise control over user funds[37]; or (b) where a service provider designs, configures, controls or co-controls validation logic for the wallet's transactions (e.g. it can approve/reject classes of transactions or change allow-list/limits), resulting in a practical ability to administer users' assets.

   In such cases, supervisors may consider whether the provider is performing

[35] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets ("MiCA"), OJ L 150, 9.6.2023, Article 3.
[36] BCAS, MiCA Decentralization Handbook (September 2024), https://blog.bcas.io/decentralisation-under-mica-the-definitive-handbook-for-defi
[37] Ibid.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

"custody and administration of crypto-assets on behalf of clients" within MiCA's CASP list, even if the wallet is a smart contract account and no private keys are directly held by the provider.

ii. **Management of crypto-assets**: Where a service provider offers an agent (including an AI Agent) that interacts with a user's SCA, that provider may be deemed to be providing portfolio management services. In this context, the provider would have direct, programmatic influence over execution, a form of "means of access" that may disqualify a pure "self-custody" model, even if the keys remain under the user's SCA and the logic is pre-programmed[38].

In these instances, the regulatory challenge lies in defining the precise threshold of control or influence that would transition a service provider from a technical facilitator into a CASP providing custody and administration services and/or portfolio management services under MiCA.

6.3 AML/CFT and Financial Crime preliminary considerations

AML/CFT considerations in the context of AA may arise where it is combined with:

- transaction facilitation on behalf of users;
- gas fee sponsorship; or
- automated execution of transactions as a service.

The applicability of AML/CFT requirements in these instances depends on whether the relevant entity qualifies as an 'obliged entity' under the AMLR, as supplemented by sectoral legislation (MiCA, PSD2, EMD2). In particular, the nature of the service provided, the assets involved, and whether the activity is conducted on a professional and commercial basis, determines the classification.

For example, if a Paymaster accepts fiat currency or issues/receives Electronic Money Tokens (EMTs) in exchange for transaction-fee (gas) sponsorship, the operator may fall within the scope of the EU payments framework (currently PSD2,

[38] BCAS, MiCA Decentralization Handbook.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

and in due course PSD3/PSR), potentially qualifying as a Payment Institution or EMI. Conversely, if the service involves the exchange of crypto-assets, the custody or administration of crypto-assets on behalf of clients, or the facilitation of transfers as a service, the operator may require authorisation as a CASP under MiCA. In either scenario, such classification would bring the Paymaster operator within the full scope of applicable AML/CFT obligations, including customer due-diligence, transaction monitoring, and sanctions screening requirements[39].

Further to the above, gas sponsorship mechanisms by Paymasters, together with transaction aggregation activities performed by Bundlers, introduce intermediary layers in otherwise peer-to-peer transaction flows. These layers could potentially obscure the source of funds, blur the identification of the originator and beneficiary, or facilitate transactions involving sanctioned or high-risk addresses, thereby challenging the efficacy of existing AML/CFT monitoring and the Travel Rule. framework. The risk is heightened where such services are offered at scale and on a commercial basis, particularly where discretion exists to sponsor, prioritise, or aggregate transactions.

At the same time, AA may also create opportunities for "embedded compliance" or compliance-by-design, by integrating compliance logic directly at the wallet level, for instance by programming SCAs to require off-chain identity verification, sanctions screening, address risk-scoring, as a programmable precondition for transaction execution. Such mechanisms could complement traditional AMF/CFT controls by shifting certain checks upstream to the point of transaction initiation. However, the extent to which such mechanisms can meaningfully support regulatory outcomes without re-introducing centralised choke points, discretion, or new forms of effective control warrants further examination from both a legal and supervisory perspective.

Q26. How should control and influence in account-abstracted wallets be assessed for the purpose of MiCA? Which Smart Contract Account (SCA) features, such as recovery mechanisms, validation-logic controls, spending limits, emergency powers, or agent delegation, are most relevant when

[39] European Banking Authority, Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens (June 2025), link.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

determining whether custody or administration of crypto-assets exists under MiCA?

Q27. To what extent should actors such as paymasters, bundlers, or AI-agent operators be considered as providing crypto-asset services under MiCA when such activities are offered on a professional and commercial basis?

Q28. To what extent is a "compliance-by-design" model viable within Account Abstraction architectures? Can SCAs meaningfully support or automate elements of AML/CFT obligations and regulatory requirements (e.g. asset segregation) without undermining decentralisation? If so, how?

Q29. Considering the current level of market adoption and technical maturity of account abstraction, is there a need for regulatory or supervisory guidance to clarify the application of existing frameworks? If so, should such guidance focus on principles, illustrative scenarios, or supervisory expectations, or would premature intervention risk constraining experimentation and innovation?

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

7 Conclusion

The MFSA is seeking feedback from stakeholders prior to proceeding with detailed proposals on the implementation of any of the initiatives presented in this document.

The Authority is also inviting participants to contribute views on other proposals not covered in this Discussion Paper that may contribute to the further growth of the industry.

Q30. Are there any other initiatives, not considered within this discussion paper, which the Authority ought to consider?

The discussion paper is open to the public until **10 July 2026**. Industry Participants and interested parties are invited to send their responses via email to spi_consultations@mfsa.mt.

Following this consultation process, the Authority will review feedback received from stakeholders and potentially initiate work on the implementation of the respective initiatives accordingly.

In line with the Authority's Vision to enhance stakeholder engagement, draft versions of any proposed major amendments to the regulatory frameworks will be issued for public consultation.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt