MFSA MALTA FINANCIAL SERVICES AUTHORITY

Potential Use of Tokenisation of Fund Units - Tokenised Fund Units as Collateral within Permissioned DLT Networks

MFSA Position Paper

10 March 2026

CONTENTS

Disclaimer

This paper sets out the position of the Malta Financial Services Authority in relation to the potential use of tokenisation of fund units as a collateral. Apart from the regulatory viewpoint, this paper does not constitute any financial, legal or professional advice on the use and /or model of collateralisation of tokenised fund units and, accordingly, the use of this information for such a purpose is without recourse to Malta Financial Services Authority and any of its officials for any loss, damage or liability sustained.

1. Introduction

On 12 June 2025, the Malta Financial Services Authority ("MFSA" or "Authority") published a position paper[1] outlining the regulatory and operational considerations related to the transfer agency element of tokenisation of fund units. Following the growing trends in tokenised financial instruments, this document explores an emerging use case: the possibility of using tokenised fund units as collateral within a public Distributed Ledger Technology ("DLT") network while maintaining institutional-grade oversight and privacy through the use of permissioned DLT networks.

The use of tokenised fund units as collateral is intended to secure financing arrangements through regulated entities, such as Brokers, Investment Firms and Credit Institutions. Provided that comprehensive risk mitigation and safeguarding arrangements are in place, this use case can also be extended to decentralised finance protocols (DeFi) through the deployment of a permissioned network as an overlay layer. Tokenisation is considered as a technological enabler to support more efficient collateral processes through a DLT within a regulated environment in order to retain high standards of investor protection through identity verifications of the counterparts within the DLT.

2. Scope

This paper covers a use case of a model for collateralising tokenised fund units, specifically the methodology adopted, benefits, the residual risks, and operational considerations associated with this model. Tokenisation of a financial instrument shall not alter the characteristics of the underlying instrument.

While the Authority is also considering other use cases involving tokenisation of financial and non-financial instruments, including the trading of tokenised fund units, the scope of this paper is solely focused on the use case described herein. However, the regulatory implications of any model adopted should be assessed on its own merits.

3. Background and Context

Tokenisation of financial instruments has gained momentum globally as institutions explore the potential of DLT to reduce the level of intermediation. This leads to streamlined processes, reduction in settlement times, enhanced transparency, and integrity of recordkeeping. Malta's current tokenisation initiatives have been built on permissioned DLT networks, reflecting strong emphasis on AML/CFT compliance, accountability, and oversight.

[1] *June 2025, MFSA Position Paper on Tokenised Fund Units*

While these developments remain at an early stage, industry stakeholders are increasingly examining how tokenised representations of fund units could be used to support collateralised transactions. In this context, tokenisation does not alter the rights or characteristics of the underlying units. Rather, it offers an alternative operational infrastructure to represent fund units' ownership.

While maintaining the legal classification of tokenisation of fund units as financial instruments under MIFID II [2], DLT still introduces relative innovative solutions to the way such units are stored and distributed. When marketing and distributing such financial instruments to retail investors, the necessary suitability and appropriateness assessment still needs to be performed, considering the fund's underlying investment strategy and the distributor's obligations under MiFID II[3]. The suitability of these products shall be carefully evaluated as it is highly likely that they fall within the definition of complex instruments, which are not suitable for retail investors. Such assessment shall be properly documented and retained, demonstrating that it acted in the best interest of the client.

4. Applicability of Collateralisation of Tokenised Fund Units

Enhanced operational capabilities offered by tokenisation is one of the main potential benefits of this model. The application of DLT networks may contribute to better efficiency in collateral transfers, traceability, transparent recordkeeping and improved auditability, whilst maintaining costs on the lower end.

The main goal of utilising the tokenised fund units as a collateral is to streamline the traditional collateral management models into a process that should be more transparent, faster and generates additional returns to investors. Moreover, such model aims to utilise liquidity in a more efficient way. The ability to monitor pledged assets in real time enables lenders to oversee collateral positions on an ongoing basis. Furthermore, faster settlement processes reduce operational risk on the side of the lender, especially in scenarios requiring frequent collateral adjustments.

One important operational benefit is the speed of settlement/transfer of tokenised assets. Tokenised fund units can be transferred and settled nearly instantly on a designated/predetermined DLT, which would normally reduce the risk of counterparty exposure. Under normal circumstances of the transfer, the collateralisation process can mirror this speed through a rapid settlement mechanism (T+0) that ensures simultaneous movement of assets between wallets during pledging, practically eliminating any delays in settlement. Furthermore, as an additional benefit, such arrangements would be instantly available on a "24/7 settlement" cycle. The use of

[2] *Article 4(1) (15), of the Directive 2014/65/EU of the European Parliament and of the council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.*

[3] *Article 25(2) (6), of the Directive 2014/65/EU of the European Parliament and of the council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.*

smart contracts, as programmable, self-executing arrangements automates manual processes, making the collateral management framework more resilient compared to the traditional model.

From a compliance and governance oversight perspective, the DLT technology enables fund managers and brokers to adhere to their legal and regulatory obligations, while the use of an immutable and transparent distribution ledger can simplify recordkeeping and audit processes. These benefits, in general, streamline regulatory reporting and reduce the likelihood of potential fraud. Compliance and anti-money-laundering (AML) controls can be embedded at the token minting stage, with smart contracts enforcing rules that prevent transfers to unverified wallets and ensure that the predetermined requirements are met automatically. Whether permissioned or permissionless, a DLT ledger can provide a shared, time-ordered record of token transfers and resulting holdings. However, the degree of immutability and the interpretation of "ownership" depend on the chain's finality model, governance arrangements (including any administrative or upgrade powers), and whether addresses are mapped to legal and/or beneficial owners off chain. In this regard, unit holders and service providers shall exercise caution and carry out due diligence in advance on the type of DLT ledger used.

In addition, the immutability of records on a permissioned DLT allows greater traceability, providing visibility for transactions which might help institutions identify suspicious transactions. By way of example, a smart contract can be used to control access to and ownership of a tokenised fund unit and can be programmed to automatically block transactions from unidentified or blacklisted addresses.

Fund administrators may benefit from reduced paperwork and automated/accelerated KYC/AML processes. Using a hybrid architecture the fund administrators could retain the share register (off-chain) whilst also recording tokenised fund units on a distributed ledger (on- chain).

In spite the numerous benefits associated with collateralisation of tokenised fund units', the accompanying risks must be carefully considered. This is in view of the limitations and risks inherent to any new technologies and proposed market structures, in particular cyber security threats leading to potential loss of assets.

5. Regulatory Treatment

Units/shares of a fund may be represented digitally i.e. tokenised on a DLT register. The monetary value of the token represents the same traditional unit/share as in the conventional share register and does not alter the legal nature of the unit. Each share class in the fund must be mapped to a distinct digital asset, a token, and segregated from other share classes which are not tokenised. While each token may represent the underlying share/unit, tokens may be fractionalised to allow for smaller allocations, where permitted by the fund's rules and/or by the fund's constitutional documents.

Under the proposed model/s, a fund issues tokenised units on a DLT using a hybrid architecture that combines elements of both traditional (off-chain) and on-chain recordkeeping. The CIS that tokenises its fund units to be further used as collateral shall be constituted in accordance with the Investment Services Act, which provides the legal and regulatory framework governing investment services, including CISs. For this model, it is recommended that the CIS is established in the form of a SICAV as defined in the Companies Act (Investment Companies with Variable Share Capital) Regulations (as amended in Legal Notice 293 of 2023). These funds may be available to all types of investors as long as they satisfy the regulatory requirements applicable.

The fund administrator will continue to perform its transfer agency function and will retain responsibility for maintaining the share register as the official register when it comes to holdings of fund units for the purposes of legal ownership, investor identification, and regulatory oversight, while tokenised fund units are recorded and transferred on a distributed ledger (on-chain). In this configuration, the use of DLT functions as a technological and transactional layer, without constituting the legally determinative register.

The fact that the official register is retained by the recognised fund administrator, a subject person itself under the Prevention of Money Laundering and Financing of Terrorism Regulations framework, provides additional assurances with the investor identification, investor protection and recording keeping requirements applicable under the Collective Investment Scheme (CIS) Laws and Regulations, mainly the Investment Services Act, 1994. Irrespective of whether records are maintained off-chain or reflected on-chain, the valuation and NAV calculation processes will also continue to be conducted according to the CIS regulatory requirements and the fund's offering document and by an entity recognised in terms of Article 9A of the Investment Services Act. The MFSA expects that an independent valuer is appointed in the case of illiquid instruments. The valuation requirements set out in Article 19 of the Alternative Investment Fund Managers Directive (AIFMD) should likewise apply to the tokenisation of fund units in the case of funds set up as Alternative Investment Funds, including the requirements on independence of the valuation function, the frequency of valuations, and the appointment of external valuers.[4]

This does not exclude the possibility that, by time, the share register may move completely on-chain. This is subject to the legal and regulatory recognition of the ledger as the official register, as well as the necessary changes to offering documents and service agreements, which may be subject to supervisory assessment or approval processes.

The tokenised units can be used as collateral under a lending agreement granted by a regulated lender to the fund investor for the potential use of liquidity management or obtaining additional exposure through margin lending. If, alternatively, lending is conducted through a liquidator utilising Defi protocol, such liquidator must be reliable,

[4] *Article 19 of the Directive 2011/61/EU of the European Parliament and of the council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.*

whitelisted and accepted by the fund administrator. The collateral arrangement may be recorded or operationalised on-chain, off-chain, or using a combination of both approaches. A key feature of this model is that tokenisation serves as a technological enabler rather than for market innovation. It introduces efficiencies in recordkeeping, faster settlement, and facilitates monitoring without altering the nature of investor rights.

Considering that tokens of fund units are considered as financial instruments, distribution of these instruments falls within the authorisation, conduct and prudential requirements stipulated in the MiFID II regulatory framework.

As mentioned in the Position Paper issued on 12 June 2025, the offering documentation for the fund must be amended accordingly to include clear and transparent disclosures about the tokenisation, including:

- the operations of the tokenised register, the type of DLT used and the protocol safeguards;
- the manner that the wallets are managed, and custody arrangements of the wallets accepted by the recognised fund administrator;
- token issuance mechanism and the underlying technology;
- subscription and redemption process;
- transferability limitations;
- interoperability channels between the issuer and the regulated facility, if any
- all associated technology, regulatory and operational risks (smart-contract risk, cyber-security, key-management, recovery/contingency planning, identity/ privacy safeguards, third-party dependencies, governance).
- if collateralisation of tokenised fund units is utilised through DeFi network, the liquidator's role should be defined.

6. Methodology & Operational Model

Although the precise technical implementation may vary, depending on the infrastructure used by the Fund/ Fund Manager and/or the lending facility, the following describes how a tokenised-unit collateral model can be structured in a manner consistent with the MFSA's regulatory framework.

In the traditional fund set-up, the recognised fund administrator is responsible for the transfer agency function. In a tokenised structure, the fund administrator / transfer agent could also assume responsibility for managing the DLT register, whilst maintaining the official share register of the fund. If the investor already owns a wallet, its compatibility needs to be verified and accepted by the entity responsible for the transfer agency function.

Governance and operational risk frameworks must ensure that the fund's governing body and service providers have sufficient competence and sound knowledge regarding DLT and tokenisation, maintain effective risk-management, and preserve investor protection, transparency, and compliance standards already required under Maltese law.

Collateralising tokenised fund units does not impede on the collection of traditional income derived from the distribution of dividends in the case where the issuing fund is a distributor fund.

Operational Model

Figure 1 below provides a schematic representation of a model setting out the adoption of tokenisation. The collateralisation process starts with the investor providing due diligence information on the token to the lender to enable the latter to carry out its due diligence reviews. The lender validates the token origin and drafts the terms of the collateral, including the percentage of the haircut (if any). The smart contract subsequently restricts the transferability of the pledged token - for the duration of the collateral arrangement as indicated on the righthand side of Figure 1 below. While transferability and redemption rights are suspended, income distribution and yield-generating functions remain operative.

When the investor's tokenised units are used as collateral for financing, the smart contract architecture shall allow for partially blocking the transfer of the token when it is used as collateral (i.e. by restricting transferability via on-chain mechanisms or by ensuring that only approved, compliant counterparties/wallets may receive transferred tokens), but any such mechanism must be supported by the wallet/ custody and contractual arrangements described in the offering documents.

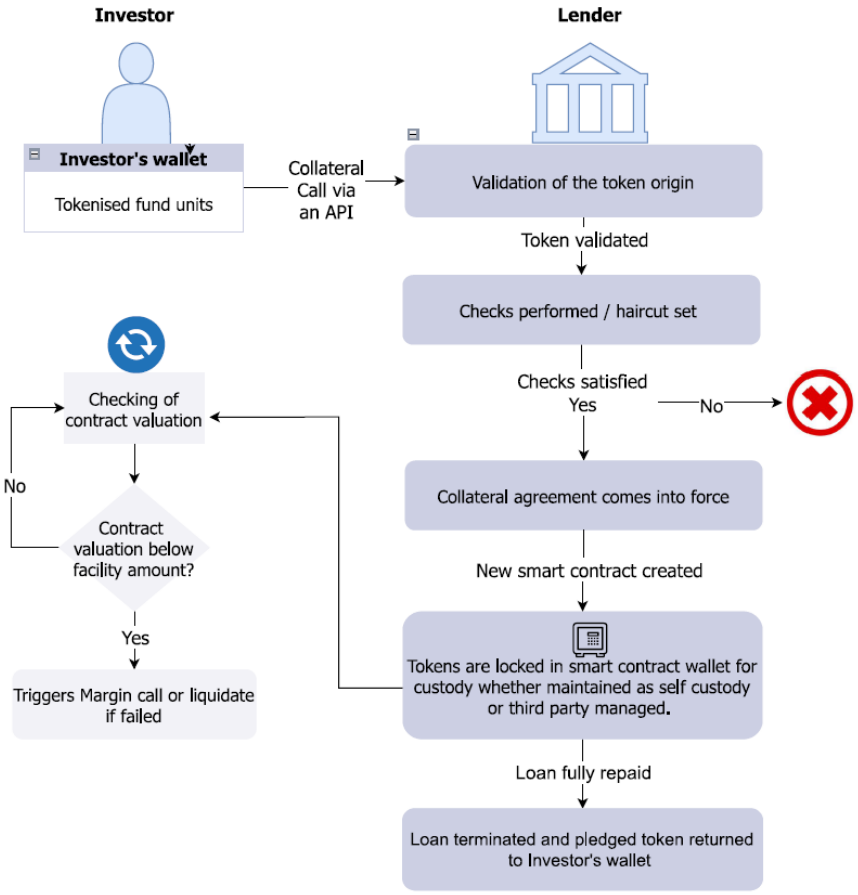

Figure 1 - In this case, tokenised fund units being used as a collateral with the lender being: (i) credit institution authorised under the CRD framework or (ii) an authorised investment firm.

In terms of the investment firms, these may offer credit or lending facilities as an ancillary to its main services as authorised under MiFID[5]. Therefore, the tokens issued by the Fund to investors may be collateralised with an investment firm by the fund investor against a trading facility. The investor is given the opportunity to generate additional returns from the funding granted by the investment firm under the brokerage account.

Termination of the smart contract can be triggered by full repayment or a default event by the investor. Unless such a trigger event occurs, the investor holding the token will remain the legal owner of the token, which at this point is pledged with the lender. Only a margin call by the lender if the margin requirements are not met will lead to the liquidation of the underlying collateral and the transfer of the token ownership to the lender. Such collateral arrangement will be automated within the smart contract which encodes margin thresholds, automation liquidation triggers and transfer mechanics upon default.

[5] *Annex 1, Section B of the Directive 2014/65/EU of the European Parliament and of the council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.*

Where the lending facility is utilised for margin lending, namely, to facilitate the borrower's purchase of other securities, the Securities Financing Transaction Regulation (SFTR)[6] reporting requirements are applicable. It is pertinent to note that in terms of the requirements emanating from Article 4 of the SFTR the transaction shall be reported to the Trade Repository. The parties involved shall assess their reporting obligations in terms of the SFTR.

Figure 1 can be further extended as illustrated below in the event that the transactions occur through DeFI protocols, whereby the specific permissioned mechanism is utilised.

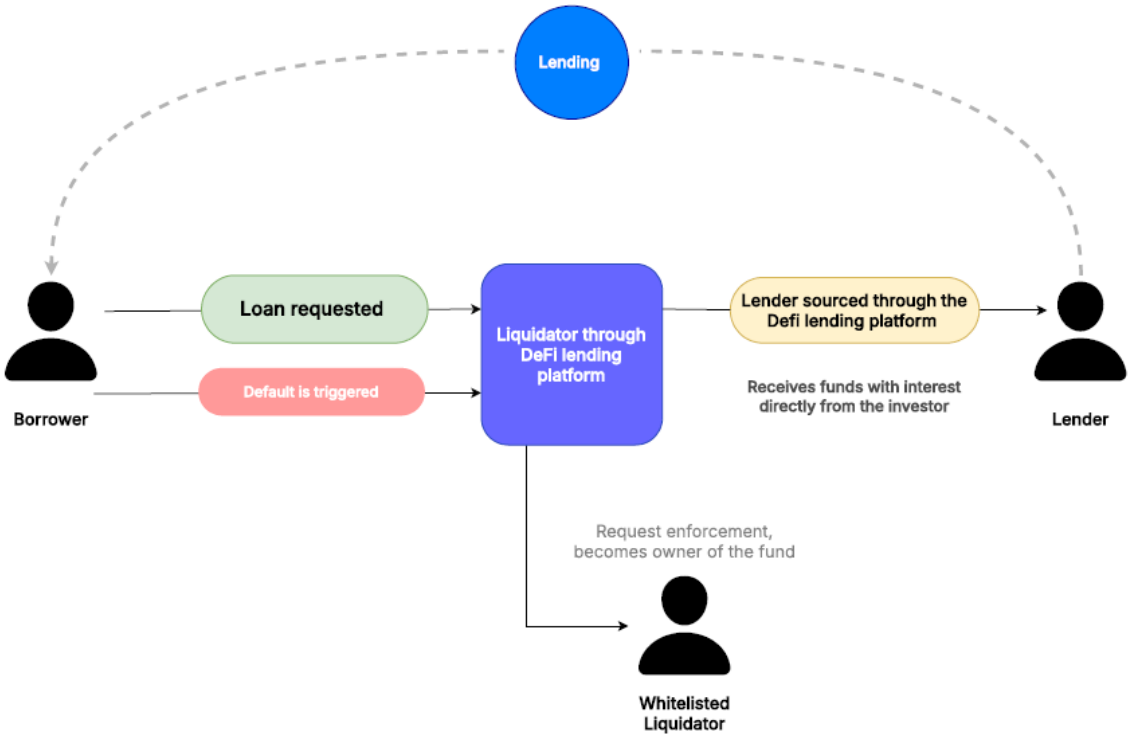

Figure 2: Lending is extended allowing collateralisation of tokenised fund units through DeFI Protocol within permissioned markets, ensuring that the liquidator is whitelisted.

This illustrates the collateralisation of fund units on DeFI protocol through a whitelisted liquidator, which has been formally approved by the protocol following the completion of the prescribed due diligence and eligibility requirements to perform liquidation functions.

Throughout this model, the investor retains ownership of tokenised units, while the relevant smart contract is locked throughout the collateral period. The lender receives payments directly from the investor and the underlying fund is excluded from this transaction.

[6] *Article 4 of the Regulation (EU) 2015/2365 of the European Parliament and of the council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012.*

The token remains in the investor's wallet in a frozen or restricted state throughout the collateral period. In the event of a default, the liquidator can request enforcement, but the actual on-chain actions are executed by the transfer agent, in order to maintain alignment between the DLT ledger and the official share register.

The liquidator shall satisfy the following non-exhaustive criteria:

- have the necessary technical infrastructure to interact with decentralised exchanges and understand the protocol risk parameters of the DeFI;
- the liquidator may operate through a DeFi protocol, the relevant protocol deployment should function within a permissioned market environment - this should be supported by restricted pools incorporating appropriate governance and compliance controls, including KYC/AML procedures and participation limited to duly whitelisted addresses;
- the appointed liquidator is to be whitelisted i.e. formally approved by the protocol following the completion of the prescribed due diligence and eligibility requirements;
- the liquidator must not have any conflict of interest with the protocol or its stakeholders;
- oversight and background checks should be carried out on the liquidator;
- the liquidator is of sufficient standing and repute and shall operate within an equivalent jurisdiction in terms of AML/ CFT standards;
- adopt the necessary financial expertise to carry out its role effectively – liquidation bonuses and fees shall be pre-determined and documented.

<u>The role of the liquidator:</u>

- The liquidator is responsible to monitoring loan collateral and executing liquidations when borrowers' positions fall below the defined threshold.
- In the event of a default, the liquidator shall assume the defaulting investor's position in accordance with the applicable protocol mechanics and contractual agreements.

The lending and collateral arrangements shall be governed by the applicable governing law specified in the contractual documentation. The parties shall carefully assess the applicable legislative framework in the case of a failed margin call, with particular attention to the implications of the applicable insolvency rules in this event.

7. Risks and Risk Mitigation Measures

Despite the potential advantages, use of tokenised assets as collateral introduces several risks that merit careful consideration. Such risks primarily emanate from the novelty and complex nature of the underlying technology.

Permissioned DLT networks are vulnerable to technology architecture risks. In particular, their closed nature combined with absence of widely adopted interoperability standards, often limits interconnectedness with other systems. At the same time, when interoperability is introduced through Application Programme Interfaces (APIs) or cross-chain bridges, these interfaces may themselves become vulnerable points for cyberattacks.

Cybersecurity also remains one of the main critical concerns. Although permissioned networks may offer enhanced control over access, they are not immune to cyber threats. For instance, if either nodes, validators or smart contracts are targeted, this could result in data integrity or data availability compromised. Also, centralised operators may also be considered a single point of weakness within permissioned networks.

Despite its advantages, the inherent immutability of DLT may pose challenges if incorrect data is recorded on-chain or if smart contracts contain coding errors. Since such errors can be difficult to detect and reverse, they may impede the integrity of collateral arrangements unless supported by strong governance frameworks.

Another risk worth noting is when tokenised fund units used as collateral are held through nominee arrangements. When a nominee is present in the transaction chain, legal ownership may be detached from the natural persons who ultimately own or control the investment. This increases the risk of inadequate customer due diligence, limiting the obliged entity's ability to adequately assess the purpose and intended nature of the business relationship. And while DLT may improve traceability and auditability of transactions, such transparency does not ensure the identification and verification of ultimate beneficial owners. It remains the responsibility of the lender to ensure that the borrower is of sufficiently good standing and to abide by the respective AML/FT regulations in the respective jurisdictions when it comes to KYC checks on lenders involving nominee structures, prior the establishment of relationship. Binding contractual obligations should require nominees to disclose and maintain accurate beneficial ownership information, provide access to due diligence documentation, and promptly notify any changes in ownership or control.

A significant and often underestimated risk is associated with the valuation of tokens used as a collateral. Tokenisation does not affect the operation of the fund and its valuation frequency. The latter is typically performed at fixed intervals—daily, monthly, quarterly, or, in certain cases, annually. This may create a potential misalignment with the real-time operational capabilities of DLT-based collateral mechanisms. For funds with illiquid assets or model-based valuations, the restricted pricing may complicate

the determination of whether collateral remains sufficient between valuation cycles. These discrepancies can lead to over- or under-collateralisation reference values.

Finally, being hybrid systems, permissioned DLTs still rely on the off-chain data, which can result in recordkeeping and ownership issues. Related operational risks further include failures in system interoperability, incorrect tagging or locking of units, and complications in processing redemptions or suspensions during collateralisation. It, therefore, must be made clear, which ledger – DLT-based or traditional Fund Administrator records – constitutes the definitive register in case of discrepancies, by establishing clear rules regarding the authoritative ledger of ownership.

To benefit from tokenisation and use of fund tokens as collateral in a secure way, the funds shall introduce robust mitigating and preventing measures. From technological standpoint, particular attention should be paid to risks arising from permissioned DLT architectures, including vendor/third-party concentration risks, where reliance on a single DLT provider, wallet provider, or a smart-contract operator could result in systemic dependency. Therefore, funds should seek assurance that permissioned DLT are subject to robust security standards, regular audits, and resilience assessments. Cybersecurity measures should be clearly defined, including secure key management, penetration testing, incident response protocols, and operational resilience measures. Smart-contract governance should also be subject to independent audits, controlled upgrade paths and formal verification where appropriate. Where permissioned DLT offers interoperability with external systems, secure interfaces and strong governance controls are necessary to minimise cyber vulnerabilities. The frequency of such checks should be pre-determined, and the verifications shall be adequately documented.

Separately, entities shall seek clarity on the legal status of tokenised units, statutory clarity on both the issuance of tokens of fund units as well as the creation, management and enforcement of pledges/ collateral combined with robust regulatory framework, governing security interests, especially when DLT infrastructure introduces new operational layers. Any reliance on third-party service providers should comply with established regulatory expectations for oversight, due diligence, and resilience.

Taken together, these measures aim to maintain the stability and integrity of the overall collateral framework, even when innovative technological structures are introduced.

8. Conclusion

Collateralisation of tokenised funds within permissioned DLT presents an opportunity to modernise existing financial processes and create additional opportunities for investors to generate returns over and above the returns generated from the investment in a fund, from the same capital invested. That said, in times of market downturn the risk of losses could be extended leading to a spiral of losses and

potential contagion, especially if the lenders do not carry out updated valuations of collateral. Consequently, transparency and disclosure are crucial to retain the robustness of the model.

The transition from traditional dematerialised records to DLT reflects a paradigm shift in the medium of representation, rather than a change in the legal classification of the instrument itself. The success of the model depends on three pillars: (a) the interoperability and transferability of the tokens to move across different DLTs; (b) the robustness of the governance structures to mitigate ML/FT, settlement and cyber risk; and (c) the implementation of rigorous KYC evaluation procedures coupled with the right choice of the DLT, typically private permissioned ledgers.

The MFSA, throughout this paper recognises the potential use of tokenisation of funds units through collateralisation and how risks can be mitigated ensuring that all standard regulatory safeguards remain fully in force specifically, AML/CFT obligations, identity verification, investor onboarding procedures, transaction monitoring, fund administration oversight all of which should be compliant with the relevant regulatory frameworks. Whilst cognisant that other use cases may exist, the MFSA recommends that stakeholders carry out a rigorous legal assessment to ensure that such structures are compliant with the respective regulatory framework, including tax implications in different jurisdictions.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt